Bachelorarbeit

Pro-endliche Gruppen

Jon Brugger

ETH Zürich
Departement Mathematik

Frühjahrssemester 2008
Betreuung: Prof. Dr. Richard Pink

Zürich, den 8. Oktober 2008

Inhaltsverzeichnis

1 Einleitung

Das Hauptziel dieser Bachelorarbeit ist es, pro-endliche Gruppen zu definieren und deren Eigenschaften zu studieren. Hierbei handelt es sich um topologische Gruppen, die kompakt und total unzusammenhängend sind. Pro-endliche Gruppen kommen in vielerlei Situationen vor. Das einfachste Beispiel sind diskrete, endliche Gruppen. Ein weniger triviales Beispiel sind die p-adischen ganzen Zahlen $\mathbb{Z}_p$. Man erhält sie dadurch, dass man $\mathbb{Z}$ bezüglich eines nicht-archimedischen Absolutbetrages $|\cdot|_p : \mathbb{Z} \to \mathbb{Q}$ metrisch vervollständigt. Es existiert jedoch auch eine algebraische Konstruktion der p-adischen ganzen Zahlen als projektiver Limes, nämlich $\mathbb{Z}_p = \varprojlim_{m\in\mathbb{N}} \mathbb{Z}/p^m\mathbb{Z}$. Der projektive Limes ist ein kategorientheoretisches Konzept, welches wir im Verlauf dieser Arbeit einführen und anschliessend fortlaufend verwenden werden. Auf die p-adischen Zahlen werden wir in den Anwendungen genauer eingehen.
Ein weiteres wichtiges Beispiel von pro-endlichen Gruppen, welches wir jedoch nicht weiter behandeln werden, sind die Galoisgruppen. Hierzu betrachtet man eine nicht notwendigerweise endliche Galoiserweiterung L/K. Man definiert nun auf $\mathrm{Gal}(L/K)$ die gröbste Topologie, so dass die kanonischen Restriktionshomomorphismen

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$$

stetig sind für sämtliche in L liegenden, endlichen Galoiserweiterungen M/K, wobei die endlichen Gruppen $\mathrm{Gal}(M/K)$ mit der diskreten Topologie versehen werden. Weiter zeigt man (vgl. [3], Kapitel 4.2), dass $\mathrm{Gal}(L/K)$ mit dieser Topologie eine pro-endliche Gruppe ist. Man kann sogar zeigen, dass $\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(M/K)$ gilt. Dies gestattet es in bestimmten Fällen, die Galoisgruppe explizit zu berechnen; ist beispielsweise $\mathbb{F}$ ein endlicher Körper und $\overline{\mathbb{F}}$ ein algebraischer Abschluss, dann kann man mit dieser Formel zeigen, dass $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ isomorph zu $\prod_p \mathbb{Z}_p$ ist (vgl. [3], Theorem 11). Interessant ist auch, dass ein Analogon des Hauptsatzes der Galoistheorie über endliche Galoiserweiterungen gilt; es stehen nämlich die abgeschlossenen Untergruppen von $\mathrm{Gal}(L/K)$ in Bijektion mit den Zwischenkörpern von L/K. Dieses Beispiel unterstreicht die Relevanz von pro-endlichen Gruppen.
Da der Begriff der topologischen Gruppe zentral für diese Arbeit ist, werden wir diesen zu Beginn definieren und wichtige Eigenschaften beweisen, die für den restlichen Teil der Arbeit die Grundlage bilden. Danach werden wir den projektiven Limes zunächst in allgemeinen Kategorien einführen und anschliessend in den für uns interessanten Kategorien – das sind z.B. topologische Gruppen – weiter behandeln. Damit sind wir dann in der Lage, pro-endliche Gruppen als Spezialfälle von pro-$\mathscr{C}$ Gruppen einzuführen und äquivalente Definitionen herzuleiten. Anschliessend behandeln wir pro-endliche Komplettierungen einer allgemeinen Gruppe. Wir definieren solche durch eine universelle Eigenschaft und zeigen die Eindeutigkeit (bis auf Isomorphie) sowie eine explizite Darstellung als projektiver Limes. Dies ist wichtig für den folgenden Anwendungsteil, in welchem wir insbesondere zeigen werden, dass die pro-endliche Komplettierung von $\mathbb{Z}$ isomorph zu $\prod_p \mathbb{Z}_p$ ist. Im letzten Kapitel beschreiben wir das Kongruenzuntergruppenproblem. Hierbei geht es, vereinfachend gesagt, um die spezielle lineare Gruppe $\mathrm{SL}_n(\mathbb{Z})$ und deren Komplettierung. Konkret untersucht man hierbei, ob jede Untergruppe von $\mathrm{SL}_n(\mathbb{Z})$, die endlichen Index hat, eine der Untergruppen $\Gamma(m), m \in \mathbb{N}^*$ enthält, wobei $\Gamma(m)$ die Menge aller Matrizen in $\mathbb{Z}^{n\times n}$ bezeichnet, die kongruent zur Einheitsmatrix modulo m sind. Ist $n \geq 3$, dann trifft dies tatsächlich zu. Wir werden in diesem Kapitel den Fall $n = 2$ untersuchen und zeigen, dass Gegenbeispiele existieren, d.h. die Aussage des Kongruenzuntergruppenproblems nicht zutrifft.
Voraussetzung für das Verständnis dieser Arbeit sind Grundkenntnisse in Algebra und mengentheoretischer Topologie.

2 Topologische Gruppen

Für die ganze Arbeit spielt der Begriff der topologischen Gruppe eine fundamentale Rolle. Zu diesem Zweck repetieren wir hier kurz die grundlegendsten Ergebnisse. Beginnen wir mit der Definition.

Definition 2.1. Eine Gruppe G zusammen mit einer Topologie, so dass die Abbildung von $G \times G$ (versehen mit der Produkttopologie) nach G gegeben durch $(x, y) \mapsto xy^{-1}$ stetig ist, bezeichnet man als *topologische Gruppe*. Die topologischen Gruppen zusammen mit den stetigen Gruppenhomomorphismen bilden eine Kategorie.
Ist R ein Ring auf welchem eine Topologie definiert ist, so dass $(R, +)$ eine topologische Gruppe ist und die Ringmultiplikation $R \times R \to R$ stetig ist, heisst ein *topologischer Ring*. Die topologischen Ringe zusammen mit den stetigen Ringhomomorphismen bilden eine Kategorie.

Die wichtigsten Eigenschaften topologischer Gruppen sind in dem folgenden Satz zusammengestellt. Wir erinnern daran, dass ein topologischer Raum *total unzusammenhängend* heisst, wenn jede Zusammenhangskomponente aus genau einem Element besteht.

Satz 2.2. Sei G eine Gruppe zusammen mit einer darauf definierten Topologie. Dann gilt die folgende Aussage:

(i) G ist genau dann eine topologische Gruppe, wenn die Multiplikation $G \times G \to G$, $(x, y) \mapsto xy$ und die Inversion $G \to G$, $x \mapsto x^{-1}$ stetig sind. Die Inversion ist dann ein Homöomorphismus.

Ist G mit dieser Topologie zusätzlich eine topologische Gruppe, dann gelten weiter:

(ii) Für jedes $g \in G$ sind die Abbildungen $x \mapsto xg$ und $x \mapsto gx$ von G nach G Homöomorphismen.

(iii) Ist H eine offene (resp. abgeschlossene) Untergruppe von G, so ist jeder Orbit gH bzw. Hg von H offen (resp. abgeschlossen) in G.

(iv) Jede offene Untergruppe von G ist abgeschlossen und jede abgeschlossene Untergruppe von endlichem Index ist offen. Ist G kompakt, dann hat jede offene Untergruppe endlichen Index.

(v) Die Topologie von G ist bereits durch eine Umgebungsbasis des Einselements festgelegt.

(vi) Ein Homomorphismus ist genau dann stetig, wenn er im Einselement stetig ist.

(vii) Ist H eine Untergruppe bzw. $K \trianglelefteq G$ eine normale Untergruppe, dann ist H mit der Teilraumtopologie bzw. G/K mit der Quotientenraumtopologie wiederum eine topologische Gruppe. Die Quotientenraumabbildung $\pi : G \to G/K$ ist offen.

(viii) G ist genau dann hausdorffsch, wenn $\{1\}$ eine abgeschlossene Menge von G ist. Für eine normale Untergruppe $K \trianglelefteq G$ ist der Quotient G/K genau dann hausdorffsch, wenn K abgeschlossen in G ist. Wenn G total unzusammenhängend ist, ist G hausdorffsch.

(ix) Sei G kompakt und seien $X_i, i \in I$ abgeschlossene Teilmengen von G mit der Eigenschaft, dass für alle $i, j \in I$ ein $k \in I$ existiert mit $X_k \subseteq X_i \cap X_j$. Ist Y eine abgeschlossene Teilmenge von G, dann ist $Y(\bigcap_{i\in I} X_i) = \bigcap_{i\in I} Y X_i$.

Beweis. Wir bezeichnen mit φ_G die Funktion $G \times G \to G$, $(x, y) \mapsto xy^{-1}$.
(i) Sind sowohl Multiplikation als auch Inversion stetig, so ist auch φ_G als Verkettung der stetigen Funktion $(x, y) \mapsto (x, y^{-1})$ mit der Multiplikation stetig. Sei umgekehrt φ_G stetig. Die Inversion ist gegeben durch Verkettung der stetigen Funktionen $x \mapsto (1, x)$ und φ_G, und ist somit stetig. Damit ist auch die Multiplikation, die sich als Verkettung von $(x, y) \mapsto (x, y^{-1})$ und φ_G darstellen lässt, stetig. Da das Inverse der Inversion die Inversion ist, muss sie ein Homöomorphismus sein.
(ii) Der Homomorphismus $\mu_g : x \mapsto xg$ ist die Komposition der stetigen Abbildung $x \mapsto (x, g)$ und der Multiplikation. Da letztere nach (i) stetig ist, ist auch μ_g stetig. Dass die inverse Funktion $x \mapsto xg^{-1}$ stetig ist, zeigt man mit dem selben Argument. Insgesamt ist somit μ_g ein Homöomorphismus. Die zweite Behauptung folgert man analog.
(iii) Dies folgt unmittelbar aus (ii).
(iv) Sei H eine Untergruppe von G. Es gilt dann $G\backslash H = \bigcup_{g \in G\backslash H} gH$. Somit ist wegen (iii) H abgeschlossen, wenn H offen ist. Sei jetzt H abgeschlossen mit endlichem Index. Dann ist $G\backslash H$ die Vereinigung von endlich vielen Orbiten, die nach (ii) alle abgeschlossen sind. Somit ist H offen. Nun sei G kompakt und H offen. Die gemäss (iii) offenen Orbite gH definieren eine offene, disjunkte Zerlegung von G. Da G kompakt ist, ist diese Zerlegung endlich und somit ist auch der Index von H endlich.
(v) Die Funktion μ_g aus (ii) ist ein Homöomorphismus und bildet Umgebungsbasen des Einselements auf Umgebungsbasen von $\mu_g(1) = g$ ab. Die Topologie ist aber durch Umgebungsbasen aller Punkte schon eindeutig bestimmt.
(vi) Sei $f : G \to G'$ ein Homomorphismus von topologischen Gruppen, der im Einselement stetig ist. Wegen (ii) ist dann $G \to G \to G' \to G', x \mapsto xg^{-1} \mapsto f(xg^{-1}) \mapsto f(xg^{-1})f(g) = f(x)$ als Verkettung von in g bzw. in 1 bzw. in $f(1)$ stetigen Funktionen stetig in g. Also ist f überall stetig.
(vii) Die Aussage über H ist klar. Sei V offen in G. Nach (iii) ist Vk für jedes $k \in K$ offen und somit ist auch VK offen. Mit $\pi^{-1}(\pi(V)) = VK$ folgt, dass $\pi(V)$ offen in G/K ist. Wir müssen also nur noch zeigen, dass $\varphi_{G/K}$ stetig ist. Dazu sei U offen in G/K und $(w_1K, w_2K) \in \varphi^{-1}_{G/K}(U)$. Da π und φ_G sowie deren Verkettung $(x, y) \mapsto xy^{-1}K$ stetig sind, existieren offene Umgebungen W_1, W_2 von w_1, w_2, so dass $W_1W_2^{-1} \subseteq \pi^{-1}(U)$. Weil π offen ist, ist $\pi(W_1) \times \pi(W_2)$ offen Umgebung von (w_1K, w_2K) in $G/K \times G/K$. Da diese Menge in $\varphi^{-1}_{G/K}(U)$ liegt, folgt die Behauptung.
(viii) Einelementige Mengen, insbesondere $\{1\}$, sind in Hausdorffräumen abgeschlossen. Sei umgekehrt $\{1\}$ abgeschlossen in G. Für zwei unterschiedliche Punkte a, b in G ist die Menge $\{a^{-1}b\}$ gemäss (iii) abgeschlossen. Daher existiert eine offene Umgebung U von 1, die $a^{-1}b$ nicht enthält. Da $\varphi_G^{-1}(U)$ offen ist, gibt es offene Umgebungen V, W von 1 mit $VW^{-1} \subseteq U$. Wegen $a^{-1}b \notin VW^{-1}$ ist $aV \cap bW = \emptyset$. Da aV, bW offene Umgebungen von a, b sind, ist G hausdorffsch. Die zweite Aussage ist eine Konsequenz der ersten Aussage und der Definition der Quotiententopologie. Die dritte Aussage folgt, da Zusammenhangskomponenten stets abgeschlossen sind.
(ix) Offensichtlich ist $Y(\bigcap_{i\in I} X_i) \subseteq \bigcap_{i\in I} YX_i$. Falls $g \notin Y(\bigcap_{i\in I} X_i)$, ist $Y^{-1}g \cap (\bigcap_{i\in I} X_i) = \emptyset$ und weil G kompakt ist, sowie $Y^{-1}g$ und X_i abgeschossen sind, gibt es Indizes $i_1, \dots i_n \in I$ mit $Y^{-1}g \cap X_{i_1} \cap \dots \cap X_{i_n} = \emptyset$. Wegen der Voraussetzung findet man induktiv ein $k \in I$ mit $X_k \subseteq X_{i_1} \cap \dots \cap X_{i_n}$, was $g \notin YX_k$ impliziert. □

Bemerkung 2.3. Sind G_i für $i \in I$ topologische Gruppen, dann ist auch $\prod_{i\in I} G_i$ eine topologische Gruppe zusammen mit der punktweisen Verknüpfung und der Produkttopologie, wie man sofort nachprüft.

