Unendliche Galoistheorie

Eine (Index-) Menge I heiße ausgerichtet, falls sie teilgeordnet ist und zu je zwei Elementen $i, j \in I$ ein $k \in I$ mit $i \le k$, $j \le k$ existiert.

Für jedes $i \in I$ liege nun eine Menge (eine Gruppe, ein Ring, ein R-Modul, ...) M_i vor und zugleich, für $i \le j$, Abbildungen (Gruppen-, Ring-, R-Modulhomomorphismen, ...) $\varphi_{ji} : M_j \to M_i$ mit

$$\varphi_{ii} = 1 \quad \text{und} \quad \varphi_{ji}\varphi_{kj} = \varphi_{ki} \quad \text{für} \quad i \le j \le k \ .$$

Solch ein System von Mengen (Gruppen, ...) heißt ein inverses System.

DEFINITION. *$\varprojlim_i M_i = \{(\dots, m_i, \dots) \in \prod_{i\in I} M_i : \ \varphi_{ji}(m_j) = m_i$ für $i \le j\}$ heißt der projektive Limes des inversen Systems $\{M_i : i \in I\}$.*

Die i-te Projektion $\prod_{i\in I} M_i \to M_i$ induziere die Abbildung $\varphi_i : \varprojlim_i M_i \to M_i$.

Beobachtungen:

1. Ist I vollständig geordnet und sind alle $M_i \neq \emptyset$ und endlich, so ist $\varprojlim_i M_i \neq \emptyset$. In diesem Fall ist nämlich $N_i = \bigcap_{j\ge i} \mathrm{im}\,(\varphi_{ji})$ eine nichtleere Teilmenge von M_i und die φ_{ji} induzieren Surjektionen $N_j \twoheadrightarrow N_i$. Und offenbar gilt $\emptyset \neq \varprojlim_i N_i = \varprojlim_i M_i$ sowie $\varprojlim_i N_i \overset{\varphi_i}{\twoheadrightarrow} N_i$ $(\forall\, i)$.

2. Der projektive Limes ist, sofern nichtleer, eine Menge (Gruppe, ...), falls die M_i Mengen (Gruppen, ...) sind.

3. $\varprojlim_i M_i$ löst die universelle Aufgabe

   Ist M eine Menge (Gruppe, ...) mit Abbildungen (Homomorphismen, ...) $\psi_i : M \to M_i$, die $\varphi_{ji}\psi_j = \psi_i$ erfüllen, so existiert genau ein(e) Abbildung (Homomorphismus, ...) $\psi : M \to \varprojlim_i M_i$ mit $\varphi_i\psi = \psi_i$.

4. Die ausgerichtete Teilmenge $I' \subset I$ heißt cofinal in I, wenn es zu jedem $i \in I$ ein $i' \in I'$ mit $i \le i'$ gibt. In dem Fall gilt $\varprojlim_i M_i = \varprojlim_{i'} M_{i'}$.

Wir betrachten im folgenden nur endliche nichtleere Mengen M_i (Gruppen, ...) und versehen diese mit der diskreten Topologie, d.h. daß jede Teilmenge von M_i offen in M_i ist. Im Fall von z.B. Gruppen M_i ist dann die Multiplikation homöomorph.

Zur Erinnerung: Eine Menge T heißt ein topologischer Raum, wenn gewisse seiner Teilmengen als “offen” ausgezeichnet sind und dafür folgende Bedingungen gelten

1. $\emptyset$ und T sind offen
2. beliebige Vereinigungen von offenen Mengen sind offen
3. endliche Durchschnitte offener Mengen sind offen.

Der topologische Raum T heißt hausdorffsch, wenn zu je zwei Elementen (Punkten) $t_1 \neq t_2$ aus T offene Mengen (Umgebungen) $O_1 \ni t_1$, $O_2 \ni t_2$ mit $O_1 \cap O_2 = \emptyset$ existieren.

T heißt kompakt, wenn T hausdorffsch ist und jede Überdeckung $T = \bigcup_\nu O_\nu$ von T durch offene Mengen O_ν eine endliche Überdeckung enthält: $T = \bigcup_{s=1}^n O_{\nu_s}$.

