universität
wien

Bachelorarbeit

Hauptsatz der Galoistheorie für unendliche Galoiserweiterungen

Noah Foeteler

betreut von
Univ. Prof. Dr. D. Burde

Wien, 2022

Studienkennzahl lt. Studienblatt :	UA 033 621
Studienrichtung lt. Studienblatt :	Bachelorstudium Mathematik

Abstract

Der sogenannte Hauptsatz der Galoistheorie ist ein zentraler Satz der Galoistheorie. Üblicherweise wird dieser nur für endliche Galoiserweiterungen formuliert. Jedoch bemerkte Dedeking bereits 1902, dass dieser Satz ungültig war für unendliche Erweiterungen. 1928 löste Krull das Problem anhand von Topologie. Die vorliegende Arbeit beschreibt zunächst den Hauptsatz in seiner üblichen Form für endliche Erweiterungen, um anschließend auch die Verallgemeinerung für unendliche Erweiterungen vorzustellen.

Inhaltsverzeichnis

Kapitel 1

Endliche Galoiserweiterungen

Im folgenden sind die Definitionen und Sätze, falls nicht zitiert, dem Skriptum "Algebra" von Prof. Dr. D. Burde entnommen (siehe [**BU62**]).

Um den Hauptsatz der Galoistheorie zunächst für endliche Körpererweiterungen zu beschreiben, braucht es offensichtlich ein Verständis an Galoistheorie. Folgende Definitionen erklären wichtige Konzepte der Algebra.

1.1 Körper

Definition 1.1.1. Eine Menge K von Elementen zusammen mit zwei binären Verknüpfungen (üblicherweise durch "+" und "$\cdot$" dargestellt) wird Körper gennant wenn folgende Eigenschaften erfüllt sind:

1. K zusammen mit "+" ist eine abelsche Gruppe.
2. K*($=K\backslash\{0\}$) zusammen mit "$\cdot$" ist eine abelsche Gruppe.
3. Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in K$

1.1.1 Körpererweiterung

Definition 1.1.2. Sei L ein Körper. Ein Teilkörper K von L ist ein Unterring von L, so dass K mit jedem Element ungleich Null auch sein multiplikatives Inverses enthält. Dann ist $K \subseteq L$ selbst ein Körper bezüglich Addition und Multiplikation von L. Man nennt L eine Körpererweiterung von K und schreibt $L \mid K$. Ein Zwischenkörper der Erweiterung $L \mid K$ ist ein Teilkörper M von L mit $K \subseteq M \subseteq L$.

Definition 1.1.3. Eine Erweiterung $L \mid K$ heißt endlich erzeugt, falls es Elemente $\alpha_1, ..., \alpha_n \in L$ gibt mit $L = K(\alpha_1, ..., \alpha_n)$. Sie heißt einfach, wenn es ein $\alpha \in L$ gibt mit $L = K(\alpha)$. Ein solches α, welches nicht eindeutig sein muss, heißt primitives Element. Der Grad einer Erweiterung $L \mid K$ ist definiert als $[L : K] := dim_K(L)$. Die Erweiterung heißt endlich, falls $[L : K] < \infty$ gilt.

Definition 1.1.4. Seien M, N zwei Zwischenkörper in einer Körpererweiterung $L \mid K$. Dann bezeichnet $MN = K(M \cup N)$ das Kompositum von M und N in $L \mid K$.

1.2 Endliche Galoistheorie

1.2.1 Galoiserweiterungen und Fixkörper

Definition 1.2.1. Sei L — K eine Körpererweiterung und $\alpha \in L$. Das Element α heißt *algebraisch über K*, wenn es ein Polynom $f \in K[X]$ gibt, mit $f \neq 0$ und $f(\alpha) = 0$. Andernfalls heißt es *transzendent über K*.

Definition 1.2.2. Sei K ein Körper und $M \mid K$ ein algebraischer Abschluss von K. Ein Polynom $f \in K[X]$ ungleich 0 heißt *separabel* über K, wenn es über M in paarweise verschiedene Linearfaktoren zerfällt, also keine mehrfachen Nullstellen in M besitzt.

Definition 1.2.3. Eine algebraische Körpererweiterung $L \mid K$ heißt *normal*, wenn für jedes $\alpha \in L$ das Minimalpolynom $\mu_\alpha \in K[X]$ von α über K in L in Linearfaktoren zerfällt.

Definition 1.2.4. Ein Gruppenhomomorphismus $\phi : G \to G$ heißt Endomorphismus. Ist er bijektiv, so heißt er Automorphismus. Die Automorphismen einer Gruppe G bilden eine Gruppe unter Komposition, die mit $Aut(G)$ bezeichnet wird.

Definition 1.2.5. Sei $L \mid K$ eine Körpererweiterung. Die Automorphismengruppe $Aut(L \mid K)$ von $L \mid K$ (in der Kategorie der Körpererweiterungen über K) ist durch die Gruppe aller Körperisomorphismen $f : L \to L$ gegeben mit $f|_K = id_K$.

Definition 1.2.6. Eine Galoiserweiterung $L \mid K$ ist eine algebraische Körpererweiterung, die normal und separabel ist. In diesem Fall bezeichnen wir
$Gal(L, K) := Aut(L \mid K)$ als die Galoisgruppe der Erweiterung $L \mid K$.

Definition 1.2.7. Sei $L \mid K$ eine Körpererweiterung und G eine Untergruppe von $Aut(L \mid K)$. Dann ist

$$L^G = \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in G\}$$

ein Zwischenkörper von $L \mid K$. Er heißt *Fixkörper* von G.

Satz 1. *Sei $L \mid K$ eine Körpererweiterung und G eine endliche Untergruppe von $Aut(L \mid K)$. Dann ist $L \mid L^G$ eine Galoiserweiterung mit*

$$[L : L^G] = |G|,$$
$$Gal(L, L^G) = G$$

Satz 2. *Sei $L \mid K$ eine Galoiserweiterung, dann gilt für jedes $\alpha \in L$, dass die Nullstellen des Minimalpolynoms über K Elemente von $\{\sigma(\alpha) : \sigma \in Gal(L, K)\}$ sind.*

1.2.2 Hauptsatz der Galoistheorie

Die Menge aller Untergruppen einer Gruppe G wird im folgenden mit U(G) bezeichnet. Die Menge aller Zwischenkörper einer Körpererweiterung $L \mid K$ wird im folgenden mit $Z(L, K)$ oder $Z(L \mid K)$ bezeichnet.