Lemma 2.4. Sei G eine kompakte topologische Gruppe. Weiter sei K eine offene und abgeschlossene Teilmenge von G, die das Einselement beinhaltet. Dann gibt es eine offene und normale Untergruppe von G, die in K enthalten ist.

Beweis. Für jedes $x \in K$ ist die Menge $W_x := Kx^{-1}$ eine offene Umgebung von 1, so dass $W_x x \subseteq K$. Da die Multiplikation $G \times G \to G$ stetig ist, gibt es offene Umgebungen L_x, R_x von 1, so dass das Bild von $L_x \times R_x$ in W_x liegt, also $L_x R_x \subseteq W_x$. Wir setzen $S_x := L_x \cap R_x$. Es gilt $S_x S_x \subseteq W_x$ und S_x ist offen. Da K kompakt ist, besitzt die Überdeckung der offenen Mengen $K \cap S_x x, x \in K$ eine endliche Teilüberdeckung, etwa $K \subseteq \bigcup_{j=1}^{n} S_{x_j} x_j$. Der Durchschnitt $S := \bigcap_{j=1}^{n} S_{x_j}$ ist offen und beinhaltet 1. Wir erhalten

$$SK \subseteq \bigcup_{j=1}^{n} S S_{x_j} x_j \subseteq \bigcup_{j=1}^{n} W_{x_j} x_j \subseteq K \tag{1}$$

und schliessen $S \subseteq K$. Offensichtlich ist $T := S \cap S^{-1}$ offen, und es gilt $T^{-1} = T$ sowie $1 \in T$. Wir definieren $T^1 := 1$ und für $n > 1$ induktiv $T^n := T^{n-1}T$ und erhalten so eine Untergruppe $H := \bigcup_{n>0} T^n$ von G. Da H eine Vereinigung von Mengen der Form yT für $y \in G$ ist, muss H offen sein. Nach (1) gilt $T \subseteq K$, was induktiv $T^n \subseteq K$ für alle $n > 0$, also insbesondere $H \subseteq K$ impliziert. Da G kompakt ist, ist der Index von H endlich nach Satz 2.2 (iv). Die Abbildung $G/H \to \{gHg^{-1} \ ; \ g \in G\}$, $gH \mapsto gHg^{-1}$ ist wohldefiniert; denn aus $gH = kH$ folgt $g = kh$ für ein $h \in H$, wonach $gHg^{-1} = khHh^{-1}k^{-1} = kHk^{-1}$ gilt. Da diese Abbildung surjektiv ist, ist die Anzahl von zu H konjugierten Untergruppen endlich. Daher definiert $\bigcap_{g \in G} gHg^{-1}$ die gewünschte offene und normale Untergruppe, die in K enthalten ist. □

Lemma 2.5. Seien X ein kompakter Hausdorffraum, $x \in X$, sowie A der Durchschnitt aller Teilmengen von X, die x enthalten und offen sowie abgeschlossen sind. Dann ist A zusammenhängend. Ist zusätzlich X total unzusammenhängend, dann ist jede offene Menge eine Vereinigung von Mengen, die sowohl offen als auch abgeschlossen sind.

Beweis. Da $x \in A$, ist $A \neq \emptyset$. Sei $A = C \cup D$ für offene, disjunkte Teilmengen C, D von A. Weiter sei $\{K_i \ ; \ i \in I\}$ die Menge aller offenen und abgeschlossenen K_i mit $x \in K_i$. Da C und D abgeschlossen in A und somit auch in X sind, finden wir, da der gegebene Raum T_4 ist, offene Umgebungen U und V von C und D mit $U \cap V = \emptyset$. Da der Durchschnitt $(U \cup V)^c \cap \bigcap_{i \in I} K_i$ leer ist, existieren Indizes $i_1, \ldots, i_n$ mit $(U \cap V)^c \cap K_{i_1} \cap \ldots \cap K_{i_n} = \emptyset$. Daher ist die Menge $I := K_{i_1} \cap \ldots \cap K_{i_n}$ in $U \cup V$ enthalten. Die Mengen $I \cap U$ und $I \cap V$ definieren eine offene Zerlegung der offenen und abgeschlossenen Menge I, sind somit also auch offen sowie abgeschlossen. Sei jetzt o.B.d.A. $x \in U$. Dann ist $A \subseteq I \cap U$, also $D \subseteq A \cap V \subseteq U \cap V = \emptyset$. Somit ist A zusammenhängend.
Sei jetzt X zusätzlich total unzusammenhängend. Die Menge U sei offen und $x \in U$. Es genügt eine Teilmenge von U zu finden, die sowohl offen als auch abgeschlossen in X ist, und die x enthält. Nach dem eben Bewiesenen gibt es für jedes $y \in X \backslash \{x\}$ eine offene und abgeschlossene Menge F_y mit $x \in F_y$ und $y \notin F_y$. Da X die Vereinigung von U und den offenen Mengen $X \backslash F_y$ ist, gibt es Indizes $y_1, \ldots, y_n$ mit $X = U \cup (X \backslash F_{y_1}) \cup \ldots \cup (X \backslash F_{y_n})$. Daher liegt $F_{y_1} \cap \ldots \cap F_{y_n}$ in U, beinhaltet x und ist offen sowie abgeschlossen. □

Proposition 2.6. Sei G eine kompakte und total unzusammenhängende topologische Gruppe. Dann gilt:

(i) Jede offene Teilmenge von G ist die Vereinigung von Orbiten von normalen, offenen Untergruppen.

(ii) Der Durchschnitt aller offenen, normalen Untergruppen ist die triviale Gruppe.

Beweis. (i) Nach Satz 2.2 (viii) ist G hausdorffsch. Sei U eine offene Teilmenge von G und sei $x \in U$. Dann ist $x^{-1}U$ offen und enthält die Eins. Nach Lemma 2.5 beinhaltet $x^{-1}U$ eine offene und abgeschlossene Teilmenge K mit $1 \in K$, welche wiederum wegen Lemma 2.4 eine offene, normale Untergruppe N_x enthält. Somit ist $U = \bigcup_{x \in U} xN_x$.
(ii) Sei $D := \bigcap\{N \ ; \ N \trianglelefteq G, N \text{ offen}\}$. Wir müssen also zeigen, dass $D \subseteq \{1\}$. Hierzu sei $y \notin \{1\}$. Da $\{1\}$ abgeschlossen ist, gibt es eine offene, zu 1 disjunkte Umgebung von y. Nach (i) existiert daher eine offene, normale Untergruppe $N \trianglelefteq G$ mit $1 \notin yN$. Somit gilt auch $y \notin N$, was $y \notin D$ bedeutet. □

3 Projektiver Limes

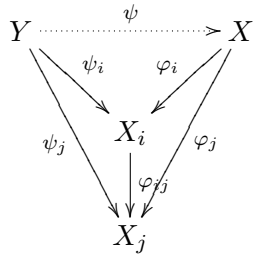
Für die Definition von pro-endlichen Gruppen benötigen wir als Hilfsmittel den projektiven Limes. Diesen werden vor allem bei Gruppen und topologischen Räume brauchen. Der projektive Limes lässt sich jedoch in jeder beliebigen Kategorie einführen, was wir im Folgenden tun werden. Für eine partiell geordnete Menge I seien $X_i, i \in I$, Objekte aus einer festen Kategorie $\mathscr{K}$ (z.B. Gruppen, topologische Räume, topologische Gruppen, Ringe, topologische Ringe, Moduln).

Definition 3.1. Ein *projektives System* (X_i, φ_{ij}, I) besteht aus einer partiell geordneten Indexmenge I, einem Objekt X_i aus der Kategorie $\mathscr{K}$ für jedes $i \in I$ sowie Morphismen $\varphi_{ij} : X_i \to X_j$ für alle $i, j \in I, j \leq i$, so dass $\varphi_{ii} = \mathrm{id}_{X_i}$ für jedes $i \in I$ und $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ für sämtliche $k \leq j \leq i$ gilt.

Definition 3.2. Sei (X_i, φ_{ij}, I) ein projektives System. Weiter sei Y ein weiteres Objekt der gegebenen Kategorie $\mathscr{K}$. Ist zu jedem $i \in I$ ein Morphismus $\psi_i : Y \to X_i$ gegeben, so heissen diese Morphismen *verträglich*, wenn für alle $i, j \in I$ mit $j \leq i$ die Beziehung $\varphi_{ij} \circ \psi_i = \psi_j$ gilt.

Definition 3.3. Ein *projektiver Limes* (X, φ_i) eines projektiven Systems (X_i, φ_{ij}, I) besteht aus einem Objekt $X \in \mathscr{K}$ und verträglichen Morphismen $\varphi_i : X \to X_i$ für $i \in I$, so dass die folgende universelle Eigenschaft gilt: Für jedes Objekt $Y \in \mathscr{K}$ und zugehörige verträgliche Morphismen $\psi_i : Y \to X_i$ mit $i \in I$ existiert genau ein Morphismus $\psi : Y \to X$ mit $\varphi_i \circ \psi = \psi_i$ für alle $i \in I$.

Die Definition des projektiven Limes wird durch die Kommutativität des folgenden Diagramms verdeutlicht.



Definition 3.4. Eine Menge I bezeichnen wir als *gerichtet*, wenn sie partiell geordnet ist, und wenn für alle $i, j \in I$ ein Element $k \in I$ existiert mit $i, j \leq k$.

Bemerkung 3.5. Manche Autoren definieren den projektiven Limes nur im Fall, wo I gerichtet ist. Für die in diesem Kapitel vorgestellten grundlegenden Eigenschaften des Limes in abstrakten Kategorien ist diese Einschränkung unnötig. Wir werden sie erst im nächsten Kapitel benötigen.

Bemerkung 3.6. Seien (X_i, φ_{ij}, I) ein projektives System mit Limes (X, φ_i) und $Y \in \mathscr{K}$. Ist $\rho : Y \to X$ ein Isomorphismus in der Kategorie $\mathscr{K}$, dann ist auch $(Y, \varphi_i \circ \rho)$ ein projektiver Limes von (X_i, φ_{ij}, I).

Im Folgenden werden wir einen projektiven Limes eines projektiven Systems (X_i, φ_{ij}, I) entweder mit $\varprojlim(X_i, \varphi_{ij}, I)$ oder $\varprojlim_{i \in I} X_i$ oder einfach mit $\varprojlim X_i$ bezeichnen. Für eine beliebige Kategorie braucht der projektive Limes nicht zu existieren.

Beispiel 3.7. Wir betrachten eine Sequenz von Morphismen aus der Kategorie $\mathscr{K}$ der endlichen Gruppen, nämlich

$$\cdots \xrightarrow{\rho_{n+2}} G^{n+1} \xrightarrow{\rho_{n+1}} G^n \xrightarrow{\rho_n} \cdots \xrightarrow{\rho_3} G^2 \xrightarrow{\rho_2} G\,,$$

wobei $G \in \mathscr{K}$ mit $\operatorname{card}(G) \geq 2$ und die ρ_n durch $(m_1, \ldots, m_n) \mapsto (m_1, \ldots, m_{n-1})$ für $n \geq 2$ gegeben sind. Offenbar definiert dies ein projektives System $(G^n, \varphi_{nm}, \mathbb{N}^*)$ von endlichen Gruppen, wenn man $\varphi_{nm} := \rho_{m+1} \circ \cdots \circ \rho_n$ sowie $\varphi_{mm} := \mathrm{id}_{G^m}$ für $1 \leq m < n$ setzt. Jedoch existiert kein projektiver Limes in dieser Kategorie, was wir jetzt zeigen wollen. Wir nehmen hierzu indirekt an, der projektive Limes $(X, \varphi_n) = \varprojlim_{n \geq 1} G^n$ würde existieren. Fixiere $l \in \mathbb{N}^*$ und definiere für jedes $n \geq 1$ einen Homomorphismus $\psi_n : G^l \to G^n$ wie folgt: Für $l < n$ setze $\psi_n : (m_1, \ldots, m_l) \mapsto (m_1, \ldots, m_l, 0, \ldots, 0)$ und sonst $\psi_n : (m_1, \ldots, m_l) \mapsto (m_1, \ldots, m_n)$. Da die Morphismen ψ_n mit dem System $(G^n, \varphi_{nm}, \mathbb{N}^*)$ verträglich sind, existiert ein Gruppenhomomorphimus $\psi : G^l \to X$, so dass $\varphi_n \circ \psi = \psi_n$ für alle $n \geq 1$ gilt. Da ψ_n für $l \leq n$ injektiv ist, ist auch ψ injektiv und wir schliessen $2^l \leq \operatorname{card}(G^l) \leq \operatorname{card}(X)$. Da l beliebig war, widerspricht dies der Annahme, dass X eine endliche Gruppe ist.