Eine Abbildung $f : T_1 \to T_2$ zwischen zwei topologischen Räumen heißt stetig, falls $f^{-1}(O_2)$ offen in T_1 für jede offene Menge $O_2 \subset T_2$ gilt. Ist f bijektiv, so heißt f ein Homöomorphisms, wenn sowohl f als auch f^{-1} stetig sind.

Sind T_ν topologische Räume, so wird $P \stackrel{\text{def}}{=} \prod_\nu T_\nu$ zu einem topologischen Raum, wenn man als offene Mengen von P beliebige Vereinigungen endlicher Durchschnitte von Mengen des Typs $\prod_\nu O_\nu$ nimmt, und zwar mit O_ν offen in T_ν und $O_\nu = T_\nu$ für alle bis auf einen Index ν_0. Diese Topologie ist so gemacht, daß die Projektionen $P \to T_\nu$ alle stetig sind. Oben angegebene Mengen zusammen bilden eine *Subbasis* der Topologie von P; die Mengen $\prod_\nu O_\nu$ mit $O_\nu = T_\nu$ für fast alle Indizes ν (d.h. alle bis auf endlich viele Ausnahmen) bilden eine *Basis* der Topologie von P.

Der Satz von Tychonov besagt: *Sind alle T_ν kompakt, so auch $P = \prod_\nu T_\nu$.*

Folgerung. *$\varprojlim_i M_i$ ist kompakt und alle φ_i sind stetig. Des weiteren: Ist in der 3. Beobachtung oben M ein topologischer Raum und sind die ψ_i stetig, so ist ψ stetig.*

Denn die M_i sind endlich, also trivialerweise kompakt, und $\varprojlim_i M_i$ ist abgeschlossen (i.e. das Komplement ist offen) im kompakten Raum $\prod_{i \in I} M_i$. Die zusätzlichen Behauptungen folgen sofort.

Definition. *Im Falle, daß alle M_i endliche Gruppen sind, heißt $\varprojlim_i M_i$ eine proendliche Gruppe.*

Man überprüft, daß dann die Multiplikation und Inversenbildung in $\varprojlim_i M_i$ Homöomorphismen sind.

Beispiele:

1. Es sei $I = \mathbb{N}$ mit $[\, i \leq j \iff i|j \,]$, $M_i = \mathbb{Z}/i$, und $\varphi_{ji} : \mathbb{Z}/j \to \mathbb{Z}/i$ sende $z \mod j$ nach $z \mod i$. Dann ist $\hat{\mathbb{Z}} \stackrel{\text{def}}{=} \varprojlim_i \mathbb{Z}/i$ sogar ein Ring und alle φ_i sind surjektiv. Des weiteren $\hat{\mathbb{Z}}^\times = \varprojlim_i (\mathbb{Z}/p^i)^\times$.

2. $I = \mathbb{N}$ mit der gewöhnlichen Anordnung und die Primzahl p liefern $M_i = \mathbb{Z}/p^i$, $\varphi_{ji} : n \mod p^j \mapsto n \mod p^i$, damit den projektiven Limes $\mathbb{Z}_p \stackrel{\text{def}}{=} \varprojlim_i \mathbb{Z}/p^i$, die sogenannten p-adichen Zahlen; $\mathbb{Z}_p$ ist wieder ein Ring.

   $\mathbb{Z}_p$ ist ein $\mathbb{Z}$ enthaltender überabzählbarer nullteilerfreier Ring. Sei nun z.B. $p = 5$. Dann gehört $\frac{1}{4} = \frac{1}{p-1}$ zu $\mathbb{Z}_5$. Denn $4 \cdot (\ldots, x_n \mod 5^n, \ldots) = 1$ mit $x_n = -(1 + 5 + \ldots + 5^{n-1}) = \frac{1}{4}(1 - 5^n)$. Betrachte nun $\sum_{k=0}^m 5^k = \frac{1}{4}(5^{m+1} - 1) \in \mathbb{Z} \subset \mathbb{Z}_5$. Die