Theorem 1. *Es sei $L \mid K$ eine endliche Galoiserweiterung und $G = Gal(L, K)$. Dann sind die Abbildungen*

$$Z(L, K) \to U(G),\ M \mapsto Gal(L, M)$$
$$U(G) \to Z(L \mid K), H \mapsto L^H$$

zueinander inverse Bijektionen. Sei M ein Zwischenkörper von $L \mid K$. Dann ist die Körpererweiterung $M \mid K$ genau dann normal, wenn $Gal(L, M)$ ein Normalteiler in $Gal(L, K)$ ist. In diesem Fall ist

$$Gal(L, K)/Gal(L, M) \to Gal(M, K),\ [\sigma] \mapsto \sigma|_M$$

ein Gruppenisomorphismus.

Beweis. Sei $H \subseteq G$ eine Untergruppe. Da G endlich, ist auch H endlich. Dann ist L^H ein Zwischenkörper von $L \mid K$ und Satz 1 liefert $Gal(L, L^H) = H$. Sei umgekehrt M ein Zwischenkörper von $L \mid K$. Dann ist $L \mid M$ eine endliche Galoiserweiterung und wir wissen, dass $M = L^{Gal(L,M)}$ gilt. Für die zweite Aussage, sei $M \mid K$ normal. Dann ist die Abbildung

$$\pi : Gal(L, K) \to Gal(M, K),\ \sigma \mapsto \sigma|_M$$

nach dem Konjugationsprinzip ein wohldefinierter Gruppenhomomorphismus mit $im(\pi) = Gal(M, K)$. Sein Kern ist

$$ker(\pi) = \{\sigma \in Gal(L,K) : \sigma|_M = id_M\} = Gal(L,M).$$

Also ist $Gal(L,M)$ ein Normalteiler in $Gal(L,K)$ und die Behauptung folgt aus dem Homomorphiesatz. Sei umgekehrt H ein Normalteiler in $Gal(L,K)$ und $\alpha \in M$. Wir müssen zeigen, dass $M \mid K$ normal ist. Da $L \mid K$ eine normale Körpererweiterung ist, zerfällt $\mu_{\alpha,K}$ über L in Linearfaktoren und es genügt zu zeigen, dass jede Nullstelle von $\mu_{\alpha,K}$ in L bereits in M liegt. Sei also $\beta \in L$ eine Nullstelle von $\mu_{\alpha,K}$. Durch mehrfache Anwendung des Konjugationsprinzips erhalten wir einen Körperisomorphismus $\sigma \in Gal(L,K)$ mit $\sigma(\alpha) = \beta$. Da H ein Normalteiler in $Gal(L,K)$ ist, gilt $H = \sigma H \sigma^{-1}$. Wegen $(\sigma \circ \tau \circ \sigma^{-1})(\beta) = (\sigma \circ \tau)(\alpha) = \sigma(\alpha) = \beta$ für alle $\tau \in H \subseteq Gal(L, L^H)$, gilt $\beta \in L^{\sigma H \sigma^{-1}} = L^H$. Nach dem ersten Teil ist also $\beta \in L^H = M$. □

Beispiel 1.2.1. Sei $f(x) = x^4 - 2$. Um die zugehörige Galoiserweiterung zu finden, findet man zunächst die vier Wurzeln $x \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. Die Galoiserweiterung ist also zum Beispiel $\mathbb{Q}(\sqrt[4]{2}, i) \mid \mathbb{Q}$. Der Grad der Erweiterung ist 8, weil das Minimalpolynom von $\sqrt[4]{2}$ Grad 4 hat und das Minimalpolynom von i Grad 2 hat. Nach der Gradregel gilt $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 4 \cdot 2 = 8$. Also $|Gal(L,K)| = 8$ mit $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[4]{2}, i)$. Da $Gal(L,K) \leq S_4$ gelten muss und S_4 drei Untergruppen der Ordnung 8 hat, muss $Gal(L,K)$ eine von den folgenden drei Gruppen sein: $\langle(1234),(13)\rangle$, $\langle(1243),(14)\rangle$ oder $\langle(1324),(12)\rangle$. Da diese drei Gruppen jedoch isomorph zu D_4 sind gilt: $Gal(L,K) = D_4 = \{1, \phi, \phi^2, \phi^3, \psi, \phi\psi, \phi^2\psi, \phi^3\psi\}$ mit Relationen $\phi^4 = 1, \psi^2 = 1, \phi\psi = \psi\phi^3$. (Hierbei entspricht ϕ einer Multiplikation von $\sqrt[4]{2}$ mit i und ψ entspricht einer Vertauschung von i und $-i$). Dies ist die Diedergruppe, welche eine nicht-zyklische Gruppe ist.

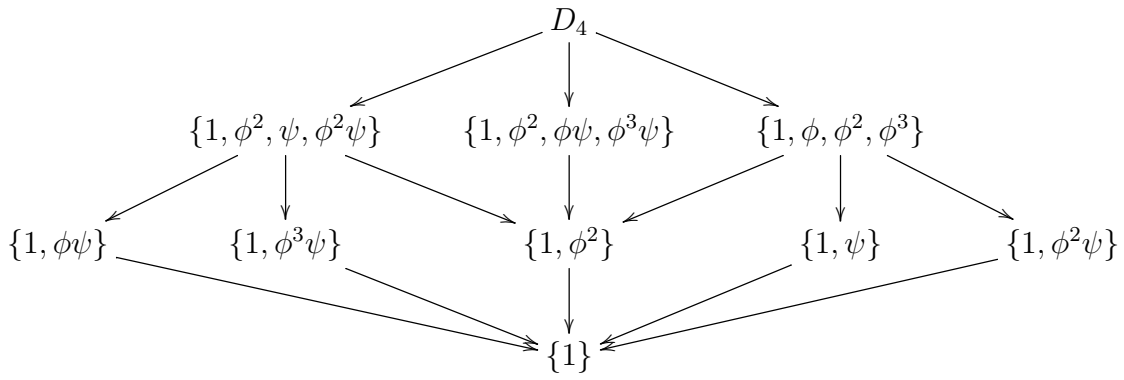
Nun wollen wir uns mit den Untergruppen von D_4 befassen. Dazu braucht man folgenden Satz:

Satz 3. *[**CO**] Jede Untergruppe von D_n ist entweder zyklisch oder selbst eine Diedergruppe. Eine komplette Auflistung der Untergruppen ist wie folgt:*

1. *$\langle r^d \rangle$ wobei $d \mid n$ mit Index $2d$, (zyklische Gruppe)*
2. *$\langle r^d, r^i s \rangle$ wobei $d \mid n$ und $0 \leq d \leq i-1$ mit Index d (Diedergrppe).*

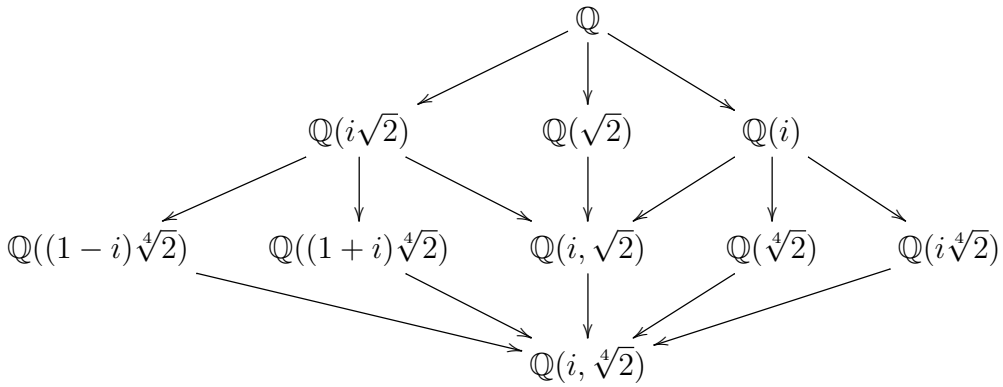
Wie findet man nun die Untergruppen von D_4? Zunächst weiss man, dass D_4 nur Untergruppen der Ordnung 1,2,4 und 8 besitzt. Die Gruppen der Ordnung 1 und 8 sind trivial. Die Untergruppen der Ordnung 2 müssen folgende Form haben: $\{1, x\}$ wobei x ein Element der Ordnung 2 ist. Die Elemente der Ordnung 2 sind: $\phi\psi, \phi^3\psi, \phi^2, \psi, \phi^2\psi$. Somit haben wir alle Untergruppen der Ordnung 2 gefunden. Zu den Untergruppen der Ordnung 4: Falls ϕ in zu einer Untergruppe gehört, so

muss auch ϕ^2 und ϕ^3 dazugehören, also hat man die Untergruppe $\{1, \phi, \phi^2, \phi^3\}$. Falls nun ϕ nicht in der Untergruppe ist, so ist auch das inverse Element $\phi^{-1} = \phi^3$ nicht in der Untergruppe. Falls ψ in der Untergruppe ist, dürfen $\phi\psi$ und $\phi^3\psi$ nicht drin sein, denn sonst wäre auch ϕ drin, und das haben wir ausgeschlossen. Das lässt uns nur noch mit den Möglichkeiten $\{1, \phi^2, \psi, \phi^2\psi\}$ und $\{1, \phi^2, \phi\psi, \phi^3\psi\}$.
Nun können wir alle Untergruppen von D_4 in ein Hasse-Diagramm eintragen:



Beachte, dass $\{1, \phi, \phi^2, \phi^3\} \cong \mathbb{Z}_4$, $\{1, \phi^2, \psi, \phi^2\psi\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ und auch $\{1, \phi^2, \phi\psi, \phi^3\psi\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Ausserdem sind alle im Diagramm enthaltene zweielementigen Mengen isomorph zu $\mathbb{Z}_2$. Beachte hierbei wiederum, dass die kleinsche Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorph zu der Diedergruppe D_2 ist. Da $\mathbb{Z}_2$ und $\mathbb{Z}_4$ beide zyklisch sind entspricht das Resultat der Aussage von Satz 3.

Zu jeder Untergruppe ist es nun leicht, einen Fixkörper zu finden. Hierbei kann man die Automorphismen auf alle Nullstellen wirken lassen. Die Fixkörper sind dann $\mathbb{Q}$, adjungiert mit jenen Elementen, die festgelassen werden. Zum Beispiel: L^{H_1} mit $L = \mathbb{Q}(\sqrt[4]{2}, i)$ und $H_1 = \{1, \phi^2\}$. ϕ^2 entspricht der Multiplikation von $\sqrt[4]{2}$ mit -1. Abgesehen von i ist das einzige Element, welches festgelassen wird $\sqrt{2}$, weil $\phi^2(\sqrt{2}) = \phi^2((\sqrt[4]{2})^2) = (-\sqrt[4]{2})^2 = \sqrt{2}$. Der zugehörige Fixkörper ist also $\mathbb{Q}(\sqrt{2}, i)$. Die restlichen Fixkörper kann man auf ähnliche Weise finden und auch in ein Hasse-Diagramm eintragen:



Beachte hierbei, dass $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(i\sqrt[4]{2})$ und $\mathbb{Q}((1+i)\sqrt[4]{2}) \cong \mathbb{Q}((1-i)\sqrt[4]{2})$.