Die Existenz ist also nicht gewährleistet. Jedoch gilt der folgende Eindeutigkeitssatz.

Satz 3.8. Der projektive Limes eines projektiven Systems (X_i, φ_{ij}, I) ist im Existenzfall eindeutig bestimmt in folgendem Sinn: Sind (X, φ_i) und (Y, ψ_i) projektive Limiten des Systems (X_i, φ_{ij}, I), dann existiert ein eindeutiger Isomorphismus $\varphi : X \to Y$ mit $\psi_i \circ \varphi = \varphi_i$ für alle $i \in I$.

Beweis. Seien (X, φ_i) und (Y, ψ_i) projektive Limiten des Systems (X_i, φ_{ij}, I). Da die Abbildungen $\psi_i : Y \to X_i$ verträglich sind, liefert die universelle Eigenschaft angewandt auf (X, φ_i) einen eindeutigen Morphismus $\psi : Y \to X$ mit $\varphi_i \circ \psi = \psi_i$ für sämtliche $i \in I$. Vertauscht man die Rollen von X und Y, erhält man genauso die Existenz eines eindeutigen Morphismus $\varphi : X \to Y$ mit $\psi_i \circ \varphi = \varphi_i$. Somit gilt für die Funktion $\psi \circ \varphi$ und für beliebiges $i \in I$ die Gleichheit $\varphi_i \circ (\psi \circ \varphi) = \varphi_i$. Da auch id_X diese Gleichung erfüllt und weil (X, φ_i) projektiver Limes ist, müssen die beiden Funktionen übereinstimmen, also $\psi \circ \varphi = \mathrm{id}_X$. Analog zeigt man $\varphi \circ \psi = \mathrm{id}_Y$. Insgesamt ist φ der gesuchte eindeutige Isomorphismus. □

Seien jetzt (X_i, φ_{ij}, I) und (X'_i, φ'_{ij}, I) projektive Systeme über der gleichen partiell geordneten Menge I und der gleichen Kategorie $\mathscr{K}$. Ein *Morphismus* $\Theta : (X_i, \varphi_{ij}, I) \to (X'_i, \varphi'_{ij}, I)$ besteht aus einer Menge von Abbildungen $\theta_i : X_i \to X'_i$ mit $i \in I$, die *Komponenten von* Θ, so dass für $j \leq i$ das Diagramm

$$\begin{array}{ccc} X_i & \xrightarrow{\varphi_{ij}} & X_j \\ {\scriptstyle\theta_i}\downarrow & & \downarrow{\scriptstyle\theta_j} \\ X'_i & \xrightarrow{\varphi'_{ij}} & X'_j \end{array}$$

kommutiert, d.h. es gilt $\theta_j \circ \varphi_{ij} = \varphi'_{ij} \circ \theta_i$. Die Zusammensetzung von zwei Morphismen $\Theta : (X_i, \varphi_{ij}, I) \to (X'_i, \varphi'_{ij}, I)$ und $\Psi : (X'_i, \varphi'_{ij}, I) \to (X''_i, \varphi''_{ij}, I)$ definiert man in kanonischer Weise; die Komponenten von $\Psi \circ \Theta : (X_i, \varphi_{ij}, I) \to (X''_i, \varphi''_{ij}, I)$ sind $\psi_i \circ \theta_i$ und es gilt tatsächlich $(\psi_j \circ \theta_j) \circ \varphi_{ij} = \psi_j \circ \varphi'_{ij} \circ \theta_i = \varphi''_{ij} \circ (\psi_i \circ \theta_i)$. Damit erhalten wir die *Kategorie der projektiven Systeme über der Kategorie* $\mathscr{K}$, wobei die identische Abbildung $\mathrm{id}_{(X_i,\varphi_{ij},I)}$ durch die Komponenten id_{X_i} gegeben ist. Wir wollen jetzt zusätzlich annehmen, dass in $\mathscr{K}$ jedes projektive System einen Limes besitzt. Somit können wir $(X, \varphi_i) := \varprojlim X_i$ und $(X', \varphi'_i) := \varprojlim X'_i$ setzen. Dann sind die Abbildungen $\theta_i \circ \varphi_i : X \to X'_i$ verträglich mit (X'_i, φ'_{ij}, I), da $\varphi'_{ij} \circ (\theta_i \circ \varphi_i) = \theta_j \circ \varphi_j$ gilt. Dies induziert eine Abbildung

$$\varprojlim \Theta : \varprojlim X_i \to \varprojlim X'_i, \tag{2}$$

welche bereits durch die Forderung $\varphi'_i \circ \varprojlim \Theta = \theta_i \circ \varphi_i$ eindeutig bestimmt ist. Es gilt nun die folgende Proposition.

Proposition 3.9. Sei $\mathscr{K}$ eine Kategorie, in welcher jedes projektive System einen Limes besitzt. Dann wird der Projektive Limes $\varprojlim$ zusammen mit der in (2) definierten Abbildung zu einem Funktor von der Kategorie der projektiven Systeme über $\mathscr{K}$ in die Kategorie $\mathscr{K}$.

Beweis. Seien Θ und Ψ Morphismen so wie oben mit zugehörigen Abbildungen $\varprojlim \Theta : \varprojlim X_i \to \varprojlim X'_i$ und $\varprojlim \Psi : \varprojlim X'_i \to \varprojlim X''_i$, dann gilt $\varphi''_i \circ (\varprojlim \Psi \circ \varprojlim \Theta) = \psi_i \circ \varphi'_i \circ \varprojlim \Theta = (\psi_i \circ \theta_i) \circ \varphi_i$, was aufgrund der Eindeutigkeit $\varprojlim \Psi \circ \Theta = \varprojlim \Psi \circ \varprojlim \Theta$ impliziert. Ausserdem gilt (erneut aufgrund der Eindeutigkeit) $\varprojlim \mathrm{id}_{(X_i,\varphi_{ij},I)} = \mathrm{id}_{\varprojlim X_i}$, womit alle Funktoreigenschaften nachgewiesen sind. □

4 Eigenschaften des projektiven Limes

In diesem Abschnitt wollen wir wichtige Eigenschaften des projektiven Limes beweisen, wobei wir uns auf bestimmte Kategorien fokussieren. Im letzten Kapitel wurde bereits bemerkt, dass der Limes nicht existieren muss. Wenn wir uns jedoch auf bestimmte Kategorien einschränken, gilt der folgende Satz.

Satz 4.1. Sei (X_i, φ_{ij}, I) ein projektives System aus der Kategorie der Gruppen bzw. der Ringe bzw. der topologischen Räume bzw. der topologischen Gruppen bzw. der topologischen Ringe. Dann existiert der projektive Limes. Er ist gegeben durch

$$X := \left\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i \; ; \; \forall j \leq i : x_j = \varphi_{ij}(x_i) \right\} \tag{3}$$

sowie $\varphi_i := \pi_i|_X$, wobei $\pi_i : \prod_{j \in I} X_j \to X_i$ die i-te Projektion bezeichnet.

Beweis. Offenbar ist X zusammen mit der punktweisen Verknüpfung bzw. Teilraumtopologie der Produkttopologie bzw. beiden Eigenschaften wieder innerhalb der entsprechenden Kategorie. Beachte, dass für den Fall von Gruppen bzw. Ringen bzw. topologischen Gruppen bzw. topologischen Ringen das Element $(1)_{i \in I}$ in X liegt, also insbesondere $X \neq \emptyset$ gilt. Genauso sind die Abbildungen φ_i Homomorphismen bzw. stetige Homomorphismen, also Morphismen der jeweiligen Kategorie. Aus der Definition von X folgt für $j \leq i$ unmittelbar $\varphi_{ij} \circ \varphi_i = \varphi_j$; die Abbildungen $\varphi_i : X \to X_i$ sind somit verträglich.
Sei nun Y ein Objekt in der jeweiligen Kategorie mit verträglichen Abbildungen $\psi_i : Y \to X_i$,

wobei $i \in I$. Wir definieren $\overline{\psi}$ als die Funktion $Y \to \prod X_i$, die das Element $y \in Y$ auf den Vektor $(\psi_i(y))_{i\in I}$ abbildet. Man sieht leicht, dass $\overline{\psi}$ einen Morphismus in der jeweiligen Kategorie definiert. Für $j \leq i$ gilt dann

$$\pi_j \circ \overline{\psi} = \psi_j = \varphi_{ij} \circ \psi_i = \varphi_{ij} \circ \pi_i \circ \overline{\psi}.$$

Dies zeigt, dass $\overline{\psi}$ die Menge Y nach X abbildet. Jetzt setzen wir $\psi : Y \to X$, $y \mapsto \overline{\psi}(y)$. Dann ist ψ ein Morphismus und für alle i gilt $\varphi_i \circ \psi = \psi_i$. Ist $\psi' : Y \to X$ eine weitere Funktion mit $\varphi_i \circ \psi' = \psi_i$, dann ist der Eintrag von $\psi'(y)$ in X_i gleich $\psi_i(y)$, also $\psi' = \psi$. Die Funktion ψ ist daher eindeutig und somit erfüllt (X, φ_i) die universelle Eigenschaft. Dies zeigt die Behauptung. □

Dieser Satz legitimiert es, vom projektiven Limes von Gruppen bzw. Ringen bzw. topologischen Räumen bzw. topologischen Gruppen bzw. topologischen Ringen zu sprechen. Im weiteren Verlauf werden wir je nach Zusammenhang das Symbol $\varprojlim X_i$ auch für den in (3) explizit definierten projektiven Limes verwenden.

Proposition 4.2. Sei (X_i, φ_{ij}, I) ein projektives System von topologischen Räumen bzw. topologischen Gruppen bzw. topologischen Ringen. Für den Limes $X := \varprojlim X_i$ gilt dann:

(i) Ist jedes X_i hausdorffsch, dann ist X eine hausdorffsche, abgeschlossene Teilmenge von $\prod_{i\in I} X_i$.

(ii) Ist jedes X_i total unzusammenhängend, dann gilt das selbe für X.

(iii) Ist jedes X_i hausdorffsch und kompakt, dann hat auch X diese Eigenschaften.

Beweis. (i) Dass X hausdorffsch ist, folgt aus der Tatsache, dass sich das hausdorffsche Trennungsaxiom auf Produkträume und Unterräume überträgt. Weiter wissen wir, dass für stetige Abbildungen $f, g : Y \to Z$ von einem topologischen Raum Y in einen Hausdorffraum Z der Differenzkern $\{y \in Y \ ; \ f(y) = g(y)\}$ abgeschlossen in Y ist. Daher ist

$$X = \bigcap_{j\leq i} \left\{ x \in \prod_{i\in I} X_i \ ; \ \varphi_{ij} \circ \pi_i(x) = \pi_j(x) \right\}$$

als Durchschnitt abgeschlossener Mengen abgeschlossen.
(ii) Die Eigenschaft, total unzusammenhängend zu sein, überträgt sich auf Unterräume. Beachtet man, dass stetige Bilder zusammenhängender Mengen wiederum zusammenhängend sind, und dass die Projektionen $\pi_i : \prod X_i \to X_i$ stetig sind, so sieht man, dass mit X_i für alle $i \in I$ auch der Produktraum $\prod X_i$ total unzusammenhängend ist. Die Aussage folgt jetzt wie im ersten Teil von (i).
(iii) Nach (i) ist X abgeschlossen in $\prod X_i$. Da letztere Menge nach dem Satz von Tychonoff kompakt ist, ist auch X kompakt. □

Lemma 4.3. Sei (X, φ_i) der projektive Limes eines projektiven Systems (X_i, φ_{ij}, I) von topologischen Räumen bzw. topologischen Gruppen bzw. topologischen Ringen. Weiter sei I gerichtet. Dann gilt:

(i) Die Mengen $\varphi_i^{-1}(U)$, wobei $i \in I$ und U offen in X_i, bilden eine Basis der Topologie auf X.

(ii) Ist Y eine Teilmenge von X, so dass für alle $i \in I$ die Bildmenge $\varphi_i(Y)$ dicht in X_i ist, dann ist Y dicht in X.