Zahl 5^{m+1}, in $\mathbb{Z}_5$ gelesen, ist $(\ldots, 5^{m+1} \mod 5^n, \ldots)_n$, hat also den Eintrag 0 für $n \leq m+1$ und "konvergiert" damit gegen 0 für $m \to \infty$, i.e.

$$1 + 5 + 5^2 + \ldots = -\frac{1}{4} \quad \text{in} \quad \mathbb{Z}_5 \, .$$

Um die Konvergenz zu rechtfertigen, brauchen wir allerdings eine Topologie auf $\mathbb{Z}_5$:
Setze, für $0 \neq z \in \mathbb{Z}$, $w_5(z) = \alpha$, wenn $z = 5^\alpha z'$ mit $5 \nmid z'$ gilt; setze auch $w_5(0) = \infty$ und $w_5(\frac{z}{n}) = w_5(z) - w_5(n)$ für $\frac{z}{n} \in \mathbb{Q}$. Dann folgt

$$w_5(ab) = w_5(a) + w_5(b) \, , \ w_5(a+b) \geq \min(w_5(a), w_5(b)) \ (\forall \, a, b \in \mathbb{Q}) \, .$$

Und $|a|_5 \overset{\text{def}}{=} 5^{-w_5(a)}$ liefert

$$|a|_5 \in \mathbb{R}_{\geq 0} \, , \, |a|_5 = 0 \iff a = 0 \, , \, |ab|_5 = |a|_5 |b|_5 \, , \, |a+b|_5 \leq \max(|a|_5, |b|_5) \leq |a|_5 + |b|_5 \, .$$

Die Eigenschaften von $|a|_5$ sind also sehr ähnlich denen vom gewöhnlichen Betrag $|a|$ von a und wir können damit nach gewohntem Muster "Umgebungen" von a definieren: $\{x \in \mathbb{Q} : |x-a|_5 < \varepsilon\}$. Insbesondere können wir von Konvergenz von Folgen im Sinne von $| \ |_5$ reden und von Cauchyfolgen. Es ist nun leicht nachzuprüfen, daß

> Z_5 genau die Menge der Grenzwerte von $| \ |_5$-Cauchyfolgen aus $\mathbb{Z}$ und
> die von $| \ |_5$ auf $\mathbb{Z}_5$ induzierte Topologie die Topologie von $\mathbb{Z}_5 = \varprojlim_i \mathbb{Z}/5^i$ ist.

3. K sei ein Körper der Charakteristik Null (oder ein endlicher Körper) und I die Menge aller endlichen galoisschen Erweiterungen L/K in K^c mit $L_1 \leq L_2$, wenn L_1 Teilkörper von L_2 ist. Setze $M_L = G_{L/K}$ mit den kanonischen Restriktionen $\varphi_{L_2 L_1} : G_{L_2/K} \twoheadrightarrow G_{L_1/K}$. Der projektive Limes $G_K \overset{\text{def}}{=} \varprojlim_L G_{L/K}$ heißt die *absolute Galoisgruppe von* K; als Limes von endlichen Gruppen ist sie per definitionem eine *profinite (proendliche) Gruppe*.
   Es gilt $G_K = \mathrm{Aut}(K^c/K)$ als abstrakte Gruppen. Denn ist σ ein Automorphismus von K^c, der K elementweise festläßt, so induziert σ durch Einschränkung Automorphismen $\sigma_L \in G_{L/K}$, und das liefert einen Homomorphismus $\mathrm{Aut}(K^c/K) \to G_K$. Ist umgekehrt $\tau \in G_K$, $\tau = (\ldots, \tau_L, \ldots)$, so erkläre σ auf K^c durch $\sigma(\alpha) = \tau_L(\alpha)$, wenn $\alpha \in L$. Dies ist unabhängig von einer speziellen Wahl von L.

4. Ersetzt man oben K durch $\mathbb{Q}$ und K^c durch

$$\mathbb{Q}^{\text{ab}} \overset{\text{def}}{=} \mathbb{Q}(\zeta_n : n \in \mathbb{N}) \overset{*}{\subset} \text{Kompositum aller endlichen abelschen Erweiterungen } L \text{ von } \mathbb{Q} \, ,$$

   so erhält man $G_{\mathbb{Q}^{\text{ab}}/\mathbb{Q}} = \varprojlim_L G_{L/\mathbb{Q}} = (\hat{\mathbb{Z}})^\times$, die Einheitengruppe des Ringes $\hat{\mathbb{Z}}$ [1]. Und ist K endlich, so ist $G_K = \hat{\mathbb{Z}}$ (mit *mal* links und *plus* rechts).