Kapitel 2

Unendliche Galoistheorie

Für unendlich-dimensionale Körpererweiterungen muss der Begriff *Galoissch* neu definiert werden, dazu folgender Satz:

Satz 4. *[**CO2**] Für eine algebraische Körpererweiterung $L \mid K$ sind die folgenden Eigenschaften äquivalent:*

1. *$L = \bigcup_i L_i$ mit $L_i \mid K$ endliche Galoiserweiterung für jedes i.*
2. *L ist der Zerfällungskörper über K von einer Menge von separablen Polynomen in $K[X]$.*
3. *$L^{Aut(L|K)} = K$.*
4. *$L \mid K$ ist separabel und normal.*

Eine Erweiterung die diese Eigenschaften erfüllt wird Galoissch genannt.

Satz 5. *Falls $L \mid K$ eine unendliche Galoiserweiterung ist, dann ist $Gal(L, K)$ eine unendliche Gruppe.*

Der Hauptsatz der Galoistheorie gilt nur für endliche Galoiserweiterungen und versagt bei unendlichen Galoiserweiterungen, wie im folgenden Beispiel:

Beispiel 2.0.1. Sei $K = \mathbb{F}_p$ und $\mathbb{F} := \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Sei $L = \mathbb{F}$. Die Erweiterung $\mathbb{F} \mid \mathbb{F}_p$ ist Galoissch mit Galoisgruppe $G = Gal(L, K)$. Sei H die Untergruppe von G, die von dem Frobeniusautomorphismus $\phi : \alpha \to \alpha^p$ erzeugt wird.

Satz 6. *Es gilt $L^H = L^G = K$ mit $H \neq G$. Also gibt es zwei verschiedene Untergruppen von G mit dem gleichen Fixkörper, d.h., der Hauptsatz gilt nicht für die Galoiserweiterung $\mathbb{F} \mid \mathbb{F}_p$.*

Beweis. Offensichtlich gilt $L^G = K$, mit $L = \mathbb{F}$ und $K = \mathbb{F}_p$. Sei $x \in L^H$. Dann ist $\phi(x) = x$, also ist x eine Nullstelle von $X^p - X \in K[X]$. Alle Elemente von K sind Nullstellen dieses Polynoms. Da K ein Körper ist, kann es nicht mehr als p Nullstellen geben. Also ist $x \in K$ und es gilt $L^H = K$. Nun wollen wir zeigen, dass H eine echte Untergruppe von G ist. Dazu genügt es, ein $\tau \in Gal(L, K)$ zu konstruieren, dass keine Potenz von ϕ ist. Das erreichen wir mit der Konstruktion eines unendlichen Zwischenkörpers M mit $K \subset M \subset L$. Man wähle ein $\tau \in Gal(L, M)$ mit $\tau \neq id$. Das macht Sinn, weil auch $L \mid M$ Galoissch ist. Angenommen, es wäre $H = G$. Dann hätten wir $\tau = \phi^n$ für ein $n \geq 1$. Wir können τ durch τ^{-1} ersetzen, falls nötig. Dann stabilisiert ϕ^n den Körper M elementweise und M ist im Fixkörper von ϕ^n enthalten, d.h. $M \subset \mathbb{F}_{p^n}$. Das ist aber ein Widerspruch, da M unendlich ist. Also gilt $H \neq G$. Um den Beweis zu vollenden, müssen wir also einen solchen unendlichen Körper M finden. Eine mögliche Wahl ist durch $M := \bigcup_{n \geq 0} \mathbb{F}_{p^{2^n}}$ gegeben. Offensichtlich ist M unendlich und in L enthalten. Wir zeigen, dass $M \neq L$ gilt. Sei C eine kubische Körpererweiterung von $K = \mathbb{F}_p$, also mit $[C : \mathbb{F}_p] = 3$. Deshalb gibt es ein $\alpha \in L$ mit $C = \mathbb{F}_p(\alpha)$. Angenommen, es gilt $\alpha \in M$. Dann gilt $\alpha \in \mathbb{F}_{p^{2^n}}$ für ein n und

$$2^n = [\mathbb{F}_{p^{2^n}} : \mathbb{F}_p] = [\mathbb{F}_{p^{2^n}} : C] \cdot [C : \mathbb{F}_p].$$

das ist ein Widerspruch zu $3 \nmid 2^n$, und wir sind fertig. □

Das hier auftretende Problem ist, dass man zwar noch immer zu jedem Zwischenkörper einer unendlichen Erweiterung eine Untergruppe und zu jeder Untergruppe einen Zwischenkörper assoziieren kann, aber diese Korrespondenz ist im Allgemeinen keine Bijektion mehr.

2.1 Topologie

Um den Hauptsatz der Galoistheorie an unendliche Galoiserweiterungen anzupassen, muss man diesen ein wenig modifizieren. Dies geschieht mit Hilfe der sogenannten Krulltopologie.
Zur Erinnerung, zunächst folgende Definition:

Definition 2.1.1. Ein Raum X mit Teilmenge $\tau \subset \mathcal{P}(X)$ heißt ein *topologischer Raum*, falls folgende Eigenschaften gelten:

- $\varnothing, X \in \tau$
- beliebige Vereinigungen von Mengen aus τ gehören zu τ.
- endliche Durchschnitte von Mengen aus τ gehören zu τ .

2.1.1 Topologische Gruppen

Definition 2.1.2. Eine Menge G zusammen mit einer Gruppenstruktur und einer Topologie heißt *topologische Gruppe*, falls die Abbildungen

$$(g,h) \mapsto gh, G \times G \to G,$$
$$g \mapsto g^{-1}, G \to G$$

beide stetig sind. Hierbei ist $G \times G$ mit der Produkt-Topologie versehen.

Beispiel 2.1.1. Einige Beispiele für topologische Gruppen:

- Eine beliebige Gruppe G zusammen mit der diskreten Topologie ist eine topologische Gruppe.
- $(\mathbb{R}^n, +)$ zusammen mit der euklidischen Topologie ist eine topologische Gruppe.
- Die Menge aller reellen invertierbaren $n \times n$-Matrizen $GL(n, \mathbb{R})$ wird zu einer topologischen Gruppe wenn man die Menge als Untergruppe von $\mathbb{R}^{n^2}$ betrachtet und die Topologie übernimmt.
- Eine Galoisgruppe zusammen mit der Krulltopologie (siehe unten) ist eine topologische Gruppe.