Beweis. Wir arbeiten in $\prod X_i$ und verwenden die Symbole aus Satz 4.1.
(i) Jede offene Menge in X ist Vereinigung von Mengen der Form $P = X \cap \pi_{i_1}^{-1}(U_1) \cap \ldots \cap \pi_{i_n}^{-1}(U_n)$, wobei n eine natürliche Zahl ist, $i_1, \ldots, i_n \in I$ und U_r offen in X_{i_r} für $r = 1, \ldots, n$. Es genügt daher zu zeigen, dass für alle $p = (p_i)_{i \in I} \in P$ ein k und eine in X_k offene Menge U existieren mit $p \in \varphi_k^{-1}(U) \subseteq P$. Wähle dazu $k \geq i_1, \ldots, i_n$; dies ist möglich, da I gerichtet ist. Die Menge $\varphi_{ki_r}^{-1}(U_r)$ ist offen in X_k und beinhaltet das Element p_k, da für alle $i \leq k$ gilt, dass $\varphi_{ki}(p_k) = p_i$. Es ist dann $U := \bigcap_{r=1}^{n} \varphi_{ki_r}^{-1}(U_r)$ eine offene Umgebung von p_k und daher $\varphi_k^{-1}(U)$ eine offene Umgebung von p in X. Für $q = (q_i) \in \varphi_k^{-1}(U)$ gilt $q_k \in U$ und $q_{i_r} = \varphi_{ki_r}(q_k) \in U_r$ für alle $r = 1, \ldots, n$. Damit folgt $\varphi_k^{-1}(U) \subseteq P$ wie gewünscht.
(ii) Für alle $i \in I$ und jede nichtleere, offene Teilmenge U in X_i haben wir $\varphi_i(Y) \cap U \neq \emptyset$ und somit $Y \cap \varphi_i^{-1}(U) \neq \emptyset$. Die Aussage folgt jetzt mit (i). □

Definition 4.4. Sei X eine nichtleere Menge. Eine nichtleere Menge $\mathscr{B}$ bestehend aus Teilmengen von X heisst eine *Filterbasis*, wenn $\emptyset \notin \mathscr{B}$ und wenn für alle $B_1, B_2 \in \mathscr{B}$ ein $B_3 \in \mathscr{B}$ existiert mit $B_3 \subseteq B_1 \cap B_2$.

Seien G eine topologische Gruppe und I eine Filterbasis, bestehend aus normalen Untergruppen von G. Setzen wir $L \preceq K$ für $K, L \in I$ genau dann, wenn $K \leq L$ gilt, dann wird I mit der partiellen Ordnung $\preceq$ zu einer gerichteten Menge. Die surjektiven Homomorphismen $q_{KL} : G/K \to G/L, gK \mapsto gL$ für $L \preceq K$ sind stetig; dies folgt aus der universellen Eigenschaft der Quotiententopologie. Es gilt die folgende Proposition.

Proposition 4.5. Seien G, I und q_{KL} so wie oben. Dann ist $(G/K, q_{KL}, I)$ ein projektives System von topologischen Gruppen. Ist $(\widehat{G}, \varphi_K) := \varprojlim G/K$ der Limes dieses Systems, dann gelten weiter die folgenden Aussagen:

(i) Es existiert ein stetiger Homomorphismus $\theta : G \to \widehat{G}$ mit Kern $\bigcap_{K \in I} K$ und dichtem Bild in $\widehat{G}$, so dass $\varphi_K \circ \theta$ die Quotientenabbildung $G \to G/K$ ist, für jedes $K \in I$.

(ii) Ist G kompakt und sind alle $K \in I$ abgeschlossen, dann ist θ surjektiv.

(iii) Ist G kompakt, sind alle $K \in I$ abgeschlossen und ist θ injektiv, dann ist θ ein Isomorphismus von topologischen Gruppen.

Beweis. Offenbar ist $q_{KK} = \mathrm{id}_{G/K}$ für alle $K \in I$, sowie $q_{LM} \circ q_{KL} = q_{KM}$ für sämtlichen $M \preceq L \preceq K$, was zeigt, dass $(G/K, q_{KL}, I)$ ein projektives System von topologischen Gruppen mit wohldefiniertem Limes $(\widehat{G}, \varphi_K)$ ist. Wir identifizieren $\widehat{G}$ als Untergruppe von $H := \prod_{K \in I} G/K$.
(i) Wir definieren die Abbildung $\bar{\theta} : G \to H, g \mapsto (gK)_{K \in I}$ und beachten $gL = q_{KL}(gK)$ für alle $L \preceq K$. Dies zeigt, dass das Bild von $\bar{\theta}$ in $\widehat{G}$ liegt und wir können somit $\theta : G \to \widehat{G}, g \mapsto (gK)_{K \in I}$ setzen. Da die einzelnen Komponenten von θ in das Produkt H Quotientenabbildungen $\varphi_K \circ \theta$ sind, welche insbesondere stetige Homomorphismen sind, ist auch θ ein stetiger Homomorphismus. Für $g \in G$ gilt $g \in \ker(\theta)$ genau dann, wenn $gK = K$ für alle $K \in I$ gilt. Dies zeigt $\ker(\theta) = \bigcap_{K \in I} K$. Da für jedes $K \in I$ gilt, dass $\varphi_K(\theta(G)) = G/K$, folgt mit Lemma 4.3 (ii), dass $\theta(G)$ dicht in $\widehat{G}$ liegt.
(ii) Seien jetzt alle $K \in I$ abgeschlossen und G kompakt. Aus Satz 2.2 (viii) folgt, dass jede Gruppe G/K hausdorffsch ist. Gemäss Proposition 4.2 (i) ist auch $\widehat{G}$ hausdorffsch. Daher ist die kompakte Menge $\theta(G)$ abgeschlossen. Aus der bereits bewiesenen Dichtheit folgt jetzt $\theta(G) = \widehat{G}$.
(iii) Ist zusätzlich θ injektiv, dann ist θ auch ein Homöomorphismus, da G kompakt ist und $\widehat{G}$ hausdorffsch. Insgesamt ist dann θ ein homöomorpher Gruppenisomorphismus. □

5 Pro-$\mathscr{C}$ Gruppen

Wir sind jetzt in der Lage, den Begriff der pro-endlichen Gruppe einzuführen. Dazu betrachten wir die allgemeinere Definition einer pro-$\mathscr{C}$ Gruppe. Hierzu sei $\mathscr{C}$ eine Klasse von endlichen Gruppen, die *abgeschlossen unter Isomorphie* ist; dies bedeutet, dass aus $G \in \mathscr{C}$ und $G \cong G'$ für Gruppen G, G' auch $G' \in \mathscr{C}$ folgt. Die Objekte von $\mathscr{C}$ heissen $\mathscr{C}$-Gruppen und werden alle mit der diskreten Topologie versehen.

Definition 5.1. Eine topologische Gruppe G heisst *pro-$\mathscr{C}$ Gruppe*, wenn ein projektives System (G_i, φ_{ij}, I) von Gruppen aus $\mathscr{C}$ existiert mit gerichteter Indexmenge I, so dass G ein projektiver Limes ist, d.h. $G = \varprojlim G_i$.

Wir bemerken, dass eine $\mathscr{C}$-Gruppe G auch eine pro-$\mathscr{C}$ Gruppe ist, da G der projektive Limes des projektiven Systems $(G, \mathrm{id}_G, \{0\})$ ist.

Definition 5.2. Wir sagen, die Kategorie $\mathscr{C}$ sei *abgeschlossen unter Untergruppenbildung*, wenn mit G auch jede Untergruppe von G eine $\mathscr{C}$-Gruppe ist, und $\mathscr{C}$ heisst *abgeschlossen unter Produktbildung*, wenn das direkte Produkt $G_1 \times G_2$ eine $\mathscr{C}$-Gruppe ist, falls $G_1, G_2 \in \mathscr{C}$. Ist für alle $\mathscr{C}$ Gruppen G und alle $K \trianglelefteq G$ auch G/K eine $\mathscr{C}$ Gruppe, so heisst $\mathscr{C}$ *abgeschlossen unter Quotientenbildung*.

Satz 5.3. Sei $\mathscr{C}$ eine Klasse von endlichen Gruppen, die abgeschlossen unter Untergruppen- und Produktbildung sowie Isomorphie ist, und sei weiter G eine topologische Gruppe. Dann sind die folgenden Aussagen äquivalent:

(i) G ist eine pro-$\mathscr{C}$ Gruppe.

(ii) G ist isomorph (als topologische Gruppe) zu einer abgeschlossenen Untergruppe eines kartesischen Produktes von $\mathscr{C}$-Gruppen.

(iii) G ist kompakt und der Durchschnitt über alle normalen und offenen Untergruppen von G mit Faktorgruppe in $\mathscr{C}$ ist die triviale Gruppe.

(iv) G ist kompakt, total unzusammenhängend und für jede offene, normale Untergruppe $L \trianglelefteq G$ existiert eine offene, normale Untergruppe $N \trianglelefteq G$ mit $N \subseteq L$ und $G/N \in \mathscr{C}$.

Ist $\mathscr{C}$ zusätzlich abgeschlossen unter Quotientenbildung, so kann man (iv) ersetzen durch

(iv)* G ist kompakt, total unzusammenhängend und $G/L \in \mathscr{C}$ für jede offene, normale Untergruppe $L \trianglelefteq G$.

Beweis. (i) $\Rightarrow$ (ii). Diese Implikation haben wir in Proposition 4.2 (i) gezeigt.
(ii) $\Rightarrow$ (iii). Sei G isomorph zu einer abgeschlossenen Untergruppe $\widehat{G}$ von $H := \prod_{i \in I} G_i$, wobei I eine nichtleere Indexmenge ist, so dass $G_i \in \mathscr{C}$ für alle $i \in I$. Es genügt die Aussage für die Menge $\widehat{G}$ zu zeigen, da Kompaktheit, Normalität und Offenheit unter Isomorphie invariant sind, und weil $\mathscr{C}$ abgeschlossen unter Isomorphie ist. Nach dem Satz von Tychonoff ist H kompakt und damit auch die abgeschlossene Teilmenge $\widehat{G}$. Seien jetzt K_i der Kern der Projektion $H \to G_i$ und $N_i := K_i \cap \widehat{G}$. Weil K_i offen und normal in H ist, muss N_i offen und normal in $\widehat{G}$ sein. Aus $\bigcap K_i = 1$ folgt automatisch $\bigcap N_i = 1$. Ausserdem erhält man mit dem ersten Isomorphiesatz $\widehat{G}/N_i \cong \widehat{G}K_i/K_i \leq H/K_i \cong G_i$. Aufgrund der Voraussetzungen an $\mathscr{C}$ gilt $\widehat{G}/N_i \in \mathscr{C}$ für alle $i \in I$. Die Behauptung folgt jetzt, da der gesuchte Durchschnitt in $\bigcap N_i = 1$ enthalten ist.
(iii) $\Rightarrow$ (i). Sei I die Menge aller offenen und normalen Untergruppen von G, deren Faktorgruppe in $\mathscr{C}$ liegt. Für $N_1, N_2 \in I$ betrachte die Abbildung von G in die $\mathscr{C}$-Gruppe $G/N_1 \times G/N_2$

gegeben durch $g \mapsto (gN_1, gN_2)$. Diese Abbildung ist offensichtlich ein stetiger Homomorphismus und der Kern ist gegeben durch $N_1 \cap N_2$. Dieser ist offen und normal in G und $G/(N_1 \cap N_2)$ ist isomorph zu einer Untergruppe von $G/N_1 \times G/N_2$. Weil $\mathscr{C}$ abgeschlossen unter Isomorphie sowie Untergruppenbildung ist, gilt $N_1 \cap N_2 \in I$. Wir haben also gezeigt, dass I eine Filterbasis von normalen Untergruppen ist. Weil offene Untergruppen nach Satz 2.2 (iv) abgeschlossen sind, können wir Proposition 4.5 anwenden und finden $G \cong \varprojlim_{N \in I} G/N$ im Sinn von topologischen Gruppen. Also ist G eine pro-$\mathscr{C}$ Gruppe gemäss Bemerkung 3.6.
(i) $\Rightarrow$ (iv). Es gelte $(G, \varphi_i) = \varprojlim_{i \in I} G_i$ für $G_i \in \mathscr{C}$. Nach dem bereits bewiesenen ist G kompakt. Proposition 4.2 (ii) zeigt, dass G total unzusammenhängend ist. Sei jetzt $L \trianglelefteq G$ offen. Weil $1 \in L$, gibt es nach Lemma 4.3 (i) ein $i \in I$ mit $N := \ker(\varphi_i) \leq L$. Nun ist N normal und offen in G und es gilt $G/N \cong \mathrm{im}(\varphi_i) \leq G_i$. Somit ist $G/N \in \mathscr{C}$.
(iv) $\Rightarrow$ (iii). Wir müssen nur zeigen, dass der angegebene Durchschnitt trivial ist, also $D := \bigcap_{N \in I} N = 1$, wobei $I = \{N \ ; \ N \trianglelefteq G, N \text{offen}, G/N \in \mathscr{C}\}$. Sei $L \trianglelefteq G$ eine offene, normale Untergruppe. Nach Voraussetzung existiert ein $N \in I$ mit $N \subseteq L$. Also gilt $D \subseteq L$ für jede offene, normale Untergruppe L. Da der Durchschnitt aller solcher L nach Proposition 2.6 (ii) trivial ist, folgt $D = 1$.
Sei jetzt $\mathscr{C}$ zusätzlich abgeschlossen unter Quotientenbildung. Wir müssen somit nur noch zeigen: (iv) $\Rightarrow$ (iv)*. Sei L eine offene, normale Untergruppe von G. Nach Voraussetzung finden wir ein $N \trianglelefteq G$, mit Faktorgruppe in $\mathscr{C}$ und $N \leq L$. Es gilt dann mit dem zweiten Isomorphiesatz $G/L \cong (G/N)/(L/N)$. Wir schliessen, dass $G/L \in \mathscr{C}$ wie behauptet. □

Definition 5.4. Ist $\mathscr{C}$ die Klasse der endlichen Gruppen, dann heissen die pro-$\mathscr{C}$ Gruppen auch *pro-endliche Gruppen*. Analog heissen die pro-$\mathscr{C}$ Gruppen im Fall, wo $\mathscr{C}$ die Klasse der endlichen p-Gruppen ist, auch *pro-p Gruppen*.