Bemerkung: Wenn es inseparable irreduzible Polynome in $K[x]$ gibt, muß der algebraische Abschluß K^c durch den separablen Abschluß $K^{\text{sep}} \subset K^c$ ersetzt werden; K^{sep} bezeichnet das Kompositum aller endlichen separablen Erweiterungen von K in K^c.

Man beachte, daß G_K eine topologische Gruppe ist. Wir interessieren uns im folgenden nicht für abstrakte Untergruppen von G_K, sondern nur für die in der Topologie von G_K abgeschlossenen darunter. Deswegen nämlich:

[1] $\overset{*}{\subset}$ ist tatsächlich eine Gleichheit (Satz von Kronecker-Weber)

Betrachte $\mathrm{Aut}(\mathbb{F}_2^c/\mathbb{F}_2)$. Darin sehen wir den Frobeniusautomorphismus φ mit $\varphi(\alpha) = \alpha^2$. Die von φ erzeugte Untergruppe in $\mathrm{Aut}(\mathbb{F}_2^c/\mathbb{F}_2)$ ist die unendliche zyklische Gruppe $\langle\varphi\rangle = \{\varphi^i : i \in \mathbb{Z}\} \simeq \mathbb{Z}$. Welches ist ihr Fixkörper?

$$\varphi^i(\alpha) = \alpha \ (\forall\, i) \iff \varphi(\alpha) = \alpha \iff \alpha^2 = \alpha\,,$$

also $\mathbb{F}_2$. Aber, im Gegensatz zur endlichen Galoistheorie, ist dennoch $\langle\varphi\rangle$ eine echte Untergruppe von $\mathrm{Aut}(\mathbb{F}_2^c/\mathbb{F}_2)$, wie wir nun zeigen.

Für $n \in \mathbb{N}$ sei n' der größte ungerade Teiler von n, $\frac{n}{n'} = 2^\nu$ und n'' eine Lösung der Kongruenz $n'n'' \equiv 1 \mod 2^\nu$. Für $m|n$ verifiziert man sofort

$$(*) \qquad m'm'' \equiv n'n'' \mod m\,.$$

Setze nun

$$\phi_n = (\varphi_{\mathbb{F}_{2^n}/\mathbb{F}_2})^{n'n''}$$

mit dem Frobeniusautomorphismus $\varphi_{\mathbb{F}_{2^n}/\mathbb{F}_2}$ von $\mathbb{F}_{2^n}/\mathbb{F}_2$, also der Einschränkung von φ auf $\mathbb{F}_{2^n}$. Für $m|n$, also $\mathbb{F}_{2^m} \subset \mathbb{F}_{2^n}$, folgt aus $(*)$

$$\phi_{n|\mathbb{F}_{2^m}} = \phi_m \quad \text{wegen} \quad \varphi^m_{\mathbb{F}_{2^m}/\mathbb{F}_2} = 1\;.$$

Wir erhalten damit durch Zusammensetzen der ϕ_n einen Automorphismus $\phi \in \mathrm{Aut}(\mathbb{F}_2^c/\mathbb{F}_2)$, der gewiß nicht in $\langle\varphi\rangle$ liegt: wäre $\phi = \varphi^i$, so wäre $\phi_n = (\varphi_{\mathbb{F}_{2^n}/\mathbb{F}_2})^{n'n''} = (\varphi_{|\mathbb{F}_{2^n}})^i$, also $i \equiv n'n'' \mod n$ und folglich $i \equiv 1 \mod 2^\nu$ für alle ν, was unmöglich ist.