2.1.2 Krulltopologie

Definition 2.1.3. [**CO2**] Sei $\sigma \in Gal(L, K)$ mit $[L : K]$ nicht notwendigerweise endlich. Eine offene Menge um σ ist eine Nebenklasse $\sigma Gal(L, F)$ mit $F \mid K$ endliche Körpererweiterung. Eine nichtleere Untermenge U von $Gal(L, K)$ ist offen, falls jedes Element von U in einer solchen Nebenklasse in U enthalten ist, also $\forall \sigma \in U, \sigma Gal(L, F) \subset U$ mit $F \mid K$ endliche Erweiterung.

Satz 7. *Die oben beschriebenen offenen Mengen, zusammen mit der leeren Menge, bilden eine Topologie auf* $Gal(L \mid K)$.

Beweis. Eine nichtleere offene Menge in $Gal(L, K)$ ist eine Vereinigung von Nebenklassen $\sigma_i Gal(L, F_i)$. Eine Vereinigung von offenen Mengen ist eine Vereinigung von einer Vereinigung von solchen Nebenklassen, welche wiederum eine Vereinigung von Nebenklassen ist. Daher ist eine Vereinigung von offenen Mengen auch offen. Seien $U_1, ..., U_n$ endlich viele offene Mengen. Wir wollen zeigen, dass $U_1 \cap \cdots \cap U_n =: U$ auch offen ist. Wir können annehmen, dass U nicht leer ist. Sei $\sigma \in U$. Da jedes U_i offen ist und σ enthält, gibt es endliche Erweiterungen $F_1, ..., F_n$ von K, sodass $\sigma Gal(L, F_i) \subset U_i$. Das Körperkompositum $F := F_1 \cdots F_n$ ist eine endliche Erweiterung von K, welches jedes F_i enthält. Also $Gal(L, F) \subset Gal(L, F_i)$ für $i \in \{1, ..., n\}$.

Daher ist $\sigma Gal(L,F) \subset U_i$ für $i \in \{1,...,n\}$. Also $\sigma Gal(L,F) \subset \bigcap_{i=1}^{n} U_i$. Wir haben gezeigt, dass jedes Element aus $\bigcap_{i=1}^{n} U_i$ in einer offenen Menge aus U enthalten ist, daher ist U offen. □

Die hier beschriebene Topologie wird *Krulltopologie* genannt.

Satz 8. *Sei $L \mid K$ Galoiserweiterung und E ein Zwischenkörper. Dann entspricht die Teilraumtopologie auf $Gal(L,E)$ als Untermenge von $Gal(L,K)$ genau der Krulltopologie auf $Gal(L,E)$.*

2.2 Unendliche Galoistheorie

2.2.1 Hauptsatz der Galoistheorie (allgemeiner Fall)

Sei im folgenden $U(G)$ die Menge aller abgeschlossenen Untergruppen einer Gruppe G und $Z(L \mid K)$ die Menge aller Zwischenkörper einer Erweiterung $L \mid K$.

Theorem 2. *Sei $L \mid K$ eine Galoiserweiterung mit Galoisgruppe $G = Gal(L,K)$, ausgestattet mit der Krulltopologie. Dann sind die Abbildungen*

$$Z(L,K) \to U(G), M \mapsto Gal(L,M)$$
$$U(G) \to Z(L \mid K), H \mapsto L^H$$

zueinander inverse Bijektionen. Es gelten folgende Aussagen.

1. *Die Korrespondenz ist inklusionsumkehrend, d.h., es gilt $H_1 \supset H_2 \iff L^{H_1} \subset L^{H_2}$.*
2. *Eine abgeschlossene Untergruppe H von G ist genau dann offen, wenn L^H endlichen Grad über K hat. Dann gilt $(G:H) = [L^H : K]$.*
3. *Die Untergruppe $\sigma H \sigma^{-1}$ korrespondiert zu dem Zwischenkörper $\sigma(M)$, d.h., es gilt $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$ und $Gal(L, \sigma(M)) = \sigma Gal(L \mid M)\sigma^{-1}$.*
4. *Eine abgeschlossene Untergruppe H von G ist genau dann Normalteiler in G, wenn $L^H \mid K$ Galoissch ist. Dann gilt $Gal(L^H, K) \cong G/H$.*

Beweis. Die Aussagen sind klar bis auf einige topologische Argumente. Für (2) beachte man, dass jede abgeschlossene Untergruppe von endlichem Index in einer topologischen Gruppe auch offen ist. Da G kompakt ist, ist umgekehrt auch jede offene Untergruppe von G immer von endlichem Index. Sei H eine solche Untergruppe von G. Dann induziert die Abbildung $\sigma \mapsto \sigma|_{L^H}$ eine Bijektion

$G/H \to Hom_K(L^H, L)$ und es folgt $(G : H) = [L^H : K]$. Zu (4) sei M in Korrespondez zu H. Aus (3) folgt, dass H genau dann Normalteiler ist, wenn M invariant unter der G-Aktion ist. Aber das gilt genau dann, wenn M eine Vereinigung von endlichen Erweiterungen von K ist, invariant unter G, d.h. eine Vereinigung von endlichen Galoiserweiterungen. Aber eine Erweiterung ist Galoissch genau dann, wenn sie eine Vereinigung von endlichen Galoiserweiterungen ist. □

Folgender Satz zeigt, wie man offene und abgeschlossene sowie normale Untergruppen charakterisieren kann.