Somit erhalten wir aus dem letzten Satz die folgenden äquivalenten Definitionen für pro-endliche Gruppen.

Korollar 5.5. Sei G eine topologische Gruppe. Dann sind äquivalent:

(i) G ist pro-endlich.

(ii) G ist isomorph (als topologische Gruppe) zu einer abgeschlossenen Untergruppe eines kartesischen Produktes von endlichen Gruppen.

(iii) G ist kompakt und der Durchschnitt aller normalen, offenen Untergruppen von G ist die triviale Gruppe.

(iv) G ist kompakt und total unzusammenhängend.

Beweis. Folgt aus Satz 5.3, da nach Satz 2.2 (iv) jede offene Untergruppe in einer kompakten Gruppe endlichen Index hat. □

Proposition 5.6. Seien G eine pro-$\mathscr{C}$ Gruppe, H eine abgeschlossene Untergruppe, $K \trianglelefteq G$ eine normale, abgeschlossene Untergruppe und I eine Filterbasis bestehend aus offenen, normalen Untergruppen, so dass $\bigcap_{N \in I} N = 1$ ist. Dann gelten

$$(G, q_N) = \varprojlim_{N \in I} G/N \ , \ (H, q'_{H \cap N}) = \varprojlim_{N \in I} H/(H \cap N) \ , \ (G/K, q''_{KN}) = \varprojlim_{N \in I} G/KN,$$

wobei $q_N : G \to G/N$, $q'_{H \cap N} : H \to H/(H \cap N)$ und $q''_{KN} : G/K \to G/KN$ die kanonischen Homomorphismen sind.

Beweis. Die ersten zwei Aussagen folgen sofort aus Proposition 4.5 und Bemerkung 3.6. Die Menge $J := \{KN\ ;\ N \in I\}$ ist eine Filterbasis aus offenen, normalen Untergruppen von G, die K enthalten. Nach Satz 2.2 (ix) gilt $\bigcap_{M\in J} M = K \bigcap_{N\in I} N = K$, was erneut wegen Proposition 4.5 zunächst $G/K \cong \varprojlim_{N\in I} G/KN$ impliziert. Die letzte Behauptung folgt jetzt mit Bemerkung 3.6. □

Der nächste Satz zeigt, wie sich pro-$\mathscr{C}$ Gruppen unter Bildung von Produkten, Untergruppen und Faktorgruppen verhalten.

Satz 5.7. Sei $\mathscr{C}$ eine Klasse von endlichen Gruppen, die abgeschlossen unter Untergruppen- und Produktbildung sowie Isomorphie ist. Dann sind abgeschlossene Untergruppen, Produkte und projektive Limiten von pro-$\mathscr{C}$ Gruppen ebenfalls pro-$\mathscr{C}$ Gruppen. Ist $\mathscr{C}$ zusätzlich abgeschlossen unter Quotientenbildung, dann sind Faktorgruppen, die von einer abgeschlossenen, normalen Untergruppe einer pro-$\mathscr{C}$ Gruppe gebildet werden, ebenfalls pro-$\mathscr{C}$ Gruppen.

Beweis. Aus der Äquivalenz von (i) und (ii) in Satz 5.3 folgt die Aussage für abgeschlossene Untergruppen, da abgeschlossene Untergruppen von abgeschlossenen Untergruppen wiederum abgeschlossen sind. Sind X_i für $i \in I$ topologische Räume und $A_i \subseteq X_i$ abgeschlossene Unterräume, dann ist $\prod_{i\in I} A_i$ abgeschlossen in $\prod_{i\in I} X_i$. Dies impliziert die Aussage für Produkte, da Produkte von Produkten trivialerweise Produkte sind. Da pro-$\mathscr{C}$ Gruppen hausdorffsch sind, ist der projektive Limes von pro-$\mathscr{C}$ Gruppen gemäss Satz 4.2 (i) isomorph zu einer abgeschlossene Untergruppe eines Produktes von pro-$\mathscr{C}$ Gruppen, also wiederum eine abgeschlossene Untergruppe eines Produktes von $\mathscr{C}$ Gruppen. Die Aussage über Faktorgruppen erhält man aus Proposition 5.6, wobei man $I := \{N \trianglelefteq G, N\text{offen}\}$ setzt und Satz 5.3 (iii), (iv)* anwendet. □

6 Komplettierung

Sei I eine Filterbasis von normalen Untergruppen einer gegebenen Gruppe G. Wie in den Vorbemerkungen zu Proposition 4.5 wird I zu einer gerichteten Menge, wenn man $L \preceq K$ für $K, L \in I$ genau dann setzt, wenn $K \leq L$ gilt. Wir können auf der Gruppe G für jedes solche I eine Topologie definieren, indem wir eine Teilmenge offen nennen, wenn sie die Vereinigung von Orbiten der Form gK ist, wobei $g \in G$ und $K \in I$. Dass dies tatsächlich eine Topologie definiert, garantiert uns die folgende Proposition.

Proposition 6.1. Sei G eine Gruppe und I eine Filterbasis von normalen Untergruppen von G. Dann ist die Menge $\mathscr{B} := \{gK\ ;\ K \in I, g \in G\}$ eine Basis einer Topologie auf G. Diese Topologie ist mit der Gruppenstruktur verträglich, d.h. G wird zu einer topologischen Gruppe.

Beweis. Da die Vereinigung aller Mengen aus $\mathscr{B} \neq \emptyset$ die ganze Gruppe G ergibt, müssen wir für den ersten Teil nur noch zeigen, dass der Schnitt zweier Elemente aus $\mathscr{B}$ eine Vereinigung von Elementen aus $\mathscr{B}$ ist. Seien also $K, K' \in I$ und $g, g' \in G$. Weil I eine Filterbasis ist, gibt es ein $K'' \in \mathscr{B}$ mit $K'' \subseteq K \cap K'$. Da die Bahnen eine Zerlegung der Gruppe definieren, finden wir für jedes x in $gK \cap g'K'$ ein $g_x \in G$ mit $x \in g_xK''$. Wir können schreiben $x = gk = g'k' = g_xk''$ für Elemente $k \in K, k' \in K', k'' \in K''$. Es gilt dann $g_xK'' = xk''^{-1}K'' = xK'' = gkK'' \subseteq gK$. Analog gilt $g_xK'' \subseteq g'K'$, woraus $g_xK'' \subseteq gK \cap g'K'$ folgt. Wir haben also wie gewünscht $gK \cap g'K' = \bigcup g_xK''$ gezeigt.
Wir müssen somit nur noch beweisen, dass $\varphi_G : (x, y) \mapsto xy^{-1}$ in jedem Punkt (x, y) stetig ist. Jede Umgebung U von xy^{-1} enthält eine Menge $gK \in \mathscr{B}$ mit $xy^{-1} \in gK$ und wir erhalten dadurch $xy^{-1}K \subseteq U$. Es existieren Punkte $h, h' \in G$, so dass x bzw. y in hK bzw. $h'K$ enthalten ist, was mit $x = hk$ bzw. $y = h'k'$ für $k, k' \in K$ gleichbedeutend ist. Die Normalität von K impliziert daher $hK(h'K)^{-1} = xk^{-1}KK^{-1}k'y^{-1} = xKy^{-1} = xy^{-1}K$. Wir haben insgesamt gezeigt,

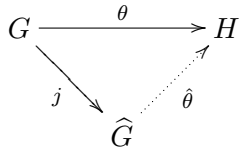
dass $\varphi_G^{-1}(U)$ die offene Menge $hK \times h'K$ von (x, y) beinhaltet. Somit ist der Homomorphismus φ_G stetig. □

Wir nennen diese durch das obige Lemma charakterisierte Topologie die von I *induzierte Topologie*. Von nun an sei die Gruppe G mit dieser Topologie versehen.

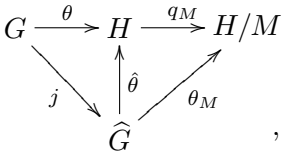
Definition 6.2. Eine *Komplettierung* $(\widehat{G}, j)$ *von* G *bezüglich* I besteht aus einer topologischen Gruppe $\widehat{G}$ und einem stetigen Homomorphismus $j : G \to \widehat{G}$ mit der folgenden universellen Eigenschaft: Für jeden stetigen Homomorphismus $\theta : G \to H$ in eine diskrete Gruppe H existiert ein eindeutiger stetiger Homomorphismus $\hat{\theta} : \widehat{G} \to H$ mit $\theta = \hat{\theta} \circ j$. Ist $\widehat{G}$ eine pro-endliche Gruppe und haben alle Untergruppen aus I endlichen Index, so spricht man von einer *pro-endlichen Komplettierung bzgl.* I.

Die universelle Eigenschaft von Komplettierungen lässt sich auf pro-endliche Gruppen ausdehnen in folgendem Sinn.

Proposition 6.3. Sei $(\widehat{G}, j)$ eine Komplettierung von G bezüglich I. Dann existiert für jeden stetigen Homomorphismus $\theta : G \to H$ in eine pro-endliche Gruppe H ein eindeutiger stetiger Homomorphismus $\hat{\theta} : \widehat{G} \to H$, so dass $\theta = \hat{\theta} \circ j$ gilt. Dies wird durch die Kommutativität des folgenden Diagramms verdeutlicht.



Beweis. Die Menge aller offenen, normalen $M \trianglelefteq H$ bezeichnen wir mit J. Weiter sei q_M die Quotientenabbildung $H \to H/M$. Wir betrachten jetzt das Diagramm



,

wobei die Abbildungen $\hat{\theta}, \theta_M$ noch zu definieren sind. Die Gruppe H ist nach Korollar 5.5 kompakt. Weiter ist H/M diskret; dies folgt aus der Tatsache, dass $q_M^{-1}(hM) = hM$ für jedes $h \in H$ offen ist. Da $\widehat{G}$ eine Komplettierung von G ist, existiert ein eindeutiger stetiger Homomorphismus $\theta_M : \widehat{G} \to H/M$ mit $q_M \circ \theta = \theta_M \circ j$. Für $M \leq N, M, N \in J$ sei q_{MN} der Homomorphismus $hM \mapsto hN$. Nach Proposition 4.5 ist $(H/M, q_{MN}, J)$ ein projektives System von topologischen Gruppen. Aus Korollar 5.5 (iii) und Proposition 5.6 wissen wir, dass (H, q_M) ein projektiver Limes dieses Systems ist. Wir haben $q_N = q_{MN} \circ q_M$ und somit

$$q_{MN} \circ \theta_M \circ j = q_{MN} \circ q_M \circ \theta = q_N \circ \theta = \theta_N \circ j.$$

Die Eindeutigkeit von θ_N zeigt, dass $q_{MN} \circ \theta_M = \theta_N$. Daher ist $(\widehat{G}, \theta_M)$ mit dem System $(H/M, q_{MN}, J)$ verträglich. Es existiert daher ein eindeutiger stetiger Homomorphismus $\hat{\theta} : \widehat{G} \to H$ mit $q_M \circ \hat{\theta} = \theta_M$. Wir wissen jetzt, dass für alle $M \in J$ und alle $g \in G$ gilt $q_M \circ \hat{\theta} \circ j(g) = q_M \circ \theta(g)$. Dies impliziert $\hat{\theta}(j(g))(\theta(g))^{-1} \in \ker q_M = M$. Korollar 5.5 zeigt $\bigcap_{M \in J} M = 1$ und wir schliessen $\hat{\theta} \circ j = \theta$ wie gewünscht. Sei jetzt $\tau : \widehat{G} \to H$ ein weiterer stetiger Homomorphismus mit $\tau \circ j = \theta$. Dann ist $(q_M \circ \tau) \circ j = q_M \circ \theta$ und es folgt $q_M \circ \tau = \theta_M$ aufgrund der Eindeutigkeit von θ_M. Wie oben folgt für jedes $u \in \widehat{G}$ aus $q_M(\tau(u)) = q_M(\hat{\theta}(u))$ die Beziehung $\hat{\theta}(u)(\tau(u))^{-1} \in \ker q_M = M$ für alle $M \in J$. Wie oben schliessen wir $\tau = \hat{\theta}$. □

Jetzt sind wir in der Lage zu zeigen, dass eine pro-endliche Komplettierung existiert und bis auf Isomorphie sogar eindeutig ist. Definiere dazu für $K, L \in I$ mit $L \leq K$ die surjektive Abbildung $q_{LK} : G/L \to G/K$, welche gL auf gK abbildet. Damit wird (G, q_{LK}, I) gemäss Proposition 4.5 zu einem projektiven System mit Limes $(\widehat{G}, \varphi_K) := \varprojlim_{K \in I} G/K$.