Lemma. *$G = \varprojlim_i G_i$ sei eine proendliche Gruppe.*

1. *Mit $H_i = \bigcap_{j\geq i} \mathrm{im}\,\varphi_{ji}$ gilt $\varphi_{ji} : H_j \twoheadrightarrow H_i$, $G = \varprojlim_i H_i$, $\varphi_i : G \twoheadrightarrow H_i$.*
2. *Ist U eine offene Untergruppe von G, so ist $[G:U] < \infty$ und U abgeschlossen; ist $U \leq G$ abgeschlossen und von endlichem Index in G, so ist U offen.*
3. *Der Durchschnitt aller offenen normalen Untergruppen von G ist $= 1$.*
4. *$G = \varprojlim_{U \text{ offen}} G/U$ [2] (die gerichtete Menge I zu dem projektiven Limes rechts ist die Menge aller offenen normalen Untergruppen U von G mit $[U_1 \leq U_2 \overset{df}{\iff} U_1 \supset U_2]$).*
5. *Ist H eine abgeschlossene Untergruppe von G, so ist H proendlich, nämlich $H = \varprojlim_{U \lhd G \text{ offen}} H/H\cap U$.*

   Ist H ein abgeschlossener Normalteiler in G, so ist G/H proendlich und $G/H = \varprojlim_{U \lhd G \text{ offen}} G/UH$.

1. kann noch zu *der projektive Limes nichtleerer kompakter Mengen ist nichtleer* verschärft werden. 2. ist eine direkte Konsequenz aus der Kompaktheit von G. Für den Beweis von 3. starte mit den offenen normalen Untergruppen $\{1\} \times \prod_{i\neq i_0} G_i$ von $\prod_i G_i$, wobei i_0 die Menge I durchlaufe. Mit Bezug auf 4. sind drei Bemerkungen hilfreich:

[2] die Gleichheit meint einen kanonischen Homöomorphismus

i) In einem kompakten Raum sind die Begriffe *abgeschlossen* und *kompakt* gleich. Stetige Abbildungen $\varphi : T_1 \to T_2$ zwischen hausdorffschen Räumen T_1, T_2 erfüllen $[\,T_1$ kompakt $\Longrightarrow \varphi(T_1)$ kompakt$\,]$. Ist φ stetig und bijektiv und sind T_1, T_2 beide kompakt, so ist φ offen, d.h. $\varphi(O_1)$ ist offen in T_2 für offene O_1 in T_1.

ii) G sei eine topologische Gruppe, also eine Gruppe, die zugleich ein topologischer Raum ist und so, daß $(a,b) \mapsto ab : G \times G \to G$ und $a \mapsto a^{-1} : G \to G$ stetige Abbildungen sind. Ist N ein Normalteiler von G, so mache G/N zu einer topologischen Gruppe über die Definition

$$\{O \mod N\} \text{ mit } O \text{ offen in } G \text{ sei eine Subbasis der Topologie von } G/N\,.$$

Dann ist die kanonische Restklassenabbildung $G \xrightarrow{\varphi} G/N$ offen und stetig – letzteres wegen $\varphi^{-1}(O \mod N) = O \cdot N = \bigcup_{n \in N} On$.

iii) Ist N ein abgeschlossener Normalteiler der topologischen Gruppe G, so ist G/N hausdorffsch.

Hauptsatz der Galoistheorie *Die Zwischenkörper $K^{\mathrm{sep}} \supset L \supset K$ entsprechen eineindeutig und inklusionsumkehrend den abgeschlossenen Untergruppen H von G_K :*

zu H gehört der Fixkörper von H in K^{sep} ; zu L gehört $G_L \leq G_K$. Die endlichen Erweiterungen L/K korrespondieren mit den offenen Untergruppen H und $[L : K] = [G_K : H]$. Den abgeschlossenen Normalteilern $H \lhd G_K$ entsprechen die über K galoisschen Erweiterungen L (das sind die $K \subset L \subset K^{\mathrm{sep}}$ mit $\sigma(L) \subset L$ [3] für alle K-Isomorphismen $\sigma : L \to K^{\mathrm{c}}$) und es gilt $G_K/H \simeq G_{L/K} \stackrel{\mathrm{def}}{=} \varprojlim_M G_{M/K}$ (mit $K \subset M \subset L$, M/K endlich galoissch).
Der Hauptsatz bleibt richtig bei Ersetzung von (K^{sep}, G_K) durch $(L, G_{L/K})$ für eine galoissche Erweiterung L von K.