Satz 9. *Sei $L \mid K$ Galoiserweiterung*

1. *Die abgeschlossenen Untergruppen von $Gal(L, K)$ sind $Gal(L, E)$ mit E Zwischenkörper von $L \mid K$.*

2. *Die offenen Untergruppen von $Gal(L, K)$ sind $Gal(L, F)$ mit $F \mid K$ endliche Erweiterung.*

3. *Die abgeschlossenen normalen Untergruppen von $Gal(L, K)$ sind $Gal(L, E)$ mit $E \mid K$ Galoiserweiterung. Äquivalent dazu ist eine abgeschlossene Untergruppe H von $Gal(L, K)$ genau dann normal, wenn $L^H \mid K$ Galoiserweiterung ist.*

4. *Die offenen normalen Untergruppen von $Gal(L, K)$ sind $Gal(L, F)$ mit $F \mid K$ endliche Galoiserweiterung. Äquivalent dazu ist eine offene Untergruppe H von $Gal(L, K)$ genau dann normal, wenn $L^H \mid K$ endliche Galoiserweiterung ist.*

Fortsetzung von Beispiel 2.0.1: Jetzt ist es möglich, das am Anfang gestellte Problem zu lösen. Um die Galoisgruppe von $\mathbb{F} \mid \mathbb{F}_p$ zu finden, beschreiben wir zunächst eine Topologie auf $(\mathbb{Z}, +)$. Eine offene Umgebungsbasis von $m \in \mathbb{Z}$ ist gegeben durch $(m + n\mathbb{Z})_{n \in \mathbb{N}^*}$. Also für eine offene Umgebung U von $m_1 \in \mathbb{Z}$ gilt $U \subseteq m_1 + n\mathbb{Z}$ für mindestens ein $n \in \mathbb{N}^*$. Falls ein m_2 nahe an m_1 liegt, also $m_2 \in U$ folgt, $m_2 \in m_1 + n\mathbb{Z} \iff n$ teilt $m_1 - m_2$. Damit ist $\mathbb{Z}$ eine topologische Gruppe, die man vervollständigen kann. Definiere dafür eine Cauchyfolge $(a_i)_{i \in I}$ mit $a_i \in \mathbb{Z}$ für die gilt: $\forall n \geq 1, \exists N, \forall i, j > N : a_i \equiv a_j \mod n$. Man nennt eine Cauchyfolge *trivial* falls $\forall n \geq 1, \exists N, \forall i > N : a_i \equiv 0 \mod n$, also $a_i \to 0$ wenn $i \to \infty$.
Sei nun C die Gruppe aller Cauchyfolgen und T die Gruppe aller trivialen Cauchyfolgen. T bildet eine Untergruppe von C. Definiere folgende Quotientengruppe:

$$\widehat{\mathbb{Z}} = C/T$$

Dies führt uns nun zum Resultat des Problems:

Satz 10. *Sei $\mathbb{F}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann ist die Galoisgruppe von $\mathbb{F} \mid \mathbb{F}_p$ gegeben durch:*

$$Gal(\mathbb{F}, \mathbb{F}_p) \cong \widehat{\mathbb{Z}} \cong \prod_{p \in \mathbb{P}} \mathbb{Z}_p$$

Beweis. Sei $\alpha \in \widehat{\mathbb{Z}}$ durch die Cauchyfolge (a_i) representiert, $G = Gal(\mathbb{F}, \mathbb{F}_p)$ und $\sigma \in G$. Dann hat die Einschränkung $\tilde{\sigma}$ von σ auf $\mathbb{F}_{p^n}$ die Ordnung n. Also ist $\tilde{\sigma}^{a_i}$ unabhängig von i für genügend großes i und wir können σ^α durch

$$\sigma^\alpha|_{\mathbb{F}_{p^n}} = \tilde{\sigma}^{a_i}$$

für alle n und alle $i \geq n_0$, abhängig von n, definieren. Damit erhalten wir eine Abbildung

$$\widehat{\mathbb{Z}} \to Gal(\mathbb{F}, \mathbb{F}_p), \alpha \mapsto \sigma^\alpha$$

die offensichtlich ein Isomorphismus ist. □

Beispiel 2.2.1. [**CO2**] Weitere Beispiele für unendliche Körpererweiterungen sind:

- $\overline{\mathbb{Q}} \mid \mathbb{Q}$
- $\mathbb{Q}(\zeta_{p^\infty}) \mid \mathbb{Q}$, mit $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n})$ und $\zeta_{p^n} = e^{2\pi i/p^n}$ die p^n-te Einheitswurzel.
- $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, ...) \mid \mathbb{Q}$, also das Körperkompositum aller quadratischen Zahlenkörper.

Diese drei Körpererweiterungen sind Galoiserweiterungen. Für das zweite und dritte Beispiel ist dies leicht zu sehen. Um zu zeigen, dass $\overline{\mathbb{Q}} \mid \mathbb{Q}$ galoissch ist, benutzte die Definition $L^{Aut(L|K)} = K$ mit $L = \overline{\mathbb{Q}}$ und $K = \mathbb{Q}$. Man muss also zu jedem Element $q \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$ einen K-Automorphismus σ_q finden mit $\sigma_q(q) \neq q$. Jedes Element q hat aber ein Minimalpolynom mit Grad ≥ 2, da jedes Element mit Minimalpolynom vom Grad 1 über $\mathbb{Q}$ Element von $\mathbb{Q}$ ist. Nun ist $\mathbb{Q}$ aber volkommen, also jede Erweiterung ist separabel. Zu jedem Element $q \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$ gibt es also ein Element $r \in \overline{\mathbb{Q}}$, welches Nullstelle des gleichen Minimalpolynoms wie q ist. Verwende nun den Fakt, dass es zu zwei verschiedenen Nullstellen q, r des gleichen Minimalpolynoms einen $\mathbb{Q}$-Homomorphismus $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ gibt mit $\sigma(q) = r$. Das ist also der gesuchte Automorphismus und somit ist die Aussage bewiesen.