Proposition 6.4. Sei I eine Filterbasis von normalen Untergruppen von G mit endlichen Index. Dann existiert die pro-endliche Komplettierung bzgl. I und ist bis auf Isomorphie eindeutig. Genauer gilt:

(i) Die Gruppe $\widehat{G} := \varprojlim G/K$ zusammen mit der Abbildung $j : G \to \widehat{G}$ gegeben durch $g \mapsto (gK)_{K \in I}$ ist eine pro-endliche Komplettierung von G bezüglich I.

(ii) Sind $(\widehat{G}_1, j_1)$, $(\widehat{G}_2, j_2)$ pro-endliche Komplettierungen von G bezüglich I, dann existiert ein eindeutiger Isomorphismus von topologischen Gruppen $\alpha : \widehat{G}_1 \to \widehat{G}_2$ mit $\alpha \circ j_1 = j_2$.

Beweis. (i) Dass j stetig und wohldefiniert ist, haben wir in Proposition 4.5 gezeigt. Seien H eine diskrete topologische Gruppe und $\theta : G \to H$ ein stetiger Homomorphismus. Da $\ker(\theta)$ offen ist, existiert wegen Proposition 6.1 ein $L \in I$ mit $L \subseteq \ker(\theta)$. Wir definieren $\hat{\theta} : \widehat{G} \to H$ als die Abbildung $\theta' \circ \varphi_L$, wobei $\theta' : G/L \to H$ durch $gL \mapsto \theta(g)$ gegeben ist. Offensichtlich ist $\hat{\theta}$ wohldefiniert, stetig und ein Homomorphismus mit $\theta = \hat{\theta} \circ j$. Ist $\tau : \widehat{G} \to H$ ein weiterer stetiger Homomorphismus mit $\theta = \tau \circ j$, dann stimmen $\hat{\theta}$ und τ auf der dichten Menge $j(G)$ überein (vgl. Proposition 4.5). Da der Differenzkern der Abbildungen $\hat{\theta}$ und τ in den Hausdorffraum H abgeschlossen ist, gilt $\hat{\theta} = \tau$. Damit ist $\hat{\theta}$ eindeutig.
(ii) Betrachten wir die Komplettierung $(\widehat{G}_1, j_1)$ und den stetigen Homomorphismus j_2, so liefert Proposition 6.3 einen eindeutigen stetigen Homomorphismus $\alpha : \widehat{G}_1 \to \widehat{G}_2$ mit $\alpha \circ j_1 = j_2$. Vertauschen wir die Rollen von $\widehat{G}_1$ und $\widehat{G}_2$, erhalten wir einen eindeutigen stetigen Homomorphismus β mit $\beta \circ j_2 = j_1$. Damit gilt $j_1 = (\mathrm{id}_{\widehat{G}_1}) \circ j_1 = (\beta \circ \alpha) \circ j_1$. Mit der Eindeutigkeit aus Proposition 6.3 schliessen wir $\mathrm{id}_{\widehat{G}_1} = \beta \circ \alpha$. Analog zeigt man $\mathrm{id}_{\widehat{G}_2} = \alpha \circ \beta$. Also ist α ein Isomorphismus. □

Proposition 6.5. Sei $(\widehat{G}, j)$ eine pro-endliche Komplettierung von G bzgl. I, wobei alle Untergruppen aus I endlichen Index haben. Dann ist $j(G)$ dicht in $\widehat{G}$ und $\ker j = \bigcap_{K \in I} K$. Ist G kompakt, so ist j surjektiv. Ist G kompakt und j injektiv, so ist j ein Isomorphismus von topologischen Gruppen.

Beweis. Nach Proposition 6.4 können wir annehmen, dass $\widehat{G} = \varprojlim_{K \in I} G/K$ gilt. Die Aussage folgt jetzt direkt aus Proposition 4.5, da offene Mengen von topologischen Gruppen abgeschlossen sind. □

Sei jetzt $\mathscr{C}$ eine Klasse von endlichen Gruppen, die abgeschlossen unter Untergruppenbildung, Produktbildung und Isomorphie ist. Seien weiter G eine Gruppe und K, L normale Untergruppen mit G/K und G/L in $\mathscr{C}$. Dann ist $K \cap L$ der Kern des Homomorphismus $G \to G/K \times G/L$ gegeben durch $g \mapsto (gK, gL)$. Somit ist auch die Faktorgruppe von G nach $K \cap L$ in $\mathscr{C}$. Die Menge aller normalen Untergruppen von G mit Faktorgruppe in $\mathscr{C}$ bildet somit eine Filterbasis und wir können definieren:

Definition 6.6. Die *pro-$\mathscr{C}$ Komplettierung* $\widehat{G}$ einer Gruppe G ist die pro-endliche Komplettierung bezüglich der Filterbasis, bestehend aus allen normalen Untergruppen von G mit Faktorgruppe in $\mathscr{C}$. Nach Proposition 6.4 gilt also $\widehat{G} = \varprojlim_{K \in I} G/K$, wobei $I := \{K \trianglelefteq G \,;\, G/K \in \mathscr{C}\}$. Ist $\mathscr{C}$ die Klasse aller endlichen Gruppen, so nennen wir die pro-$\mathscr{C}$ Komplettierung auch die *pro-endliche Komplettierung.*

7 p-adische Zahlen

Wir wollen hier ein wichtiges Beispiel einer Komplettierung genauer betrachten, nämlich die Gruppe $\widehat{\mathbb{Z}}$. Hierzu benötigen wir den Begriff der p-adischen Zahlen $\mathbb{Z}_p$.

Definition 7.1. Sei $(\mathbb{Z}/p^m\mathbb{Z}, \rho_{p,mn}, \mathbb{N})$ das projektive System von topologischen Ringen, wobei p eine feste Primzahl ist, und für $m, n \in \mathbb{N}, n \leq m$ der Morphismus $\rho_{p,mn}$ definiert ist als $r + \mathbb{Z}/p^m\mathbb{Z} \mapsto r + \mathbb{Z}/p^n\mathbb{Z}$. Der projektive Limes $(\mathbb{Z}_p, \rho_{p,m}) := \varprojlim_{m\in\mathbb{N}} \mathbb{Z}/p^m\mathbb{Z}$ heisst der *Ring der p-adischen Zahlen.*

Wir betrachten jetzt die pro-endliche Komplettierung von $\mathbb{Z}$, also $(\widehat{\mathbb{Z}}, \sigma_k) := \varprojlim_{k\in\mathbb{N}^*} \mathbb{Z}/k\mathbb{Z}$. Wir fassen dies als projektiven Limes des projektiven Systems $(\mathbb{Z}/k\mathbb{Z}, \sigma_{kl}, \mathbb{N}^*)$ von topologischen Ringen auf, wobei $\mathbb{N}^*$ mit der Teilbarkeitsrelation zu einer gerichteten Menge wird und wo $\sigma_{kl} : \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/l\mathbb{Z}$ für $l|k$ der kanonische Ringepimorphismus ist. Es gilt dann der folgende wichtige Satz über die Komplettierung von $\mathbb{Z}$.

Satz 7.2. Es bezeichne $\mathbb{P}$ die Menge aller Primzahlen. Dann existiert ein Isomorphismus von topologischen Ringen

$$\widehat{\mathbb{Z}} \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p.$$

Beweis. Wir verwenden die Symbole von oben und setzen zur Abkürzung $R := \prod_{p\in\mathbb{P}} \mathbb{Z}_p$. Sei $k \in \mathbb{N}^*$ mit Primfaktorzerlegung $k = \prod_{p\in\mathbb{P}} p^{\alpha_p(k)}$, wobei natürlich fast alle Exponenten $\alpha_p(k) \in \mathbb{N}$ verschwinden. Der chinesische Restsatz liefert dann einen kanonischen Ringisomorphismus $\nu_k : \mathbb{Z}/k\mathbb{Z} \to \prod_{p\in\mathbb{P}} \mathbb{Z}/p^{\alpha_p(k)}\mathbb{Z}$, der zu einem Isomorphismus von topologischen Ringen wird, wenn wir beide Seiten mit der diskreten Topologie versehen. Weiter ist die komponentenweise gebildete Funktion

$$\mu_k : R \to \prod_{p\in\mathbb{P}} \mathbb{Z}/p^{\alpha_p(k)}\mathbb{Z}\ ,\ (x_p)_{p\in\mathbb{P}} \mapsto (\rho_{p,\alpha_p(k)}(x_p))_{p\in\mathbb{P}}$$

ein stetiger Ringhomomorphismus. Somit können wir für jedes $k \in \mathbb{N}^*$ einen Morphismus $\varphi_k := \nu_k^{-1} \circ \mu_k : R \to \mathbb{Z}/k\mathbb{Z}$ von topologischen Ringen definieren. Für alle $k, l \in \mathbb{N}^*$ mit $l|k$ gilt dann $\sigma_{kl} \circ \varphi_k = \varphi_l$; dies folgt nämlich aus der Kommutativität des folgenden Diagramms.

$$\begin{array}{ccccc}
\mathbb{Z}_p & \xrightarrow{\rho_{p,\alpha_p(k)}} & \mathbb{Z}/p^{\alpha_p(k)}\mathbb{Z} & \twoheadleftarrow & \mathbb{Z}/k\mathbb{Z} \\
\Big\downarrow{\scriptstyle \mathrm{id}} & & \Big\downarrow{\scriptstyle \rho_{p,\alpha_p(k)\alpha_p(l)}} & & \Big\downarrow{\scriptstyle \sigma_{kl}} \\
\mathbb{Z}_p & \xrightarrow{\rho_{p,\alpha_p(l)}} & \mathbb{Z}/p^{\alpha_p(l)}\mathbb{Z} & \twoheadleftarrow & \mathbb{Z}/l\mathbb{Z}
\end{array}$$

Daher sind diese Morphismen verträglich mit dem projektiven System $(\mathbb{Z}/k\mathbb{Z}, \sigma_{kl}, \mathbb{N}^*)$ von topologischen Ringen.
Sei jetzt S ein weiterer topologischer Ring mit Morphismen $\psi_k : S \to \mathbb{Z}/k\mathbb{Z}$, die ebenfalls mit dem System $(\mathbb{Z}/k\mathbb{Z}, \sigma_{kl}, \mathbb{N}^*)$ verträglich sind. Indem man die Projektionen $\tau_{p,k} : \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/p^{\alpha_p(k)}\mathbb{Z}$ anwendet, erhält man für jede Primzahl p einen Morphismus $\psi_{p,k} = \tau_{p,k} \circ \psi_k : S \to \mathbb{Z}/p^{\alpha_p(k)}\mathbb{Z}$, wobei für $l \mid k$ gilt, dass $\rho_{p,\alpha_p(k)\alpha_p(l)} \circ \psi_{p,k} = \rho_{p,\alpha_p(k)\alpha_p(l)} \circ \tau_{p,k} \circ \psi_k = \tau_{p,l} \circ \sigma_{kl} \circ \psi_k = \psi_{p,l}$. Insbesondere ist $\psi_{p,k} = \psi_{p,k'}$ falls $\alpha_p(k) = \alpha_p(k')$. Wir erhalten daher für festes $p \in \mathbb{P}$ und für jedes $m \in \mathbb{N}$ eine eindeutige Abbildung $S \to \mathbb{Z}/p^m\mathbb{Z}$, und diese Abbildungen sind mit dem System $(\mathbb{Z}/p^m\mathbb{Z}, \rho_{p,mn}, \mathbb{N})$ verträglich. Somit existiert ein eindeutiger Morphismus $\psi'_p : S \to \mathbb{Z}_p$ mit $\rho_{p,\alpha_p(k)} \circ \psi'_p = \psi_{p,k}$. Für den induzierten Morphismus $\psi : S \to R\ ,\ s \mapsto (\psi'_p(s))_{p\in\mathbb{P}}$ gilt dann offenbar $\varphi_k \circ \psi = \nu_k^{-1} \circ (\rho_{p,\alpha_p(k)} \circ \psi'_p)_{p\in\mathbb{P}} = \nu_k^{-1} \circ (\psi_{p,k})_{p\in\mathbb{P}} = \psi_k$. Weil die ψ'_p den Morphismus

ψ mit dieser Gleichung komponentenweise bestimmen, muss, da die ψ'_p eindeutig sind, auch ψ eindeutig sein. Wir haben somit gezeigt, dass (R, φ_k) ein projektiver Limes von $(\mathbb{Z}/k\mathbb{Z}, \sigma_{kl}, \mathbb{N}^*)$ ist. Die Behauptung folgt jetzt aus Satz 3.8. □

Definition 7.3. Sei R ein kommutativer, unitärer Ring, $n \in \mathbb{N}^*$ sowie $X = (x_{ij})_{i,j} \in R^{n\times n}$. Wie üblich definiert man dann die *Determinante* von X als

$$\det(X) := \sum_{\sigma\in\mathscr{S}_n} \operatorname{sgn}(\sigma) x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{n\sigma(n)} ,$$

wobei $\mathscr{S}_n$ die n-te symmetrische Gruppe bezeichnet. Die gewöhnlichen Rechenregeln für Determinanten über Körpern lassen sich dann sinngemäss auf kommutative, unitäre Ringe übertragen. Ist R' ein weiterer Ring und $f : R \to R'$ ein Ringhomomorphismus, so gilt für die Matrix $f(X) := (f(x_{ij}))_{i,j}$ offensichtlich $\det(f(X)) = f(\det(X))$.