Anhang: Skizze eines Beweises vom Satz von Tychonov

Der Beweis beruht auf dem Begriff eines *Filters* auf einem topologischen Raum $T \neq \emptyset$; in diesem sind grundlegende topologische Eigenschaften von T kodiert.

Definition. *Ein Filter $\mathfrak{F}$ auf T ist eine nichtleere Teilmenge der Potenzmenge $\mathfrak{P}(T)$ mit*

1. $F \in \mathfrak{F}\,,\ F \subset F_1 \subset T \implies F_1 \in \mathfrak{F}$
2. $F_1, F_2 \in \mathfrak{F} \implies F_1 \cap F_2 \in \mathfrak{F}$
3. $\emptyset \notin \mathfrak{F}$

Ein Beispiel ist der sogenannte Umgebungsfilter $\mathfrak{F}_t$ eines Punktes $t \in T$: der besteht aus allen Umgebungen von t, also aus allen Teilmengen von T, die ein offenes $O \subset T$ mit $t \in O$ enthalten. Ein zweites Beispiel entsteht aus einem nichtleeren $\mathfrak{B} \subset \mathfrak{P}(T)$ mit

$$F_1, F_2 \in \mathfrak{B} \implies \exists\, F \in \mathfrak{B}\,,\ F \subset F_1 \cap F_2\,,$$

[3] wegen $L = \cup M$ gilt $[\,\sigma(L) \subset L \iff \sigma(L) = L\,]$

indem man $\mathfrak{F}_{\mathfrak{B}}$ als den Filter definiert, der aus den sämtlichen Obermengen der Mengen aus $\mathfrak{B}$ besteht.

Wir nennen den Filter $\mathfrak{F}_1$ feiner als $\mathfrak{F}$, in Zeichen $\mathfrak{F}_1 \geq \mathfrak{F}$, wenn jedes $F \in \mathfrak{F}$ zu $\mathfrak{F}_1$ gehört.

LEMMA 1. *Die Menge $\mathcal{F}_T$ aller Filter auf T ist bezüglich "$\geq$" zornsch, d.h. es gibt maximale Elemente in $\mathcal{F}_T$. Jedes solche heißt ein Ultrafilter (auf T).*

LEMMA 2. *Für ein $\emptyset \neq B \subset T$ und einen Filter $\mathfrak{F}$ auf T gilt*

$$\exists \, \text{Filter } \mathfrak{F}_1 \geq \mathfrak{F} \text{ mit } B \in \mathfrak{F}_1 \iff \complement B \notin \mathfrak{F} \, .$$

Als unmittelbare Folgerung notieren wir

$$\mathfrak{F} \text{ ist Ultrafilter} \iff [\, B \subset T \implies B \in \mathfrak{F} \text{ oder } \complement B \in \mathfrak{F} \,] \, .$$

DEFINITION. *1. $\mathfrak{F}$ konvergiere gegen $t \in T$, in Zeichen $\mathfrak{F} \to t$, wenn $\mathfrak{F} \geq \mathfrak{F}_t$ gilt.*

2. $t \in T$ heiße ein Häufungspunkt von $\mathfrak{F}$ $\iff$ $x \in A$ für alle abgeschlossenen Mengen $A \in \mathfrak{F}$.

Erinnerung: $t \in T$ heißt ein Häufungspunkt von $X \subset T$, wenn jede Umgebung von t ein $x \neq t$ aus X enthält. Der Abschluß $\overline{X}$ von X in T besteht aus X und allen Häufungspunkten von X.

LEMMA 4. *$t \in T$ ist ein Häufungspunkt des Filters $\mathfrak{F}$ $\iff$ $\exists \, \mathfrak{F}_1 \geq \mathfrak{F}$ mit $\mathfrak{F}_1 \to t$.*

Bemerkung: Gilt $\mathfrak{F} \to t$, so ist also t ein Häufungspunkt von $\mathfrak{F}$; er ist der einzige, falls T hausdorffsch ist.