Nun kann man die Galoisgruppen zu den Beispielen finden. Zunächst $Gal(\mathbb{Q}(\zeta_{p^\infty}), \mathbb{Q})$: Dafür zeigen wir, dass $Gal(\mathbb{Q}(\zeta_{p^n}), \mathbb{Q}) = (\mathbb{Z}/p^n\mathbb{Z})^*$.
Sei also $\phi \in Gal(\mathbb{Q}(\zeta_n), \mathbb{Q}) \iff \zeta_n^k$ ist primitiv $\iff ggt(k, n) = 1 \iff$

$k \in (\mathbb{Z}/n\mathbb{Z})^*$. Also gilt $Gal(\mathbb{Q}(\zeta_n), \mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$. Nun für $n, m \in \mathbb{N}^*$ mit $n \mid m$ kommutiert folgendes Diagramm:

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & Gal(\mathbb{Q}(\zeta_m), \mathbb{Q}) \\ \downarrow & & \downarrow \\ (\mathbb{Z}/n\mathbb{Z})^* & \longrightarrow & Gal(\mathbb{Q}(\zeta_n), \mathbb{Q}) \end{array}$$

Folglich gilt die Isomorphie $\varprojlim(\mathbb{Z}/n\mathbb{Z})^* \cong \varprojlim Gal(\mathbb{Q}(\zeta_n), \mathbb{Q})$ und daher auch $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})^* \cong \varprojlim Gal(\mathbb{Q}(\zeta_{p^n}), \mathbb{Q})$. Nun ist für eine aufsteigende Kette von Galoiserweiterungen $(F_i)_{i \in I}$ in $\overline{K}$ von K folgende Abbildung ein Isomorphismus von topologischen Gruppen:
$Gal(\bigcup_{i \in I} F_i, K) \to \varprojlim Gal(F_i, K)$. Daraus folgt dann schließlich $\varprojlim(\mathbb{Z}/p^n\mathbb{Z})^* \cong \varprojlim Gal(\mathbb{Q}(\zeta_{p^n}), \mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_{p^\infty}), \mathbb{Q})$.

Nun zum dritten Beispiel. Dafür sei $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, ...)$ und $K = \mathbb{Q}$. Sei weiters $a_0 = -1$ und a_i die i-te Primzahl. $K_0 = K$ und $K_{n+1} = K_n(\sqrt{a_n})$. Schlussendlich sei $M_n = \{\sqrt{a_0}, ..., \sqrt{a_n}\}$.
Des Weiteren ist $\{1, \sqrt{a_{n+1}}\}$ eine Basis von K_{n+1} über K_n. Also ist die Galoisgruppe von K_{n+1} über K_n gleich $\{\pm 1\} \cong \mathbb{Z}_3^*$ (multiplikative Schreibweise), denn $|K_{n+1} : K_n| = 2$. Die dazugehörige Erweiterung ist normal, da jede Erweiterung vom Grad 2 normal ist. Nach dem Hauptsatz der Galoistheorie, ist $Gal(K_{n+1}, K_n)$ ein Normalteiler von $Gal(K_{n+1}, K_0)$ und $Gal(K_{n+1}, K_0)/Gal(K_{n+1}, K_n)$ ist isomorph zu $Gal(K_n, K_0)$. Es gilt sogar $Gal(K_{n+1}, K_0) \cong Gal(K_{n+1}, K_n) \times Gal(K_n, K_0)$. Induktiv kann dann gezeigt werden, dass $Gal(K_n, K_0) \cong \{\pm 1\}^n$ gilt. Daraus folgt dann, dass $Gal(L, K) = \prod\{\pm 1\}$ ist.
Diese Erweiterung hat jedoch die Eigenschaft, dass die Anzahl der Untergruppen von $Gal(L, K)$ nicht mit den Zwischenkörper der Erweiterung übereinstimmt. Definiere dafür für jede Teilmenge X von $\mathbb{P} \cup \{-1\}$ die Menge G_p mit

$$G_p = \begin{cases} \mathbb{Z}_3^* & \text{falls } p \in X \\ 1 & \text{sonst} \end{cases} .$$

Somit gilt, dass $\prod_{p \in \mathbb{P} \cup \{-1\}} G_p$ eine Untergruppe von $\prod_{p \in \mathbb{P} \cup \{-1\}} \mathbb{Z}_3^*$ ist. Die Menge der Untergruppen hat die gleiche Kardinalität wie $\mathcal{P}(\mathbb{P})$, welche überabzählbar ist. Da $\prod_{p \in \mathbb{P} \cup \{-1\}} \mathbb{Z}_3^*$ überabzählbar viele Untergruppen hat, ist die Gruppe selbst überabzählbar. $Gal(L, K)$ hat also überabzählbar viele Untergruppen der Ordnung 2. Jedoch hat $L \mid K$ nur abzählbar viele Zwischenkörper mit Grad 2. Die Kardinalitäten stimmen also nicht überein.

Bemerkung: Die absolute Galoisgruppe $Gal(\overline{\mathbb{Q}}, \mathbb{Q})$ ist bisher unbekannt. Sie und ihre Untergruppen zu finden ist eines der großen Ziele der Zahlentheorie. Wenn man die Gruppe $Gal(\overline{\mathbb{Q}}, \mathbb{Q})$ versteht, dann auch viele endliche Galoisgruppen, die man von $Gal(\overline{\mathbb{Q}}, \mathbb{Q})$ ableiten kann. In diesem Kontext gibt es die sogenannten *dessins d'enfants* welche Werkzeuge zur Studie von Riemannschen Flächen sind und genutzt werden um kombinatorische Invarianten für die Operationen auf $Gal(\overline{\mathbb{Q}}, \mathbb{Q})$ zu liefern.

2.2.2 Pro-endliche Gruppe und Limes

Definition 2.2.1. Eine Familie (G_i, π_{ji}) heißt *projektives System*, falls i Element einer gerichteten Menge $(I, \leq)$ ist und die Abbildung $\pi_{ji} : G_j \to G_i$ mit $i \leq j$ folgende Eigenschaften erfüllt:

1. $\forall i \in I : \pi_{ii} = id$
2. $\forall i \leq j \leq k : \pi_{ji} \circ \pi_{kj} = \pi_{ki}$

Definition 2.2.2. Für ein projektives System (G_i, π_{ji}) definiert man den *projektiven Limes* durch:

$$\varprojlim G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \pi_{ji}(g_j) = g_j \text{ wann immer } i \leq j\}$$

$\varprojlim G_i$ ist als Untergruppe von $\prod_{i \in I} G_i$ wieder eine Gruppe. Des Weiteren kann man $\varprojlim G_i$ mit einer Topologie versehen, um es zu einer topologischen Gruppe zu machen.