Definition 7.4. Seien R ein kommutativer, unitärer Ring und $n \in \mathbb{N}^*$. Dann ist die *spezielle lineare Gruppe* $\mathrm{SL}_n(R)$ die Menge aller $n \times n$ Matrizen mit Einträgen in R und Determinante gleich 1. Aufgrund der Cramer'schen Regel sind Elemente aus $\mathrm{SL}_n(R)$ invertierbar. Die Inversen Elemente liegen dann auch wieder in $\mathrm{SL}_n(R)$, was zeigt, dass es sich tatsächlich um eine Gruppe handelt. Ist R ein topologischer Ring, so versehen wir $\mathrm{SL}_n(R) \subseteq R^{n^2}$ mit der Unterraumtopologie des Produktraumes R^{n^2}. Weil Matrixmultiplikation und Matrixinversion in $\mathrm{SL}_n(R)$ sich auf Multiplikation und Addition in R zurückführen lassen, wird die spezielle lineare Gruppe zu einer topologischen Gruppe.

Proposition 7.5. Es gibt einen Isomorphismus von topologischen Gruppen

$$\mathrm{SL}_n(\widehat{\mathbb{Z}}) \cong \prod_{p\in\mathbb{P}} \mathrm{SL}_n(\mathbb{Z}_p).$$

Beweis. Sowohl $\widehat{\mathbb{Z}}$ als auch $\mathbb{Z}_p$ sind kommutative, unitäre topologische Ringe. Nach Satz 7.2 existiert ein Isomorphismus $\varphi : \widehat{\mathbb{Z}} \to \prod_{p\in\mathbb{P}} \mathbb{Z}_p$ von topologischen Ringen. Ist q eine Primzahl, so bezeichnen wir mit $\pi_q : \prod_{p\in\mathbb{P}} \mathbb{Z}_p \to \mathbb{Z}_q$ die q-te Projektion. Wir wollen nun zeigen, dass die Abbildung

$$\psi : \mathrm{SL}_n(\widehat{\mathbb{Z}}) \to \prod_{p\in\mathbb{P}} \mathrm{SL}_n(\mathbb{Z}_p) \ , \ (x_{ij})_{i,j} \mapsto ((\pi_p \circ \varphi(x_{ij}))_{i,j})_{p\in\mathbb{P}}$$

einen Isomorphismus von topologischen Gruppen definiert. Die Abbildung ψ ist wegen $\det((\pi_p \circ \varphi(x_{ij}))_{i,j}) = \pi_p \circ \varphi(\det((x_{ij})_{i,j}))$ wohldefiniert. Betrachtet man diese Funktion komponentenweise für alle $p \in \mathbb{P}$ und für alle $(i, j) \in n \times n$, so sieht man sofort, dass es sich um einen stetigen Gruppenhomomorphismus handelt. Sei nun $\psi(x) = (\mathrm{id})_{p\in\mathbb{P}}$ für ein $x = (x_{ij})_{i,j} \in \mathrm{SL}_n(\widehat{\mathbb{Z}})$. Dann gilt $\forall p, i \neq j : \pi_p \circ \varphi(x_{ij}) = 0 \wedge \pi_p \circ \varphi(x_{ii}) = 1$ woraus $\forall i \neq j : \varphi(x_{ij}) = 0 \wedge \varphi(x_{ii}) = 1$ und schlussendlich $x = \mathrm{id}$ folgt. Wir haben somit gezeigt, dass ψ injektiv ist. Ist $y = ((y_{p,ij})_{i,j})_{p\in\mathbb{P}} \in \prod_{p\in\mathbb{P}} \mathrm{SL}_n(\mathbb{Z}_p)$, so gilt für alle $p \in \mathbb{P}$, dass $\det((y_{p,ij})_{i,j}) = 1$. Daher hat auch $((y_{p,ij})_{p\in\mathbb{P}})_{i,j} \in \left(\prod_{p\in\mathbb{P}} \mathbb{Z}_p\right)^{n\times n}$ Determinante 1. Setzen wir $x := (\varphi^{-1}((y_{p,ij})_{p\in\mathbb{P}}))_{i,j} \in \widehat{\mathbb{Z}}^{n\times n}$, so sehen wir, dass $x \in \mathrm{SL}_n(\widehat{\mathbb{Z}})$ und $\psi(x) = y$ gelten. Somit ist ψ auch surjektiv. □

8 Das Kongruenzuntergruppenproblem

An dieser Stelle soll ein Problem aus der Zahlentheorie und der Gruppentheorie vorstellt werden. Es handelt sich dabei um das Kongruenzuntergruppenproblem. Pro-endliche Gruppen spielen dabei eine wichtige Rolle. Wesentlich für dieses Problem sind die folgenden Definitionen. Dazu so von nun an immer $n \in \mathbb{N}^*$ vorausgesetzt.

Definition 8.1. Sei H eine Untergruppe von $\mathrm{SL}_n(\mathbb{Z})$. Dann heisst H eine *arithmetische Untergruppe*, falls der Index endlich ist.

Definition 8.2. Sei $0 \neq k\mathbb{Z} \subseteq \mathbb{Z}$ ein nichttriviales Ideal und $\pi_k : \mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ die komponentenweise Projektion. Dann heisst $\Gamma(k) := \ker(\pi_k)$ eine *Hauptkongruenzuntergruppe*. Jede Untergruppe von $\mathrm{SL}_n(\mathbb{Z})$, die eine Hauptkongruenzuntergruppe enthält, nennen wir eine *Kongruenzuntergruppe*.

Da $\mathbb{Z}/k\mathbb{Z}$ eine endliche Gruppe ist, ist auch $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ endlich und daher hat $\Gamma(k)$ endlichen Index in $\mathrm{SL}_n(\mathbb{Z})$. Hieraus folgt, dass Kongruenzuntergruppen endlichen Index besitzen, d.h. Kongruenzuntergruppen sind arithmetische Untergruppen. Umgekehrt kann man sich die Frage stellen, ob jede arithmetische Untergruppe von $\mathrm{SL}_n(\mathbb{Z})$ eine Kongruenzuntergruppe ist. Dies bezeichnet man als das sog. *Kongruenzuntergruppenproblem*. In der modernen Formulierung kann man dieses Problem noch auf weitere Gruppen ausdehnen. Man beachte, dass Kongruenzuntergruppen in vielen Situationen auftreten; z.B. im Hauptschritt von Wiles' Beweis des grossen Fermat'schen Satzes.
Für diesen hier betrachteten Spezialfall wurde das Kongruenzuntergruppenproblem bereits 1962 vollständig gelöst. Es gilt nämlich der folgende Satz, den Bass, Lazard und Serre sowie unabhängig Mennicke gezeigt haben. Dieses Resultat wurden 1965 von Bass, Milnor und Serre verallgemeinert. Für einen Beweis siehe [2].

Satz 8.3. Jede arithmetische Untergruppe von $\mathrm{SL}_n(\mathbb{Z})$ für $n \geq 3$ ist eine Kongruenzuntergruppe.

An dieser Stelle soll noch kurz auf den Zusammenhang zwischen diesem Satz und den pro-endlichen Gruppen bzw. der pro-endlichen Komplettierung eingegangen werden. Zunächst ein Lemma.

Lemma 8.4. Sei $(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \varphi_{kl}, \mathbb{N}^*)$ das projektive System von topologischen Gruppen mit den kanonischen, stetigen Homomorphismen $\varphi_{kl} : \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/l\mathbb{Z})$ für $l \mid k$. Es gibt dann einen Isomorphismus von topologischen Gruppen

$$\mathrm{SL}_n(\widehat{\mathbb{Z}}) \cong \varprojlim_{k \in \mathbb{N}^*} \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}).$$

Beweis. Wir setzen $\varphi_k : \mathrm{SL}_n(\widehat{\mathbb{Z}}) \to \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$, $(x_{ij})_{i,j} \mapsto (\sigma_k(x_{ij}))_{i,j}$, wobei $\sigma_k : \widehat{\mathbb{Z}} \to \mathbb{Z}/k\mathbb{Z}$ so wie im letzten Kapitel definiert ist. Da die Abbildungen σ_k mit dem System $(\mathbb{Z}/k\mathbb{Z}, \sigma_{kl}, \mathbb{N})$ verträglich sind, gilt $\varphi_{kl} \circ \varphi_k = \varphi_l$, d.h. die φ_k sind mit $(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \varphi_{kl}, \mathbb{N}^*)$ verträglich. Sei Y eine weitere topologische Gruppe mit verträglichen Abbildungen $\psi_k : Y \to \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ für alle $k \in \mathbb{N}^*$. Wir betrachten nun die einzelnen Komponenten $\psi_{ij,k} : Y \to \mathbb{Z}/k\mathbb{Z}$ für alle $(i,j) \in n \times n$ von ψ_k. Für fixe i, j sind die Homomorphismen $\psi_{ij,k}$ mit dem projektiven System $(\mathbb{Z}/k\mathbb{Z}, \sigma_{kl}, \mathbb{N}^*)$ verträglich, daher existiert eine eindeutige Abbildung $\psi_{ij} : Y \to \widehat{\mathbb{Z}}$ mit $\sigma_k \circ \psi_{ij} = \psi_{ij,k}$. Offenbar ist $\psi' := (\psi_{ij})_{i,j} : Y \to \widehat{\mathbb{Z}}^{n \times n}$ ein stetiger Ringhomomorphismus. Bezeichnet $\pi_k : \widehat{\mathbb{Z}}^{n \times n} \to (\mathbb{Z}/k\mathbb{Z})^{n \times n}$ die Abbildung $(x_{ij})_{i,j} \mapsto (\sigma_k(x_{ij}))_{i,j}$, dann gilt $\psi_k = \pi_k \circ \psi'$. Dies impliziert für beliebiges $y \in Y$, dass $\sigma_k(\det(\psi'(y))) = 1$. Da dies für alle k gilt, ist, weil σ_k die Einschränkung der Projektion ist, $\det(\psi'(y)) = 1$ und wir können $\psi : Y \to \mathrm{SL}_n(\widehat{\mathbb{Z}})$, $y \mapsto \psi'(y)$ setzen. Damit gilt $\varphi_k \circ \psi = \psi_k$. Durch diese Gleichung ist ψ bereits eindeutig festgelegt, da alle ψ_{ij} eindeutig sind. Wir haben insgesamt gezeigt, dass $(\mathrm{SL}_n(\widehat{\mathbb{Z}}), \varphi_k)$ ein projektiver Limes ist. Die Behauptung folgt jetzt aus Satz 3.8. □

Bemerkung 8.5. Man kann zeigen, dass die Homomorphismen $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ für alle $k \in \mathbb{N}^*$ surjektiv sind. Somit gilt auch $\mathrm{SL}_n(\mathbb{Z})/\Gamma(k) \cong \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$. Wir verzichten jedoch auf einen Beweis dieser nichttrivialen Tatsache (vgl. [4], S. 158 (ii) und [1], S. 18, Corollary 5.2).

Korollar 8.6. Die pro-endliche Komplettierung von $\mathrm{SL}_n(\mathbb{Z})$ ist für $n \geq 3$ isomorph zu $\mathrm{SL}_n(\widehat{\mathbb{Z}})$.