LEMMA 5. *Gleichbedeutend sind*

i) T ist kompakt, ii) jeder Filter auf T besitzt einen Häufungspunkt, iii) jeder Ultrafilter auf T konvergiert gegen ein $t \in T$.

Nun sei $f : T \to T'$ eine Abbildung zwischen topologischen nichtleeren Räumen. Ist $\mathfrak{F}$ ein Filter auf T, so induziert $\mathfrak{B}' = \{f(F) : F \in \mathfrak{F}\} \subset \mathfrak{P}(T')$ den Filter

$$f(\mathfrak{F}) = \mathfrak{F}' \stackrel{\text{def}}{=} \mathfrak{F}_{\mathfrak{B}'} \, .$$

Umgekehrt, ist $\mathfrak{F}'$ ein Filter auf T', so betrachte $\mathfrak{B} \stackrel{\text{def}}{=} \{f^{-1}(F') : F' \in \mathfrak{F}'\} \subset \mathfrak{P}(t)$. Es kann $f^{-1}(F') = \emptyset$ passieren – allerdings nicht, wenn f surjektiv ist. Falls $\emptyset \notin \mathfrak{B}$, setze $f^{-1}(\mathfrak{F}') = \mathfrak{F}_{\mathfrak{B}}$.

LEMMA 6. *$f : T \to T'$ ist stetig im Punkte $t \in T$ $\iff$ $f(\mathfrak{F}_t) \to f(t)$.*

LEMMA 7. *T_i, für i aus einer Indexmenge I, seien topologische nichtleere Räume, $T = \prod_I T_i$ der Produktraum und $\pi_i : T \to T_i$ die Projektion von T auf T_i. Dann gilt*

$$\text{der Filter } \mathfrak{F} \text{ auf } T \text{ konvergiert gegen } t \iff \pi_i(\mathfrak{F}) \to \pi_i(t) \ (\forall \, i \in I) \, .$$

Der Satz von Tychonov folgt nun ohne weiteres aus den Lemmas 5 und 7.

Ein paar abschließende Bemerkungen zu proendlichen Gruppen G.

1. Die topologische Gruppe G ist geau dann proendlich, wenn

   a) G kompakt ist,

   b) jede offene Umgebung der 1 eine offene normale Untergruppe von G enthält,

   c) $\bigcap U = 1$ ist, wenn U die offenen Normalteiler von G durchläuft.

2. Abelsche Charaktere einer proendlichen Gruppe G sind per definitionem stetige Homomorphismen $\chi : G \to S^1 \overset{\text{def}}{=} \{z \in \mathbb{C} : |z| = 1\}$. Damit ist $H = \chi^{-1}(1)$ eine abgeschlossene Untergruppe in G, weshalb mit G auch G/H proendlich und insbesondere kompakt ist und χ folglich einen Homöomorphismus $G/H \simeq \mathrm{im}(\chi)$ induziert. Das Urbild der ε-Umgebung $U_\varepsilon(1) = \{z \in S^1 : |z-1| < \varepsilon\}$ der 1 in S^1 ist eine offene Umgebung der 1 in G/H und enthält daher einen offenen Normalteiler von G/H. Dessen χ-Bild wiederum ist eine Untergruppe der S^1 und kann also nur in $U_\varepsilon(1)$ liegen, wenn es $= 1$ ist ("Multiplikation in $S^1 \leftrightarrow$ Addition der Winkel"). Somit ist gezeigt, daß H selbst offen ist.

   Anwendung: Für einen Körper K mit $\mathrm{char}(K) \nmid n$ und $\zeta_n \in K$ sei $K^{\mathrm{ab},n}$ die maximal abelsche Erweiterung von K vom Exponenten $\mid n$, d.h. $K^{\mathrm{ab},n}$ ist das Kompositum aller endlichen abelschen Erweiterungen L/K mit $\exp(G_{L/K}) \mid n$. Die Kummertheorie zeigt $\mathrm{Hom}(G_{K^{\mathrm{ab},n}/K}, S^1) = K^\times/(K^\times)^n$.

   Beachte, daß in dieser i.Allg. unendlichen Galoisgruppe $G_{K^{\mathrm{ab},n}/K}$ alle Elemene endliche Ordnung haben (nämlich Teiler von n) – im Gegensatz zur absoluten Galoisgruppe G_K von K, deren Elemene σ endlicher Ordnung $\sigma^2 = 1$ erfüllen (vgl. den SATZ zwischen Satz 9 und 10).

   In dem Zusammenhang:

   i) Analog zu $K^{\mathrm{ab},n}$ man K^{ab}, $K^{(p)}$, K^{nilp}, K^{sol}, die maximal abelsche, p-, nilpotente, bzw. auflösbare Erweiterung eines Körpers K definieren. Z.B. ist dann $G_{K^{\mathrm{ab}}/K} = G_K/[G_K, G_K]$ mit dem topologischen Abschluß $[G_K, G_K]$ der von den Kommutatoren $\sigma\tau\sigma^{-1}\tau^{-1}$, $\sigma, \tau \in G_K$, erzeugten *Kommutatoruntergruppe* von G_K (man vergegenwärtige sich, daß der Abschluß einer Untergruppe einer topologischen Gruppe selbst wieder eine Untergruppe ist).

   ii) Es gibt keinen Körper $K \neq \mathbb{R}$ mit: $\mathbb{R}/K$ ist algebraisch und galoissch. Denn $\mathrm{Aut}(\mathbb{R}) = 1$, wie die folgende Schlußkette zeigt

   $$\sigma \in \mathrm{Aut}(\mathbb{R}) \implies \sigma(1) = 1 \implies \sigma(n) = n \text{ für } n \in \mathbb{N} \implies \sigma(z) = z \text{ für } z \in \mathbb{Z} \implies \sigma(q) = q \text{ für } q \in \mathbb{Q} \overset{*}{\implies} \sigma(x) = x \text{ für } x \in \mathbb{R}$$

   mit $*$ wegen

   $$\begin{aligned} &x \geq 0 \iff x = y^2 \implies \sigma(x) = \sigma(y)^2 \implies \sigma(x) \geq 0 \\ &x = \inf\{q \in \mathbb{Q} : x \leq q\}\,. \end{aligned}$$

3. Der Index einer abgeschlossenen Untergruppe H von G:

   Um den zu erklären, braucht man den Begriff der *übernatürlichen* Zahlen. Dies sind per definitionem die Produkte $\prod_p p^{n_p}$ über alle Primzahlen p mit Exponenten $n_p \in \mathbb{N} \cup 0 \cup \infty$.

Man definiert weiter

$$\mathrm{kgV}(\prod_p p^{n_p}, \prod_p p^{m_p}) = \prod_p p^{\max(n_p, m_p)}\,.$$

Nun setze $[G:H] = \mathrm{kgV}([G/U : H/(H\cap U)]$, wobei U durch die Menge der offenen Untergruppen von G laufe. Offenbar gilt dann $[G:H] = \mathrm{kgV}(\,[G:U] : G \supset U \supset H\,)$, U natürlich wieder offen. Des weiteren: $[G:H] = [G:K]\cdot[K:H]$ für $H \leq K \leq G$ und H, K abgeschlossen in G.

4. p sei nun eine feste Primzahl. Die proendliche Gruppe G heiße eine pro-p Gruppe, sofern $|G| = [G:1] = p^n$ mit $n \in \mathbb{N} \cup 0 \cup \infty$. Gleichbedeutend ist $G = \varprojlim_i G_i$ mit endlichen p-Gruppen G_i. Jede abgeschlossene Untergruppe einer pro-p Gruppe ist pro-p, jede Faktorgruppe G/H einer pro-p Gruppe nach einem abgeschlossenen Normalteiler ist pro-p.

   Eine abgeschlossene Untergruppe S einer proendlichen Gruppe G heißt eine Sylow p-Untergruppe von G, wenn S eine pro-p Gruppe und $[G:S]$ prim zu p ist. Solche existieren stets und zwei davon sind in G konjugiert.

   Beispiel: $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$

Man erkennt wohl, daß vieles für proendliche Gruppen parallel zu dem für endliche Gruppen gemacht werden kann, und es braucht auch nicht mehr expressis verbis gesagt zu werden, was mit proabelsch, proauflösbar, etc. gemeint sein könnte.