Beweis. Sei I die Menge der Hauptkongruenzuntergruppen $\Gamma(k)$ für $k \in \mathbb{N}^*$ in $\mathrm{SL}_n(\mathbb{Z})$. Dies ist eine Filterbasis von normalen Untergruppen mit endlichem Index, da $\Gamma(kk') \subseteq \Gamma(k) \cap \Gamma(k')$ gilt. Gemäss Proposition 6.1 ist somit I die Umgebungsbasis des Einselements einer Topologie auf $\mathrm{SL}_n(\mathbb{Z})$. Die Menge aller normalen Untergruppen mit endlichem Index definiert genauso eine Umgebungsbasis von 1 einer weiteren Topologie auf $\mathrm{SL}_n(\mathbb{Z})$ und diese Topologie ist offensichtlich feiner. Da nach Satz 8.3 jede arithmetische Untergruppe eine Gruppe aus I enthält, induzieren diese beiden Topologien die gleichen Umgebungen von 1, sind somit gemäss Satz 2.2 (v) identisch. Weil die Komplettierung allein von der Topologie abhängt, gilt nach Proposition 6.4 also

$$\widehat{\mathrm{SL}_n(\mathbb{Z})} \cong \varprojlim_{k \in \mathbb{N}^*} \mathrm{SL}_n(\mathbb{Z})/\Gamma(k).$$

Aufgrund von Bemerkung 8.5 und wegen Proposition 3.9 (Funktoren bilden Isomorphismen auf Isomorphismen ab) gilt $\varprojlim_{k \in \mathbb{N}^*} \mathrm{SL}_n(\mathbb{Z})/\Gamma(k) \cong \varprojlim_{k \in \mathbb{N}^*} \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$. Wir können jetzt Lemma 8.4 anwenden und sind fertig. □

Erstaunlicherweise gilt Satz 8.3 nicht für den Fall $n = 2$. Diese Tatsache wurde bereits Ende des 19. Jahrhunderts von Fricke und Klein bewiesen und soll im Folgenden erarbeitet werden. Wir benötigen den folgenden Hilfssatz, der auch unter dem Namen „Ping Pong Lemma“ bekannt ist.

Lemma 8.7. Sei G eine Gruppe, die auf einer Menge S operiert. Weiter seien $S_1, S_2 \subseteq S$ Teilmengen mit $S_2 \nsubseteq S_1$ und seien G_1, G_2 Untergruppen von G mit $\mathrm{card}(G_1) \geq 3$, so dass folgendes gilt:

$$\forall g \in G_1 \backslash \{1\} : gS_2 \subseteq S_1 \ , \ \forall h \in G_2 \backslash \{1\} : hS_1 \subseteq S_2.$$

Dann ist die Untergruppe G_0, welche von $G_1 \cup G_2$ erzeugt wird, kanonisch isomorph zum freien Produkt $G_1 * G_2$.

Beweis. Aufgrund der universellen Eigenschaft des freien Produktes existiert ein kanonischer Homomorphismus $\varphi : G_1 * G_2 \to G_0$. Da dieser offenbar surjektiv ist, müssen wir nur noch die Injektivität überprüfen. Wir nehmen hierzu indirekt an, w sei ein reduziertes, nichttriviales Wort mit $\varphi(w) = 1$. Wir betrachten zuerst denn Fall, wo w mit einem Element aus G_1 anfängt und aufhört, d.h. $w = g_1 * h_1 * \cdots * g_n$ mit $g_i \in G_1 \backslash \{1\}$, $h_i \in G_2 \backslash \{1\}$ und $n > 0$. Wir erhalten aufgrund der Voraussetzungen $S_2 = \varphi(w)S_2 = g_1 h_1 \cdots g_n S_2 \subseteq S_1$, also einen Widerspruch. Wir können somit ohne Einschränkung annehmen, dass w von der Form $g * h_1 * g_1 * \cdots * h_n$ oder $h_1 * g_1 * \cdots * g^{-1}$ oder $h_1 * g_1 * \cdots * h_n$ ist, wobei $g, g_i \in G_1 \backslash \{1\}$ und $h_i \in G_2 \backslash \{1\}$. Wir wählen ein $g' \in G_1 \backslash \{1, g^{-1}\}$ und setzen $v := g' * w * g'^{-1}$. Es gilt $\varphi(v) = \varphi(g')\varphi(g'^{-1}) = 1$. Weil die reduzierte Darstellung von v mit nichttrivialen Elementen aus G_1 anfängt und aufhört, führt dies nach dem bereits Bewiesenen auf einen Widerspruch. □

Lemma 8.8. Die Matrizen $A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ und $B := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ erzeugen eine freie Untergruppe von $\mathrm{SL}_2(\mathbb{Z})$ mit freiem Erzeugendensystem $\{A, B\}$.

Beweis. Man prüft leicht nach, dass $\mathrm{SL}_2(\mathbb{Z})$ vermöge $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) := \frac{az+b}{cz+d}$ auf $\mathscr{H} := \{z \in \mathbb{C} \ ; \ \mathrm{Im}(z) > 0\}$ operiert. Wir setzen jetzt $C := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $G_1 := \langle A \rangle = \left\{ \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} \ ; \ k \in \mathbb{Z} \right\}$, $G_2 := \langle C \rangle = \{\mathrm{id}, C\}$ sowie $S_1 := \{z \in \mathscr{H} \ ; \ |\mathrm{Re}(z)| > 1\}$ und $S_2 := \{z \in \mathscr{H} \ ; \ |z| < 1\}$. Seien $z_1 \in S_1$ und $z_2 \in S_2$. Es gilt dann $|Cz_1| = |1/z_1| < 1$ sowie $\mathrm{Re}\left(\begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix} z_2 \right) = \mathrm{Re}(z_2 + 2k) > 1$ für

$k \in \mathbb{Z}^*$. Daher sind alle Bedingungen von Lemma 8.7 erfüllt und wir können schliessen, dass ein kanonischer Isomorphismus $\varphi : \langle A\rangle * \langle C\rangle \to \langle A, C\rangle$ existiert. Weiter gibt es einen kanonischen, surjektiven Homomorphismus $\psi : \langle A\rangle * \langle B\rangle \to \langle A, B\rangle$. Aus $B = CAC$ folgt $\langle A, B\rangle \subseteq \langle A, C\rangle$. Die Zuordnung $A^k \mapsto A^k$, $B^k \mapsto C * A^k * C$ induziert aufgrund der universellen Eigenschaft einen Homomorphismus $\rho : \langle A\rangle * \langle B\rangle \to \langle A\rangle * \langle C\rangle$ und es gilt $\psi = \varphi \circ \rho$ (beachte $CC = \mathrm{id}$). Da ρ nichttriviale Worte auf nichttriviale Worte abbildet, ist ρ injektiv und daher auch ψ. Daher ist ψ ein Isomorphismus. Weil A und B unendliche Ordnungen haben, ist $\langle A\rangle * \langle B\rangle$ sogar frei mit freiem Erzeugendensystem $\{A, B\}$. □

Lemma 8.9. Die Hauptkongruenzuntergruppe $\Gamma(2)$ von $\mathrm{SL}_2(\mathbb{Z})$ wird von den Elementen $A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $B := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ und $-\mathrm{id}$ erzeugt. Zudem hat die Untergruppe H, welche von A und B erzeugt wird, endlichen Index in $\Gamma(2)$.

Beweis. Offensichtlich sind die angegebenen Matrizen Elemente von $\Gamma(2)$, also ist auch die davon erzeugte Gruppe in $\Gamma(2)$ enthalten. Sei umgekehrt $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$. Ist $c = 0$, dann folgt aus $ad = 1$, dass entweder $M \in \langle A\rangle$ oder $-M \in \langle A\rangle$ gilt. Sei jetzt $c \neq 0$. Es existiert eine Darstellung $a = 2q_1c + r_1$ mit $q_1, r_1 \in \mathbb{Z}$ und $|r_1| \leq |c|$. Da a ungerade ist und c gerade, ist r_1 ungerade und daher gilt sogar $|r_1| < |c|$. Somit gilt $A^{-q_1}M = \begin{pmatrix} 1 & -2q_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r_1 & * \\ c & * \end{pmatrix} \in \Gamma(2)$. Wie oben findet man $q_2, r_2 \in \mathbb{Z}$ mit $c = 2q_2r_1 + r_2$, so dass $|r_2| < |r_1| < |c|$ und r_2 gerade ist. Jetzt gilt $B^{-q_2}A^{-q_1}M = \begin{pmatrix} 1 & 0 \\ -2q_2 & 1 \end{pmatrix}\begin{pmatrix} r_1 & * \\ c & * \end{pmatrix} = \begin{pmatrix} r_1 & * \\ r_2 & * \end{pmatrix}$. Iteriert man dieses Verfahren, erhält man nach endlich vielen Schritten eine Matrix $N \in H$ mit $NM = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. Diese letzte Matrix ist, wie wir zu Beginn dieses Beweises festgestellt haben, von der Form $\pm A^t, t \in \mathbb{Z}$. Wir haben also $\Gamma(2) \subseteq H \cup -H$ gezeigt. Offenbar gilt dann auch $\mathrm{card}(\Gamma(2)/H) \leq 2$. □

Jetzt sind wir in der Lage, den Hauptsatz dieses Kapitels zu beweisen.

Satz 8.10. Es gibt unendlich viele arithmetische Untergruppen von $\mathrm{SL}_2(\mathbb{Z})$, die keine Kongruenzuntergruppen sind.

Beweis. Aus Lemma 8.8 und 8.9 wissen wir, dass $H = \langle A, B\rangle$ frei mit Erzeugendensystem $\{A, B\}$ ist, und endlichen Index in $\Gamma(2)$ hat. Für jedes Element $w \in H$ sei $e_A(w) \in \mathbb{Z}$ die Summe aller Exponenten von A, die in w vorkommen. Da H frei ist, ist $e_A : H \to \mathbb{Z}$ ein wohldefinierter Gruppenhomomorphismus. Sind $l \geq 1$ und $\pi_l : \mathbb{Z} \to \mathbb{Z}/l\mathbb{Z}$ die Restklassenabbildung, so setzen wir $\Gamma_l := \ker(\pi_l \circ e_A)$. Da Γ_l endlichen Index in H hat, hat Γ_l auch endlichen Index in $\mathrm{SL}_2(\mathbb{Z})$, ist somit eine arithmetische Untergruppe. Wir wollen zeigen, dass Γ_l keine Kongruenzuntergruppe ist, falls l keine Potenz von 2 ist. Nehmen wir indirekt an, es sei $l = 2^t k$ mit ungeradem $k > 1$ und es existiere ein $n \in \mathbb{N}^*$ mit $\Gamma(n) \subseteq \Gamma_l$. Dann gilt aber auch $\Gamma(kn) \subseteq \Gamma_l$. Wir können also o.B.d.A. annehmen, es existiere ein ungerades n und ein $m \geq 0$ mit $\Gamma(2^m kn) \subseteq \Gamma_l$. Da $2^m 5kn$ und $5kn - 4$ teilerfremd sind, gibt es eine ganze Zahl s mit $s(5kn - 4) \equiv 1 \pmod{2^m 5kn}$. Dies impliziert $s \equiv -4s \equiv 1 \pmod 5$. Wir schreiben $s = 5r + 1$. Es gilt $P := B^r ABA^{kn-1} = \left(\begin{pmatrix} 1 & 0 \\ 2r & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\right)\left(\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2(kn-1) \\ 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 2 \\ 2r & 4r+1 \end{pmatrix}\begin{pmatrix} 1 & 2(kn-1) \\ 2 & 4kn-3 \end{pmatrix} = \begin{pmatrix} 5 & 2(5kn-4) \\ 2s & \delta \end{pmatrix} \in H$ für ein $\delta \in \mathbb{Z}$, wie man leicht nachrechnet. Aus der Bedingung $\det(P) = 1$ schliessen wir $\delta \equiv 1 \pmod{2^m kn}$. Genauso ist $Q :=$

$A^{5kn-4}B^s = \begin{pmatrix} 1 & 2(5kn-4) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2s & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 2(5kn-4) \\ 2s & 1 \end{pmatrix} \in H$ für ein $\alpha \in \mathbb{Z}$. Wie oben folgt aus $\det(Q) = 1$, dass $\alpha \equiv 5 \pmod{2^m 5kn}$. Insgesamt gilt $P \equiv Q \pmod{2^m kn}$, woraus $PQ^{-1} \in \Gamma(2^m kn)$ folgt. Jedoch gilt $e_A(PQ^{-1}) = -4kn + 4 \equiv 4 \not\equiv 0 \pmod{k}$ also auch $e_A(PQ^{-1}) \not\equiv 0 \pmod{l}$. Dies steht im Widerspruch zu $PQ^{-1} \in \Gamma_l$. □

Literaturverzeichnis

[1] Hyman Bass. *K-theory and stable algebra.* Publications mathémathiques de l'I.H.É.S., tome 22 (1964), p. 5-60.

[2] Hyman Bass, John Milnor, Jean-Pierre Serre. *Solution of the congruence subgroup problem for* $\mathrm{SL}_n(n \geq 3)$ *and* $\mathrm{Sp}_{2n}(n \geq 2)$. Publications mathémathiques de l'I.H.É.S., tome 33 (1967), p. 59-137.

[3] Siegfried Bosch. *Algebra.* Berlin, Heidelberg 2006, 6. Auflage.

[4] Luis Ribes, Pavel Zalesskii. *Profinite Groups.* Oxford University Press Inc., New York 1998.

[5] B. Sury. *The Congruence Subgroup Problem: An Elementary Approach Aimed at Applications.* Hindustan Book Agency, Neu-Delhi 2003.

[6] John S. Wilson. *Profinite Groups.* Oxford University Press Inc., New York 1998.