Definition 2.2.3. Eine topologische Gruppe, die isomorph zu einem projektiven Limes endlicher Gruppe ist, heißt *pro-endliche Gruppe.*

Satz 11. *Sei G eine topologische Gruppe. Dann sind die folgenden Aussagen äquivalent.*

1. *G ist eine pro-endliche Gruppe.*
2. *G ist eine kompakte, Hausdorffsche, und total unzusammenhängende Gruppe.*

Beispiel 2.2.2. Einige Beispiele zu pro-endlichen Gruppen:

- Jede endliche Gruppe mit der diskreten Topologie ist pro-endlich.
- Jede Galoisgruppe mit der Krulltopologie ist pro-endlich.

Der projektive Limes ist ein praktisches Mittel, um Galoisgruppen zu bestimmen, es gilt nämlich folgendes:
Betrachte die (nicht notwendigerweise endliche) Erweiterung $L \mid K$ und sei $(Z(L,K), \subset)$ die (partiell geordnete) Menge ihrer Zwischenkörper F_i, sodass $F_i \mid K$ eine endliche Galoiserweiterung ist. $(Z(L,K), \subset)$ ist des Weiteren eine gerichtete Menge, da das Kompositum zweier Zwischenkörper wiederum eine Galoiserweiterung ist. Betrachte nun für $F_j \supset F_i$ folgende Abbildung:

$$\pi_{ji} : Gal(F_j, K) \to Gal(F_i, K)$$

Nun können wir den projektiven Limes definieren:

$$Gal(L,K) = \varprojlim Gal(F_i, K)$$

Somit haben wir $Gal(L,K)$ mit der pro-endlichen Topologie ausgestattet.

Definition 2.2.4. Sei G eine Gruppe. Die *pro-endliche Vervollständigung* von G ist die pro-endliche Gruppe $\widehat{G}$, die durch $\widehat{G} = \varprojlim G/N$ definiert wird, wobei N die Normalteiler von endlichem Index in G durchläuft, nach Inklusion geordnet, und zusammen mit den natürlichen Abbildungen π_{ji}.

Beispiel 2.2.3. Die zuvor bestimmte Galoisgruppe von $\mathbb{F} \mid \mathbb{F}_p$ ist die pro-endliche Vervollständigung von der Gruppe $\mathbb{Z}$, also:

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

Definition 2.2.5. Ein *perfekter Körper*, oder auch *vollkommener Körper*, ist ein Körper K in dessen Zerfällungskörper keine Mehrfachnullstellen auftreten, also ist jedes irreduzible Polynom separabel.
Dies ist äquivalent zur Eigenschaft, dass jede algebraische (oder endliche) Erweiterung von K separabel ist.

Definition 2.2.6. [**WP1**] Ist $L \mid K$ eine separable Körpererweiterung, dann sind folgende Aussagen äquivalent:

- Jedes nicht-konstante separable Polynom in $L[X]$ zerfällt vollständig in Linearfaktoren.
- Ist C ein algebraischer Abschluss von K und ist L eingebettet in C, dann ist die Erweiterung $C \mid L$ rein inseparabel.

Zu jedem Körper K gibt es einen bis auf Isomorphie eindeutig bestimmten Körper L mit den obigen Eigenschaften. Er wird auch mit K^{sep} bezeichnet und heißt separabler Abschluss von K.

Definition 2.2.7. Ein *absolute Galoisgruppe* G_K von einem Körper K ist die zum separablen Abschluss $K^{sep} \mid K$ gehörende Galoisgruppe.
Für einen perfekten Körper K gilt demnach $G_K = Gal(\overline{K}, K)$.

Beispiel 2.2.4. Es gilt $G_{\mathbb{F}_q} = \varprojlim \mathbb{Z}/n\mathbb{Z}$

Literatur

[1] [BU62] D. Burde, *Algebra Lecture Notes*, 2020.

[2] [CO] K. Conrad, *Dihedral Groups II*, pp.6–7, 2020.

[3] [CO2] K. Conrad, *Infinite Galois Theory*, 2020.

[4] [MM1] Stefan K., *p-adische Zahlen*, 2007.

[5] [WP1] "Wikipedia", *Separabler Abschluss*, `https://de.wikipedia.org/w/index.php?title=Separabler_Abschluss&action=history`, 2021.

[6] [PO1] A.Pomerantz, *An introduction to the p-adic numbers*, 2020.

Anhang A

p-adische Zahlen

Folgendes Kapitel basiert auf dem Artikel von www.matheplanet.com (Siehe [**MM1**]) und *An introduction to the p-adic numbers* von A.Pomerantz (Siehe [**PO1**]).

In vielen Beispielen zur Galoistheorie treten die sogenannten p-adischen Zahlen auf. Daher ist es angebracht, sie näher zu betrachten.

A.0.1 p-adische Entwicklung

Jedes Polynom $P(X)$ besitzt eine Summendarstellung:

$$P(X) = \sum_{i=1}^{n} a_i(x-\alpha)^i$$

mit $a_i \in \mathbb{C}$ und $\alpha \in \mathbb{C}$ fest.
Nach der gleichen Idee lässt sich auch jede ganze Zahl f in Basis p schreiben:

$$f = \sum_{i=1}^{n} a_i p^i$$

wobei $p \in \mathbb{P}$, $a_i \in \mathbb{Z}$ und $0 \leq a_i < p$.

Definition A.0.1. Schreibt man eine Zahl $f \in \mathbb{Z}$ als Summe, wie oben, so spricht man von einer *p-adischen Entwicklung.*

Satz 12. *Jede natürliche Zahl $f \in \mathbb{N}$ besitzt eine p-adische Entwicklung, mit Koeffizienten $a_i \in \{0, 1, ..., p-1\}$. Diese Entwicklung ist eindeutig und endlich.*
Schreibweise: $f = a_0, a_1 a_2 ... a_n(p)$

Beispiel A.0.1. $247 = 2, 31(13)$
Also $2 + 3 \cdot 13 + 1 \cdot 13^2 = 247$

Um rationale Zahlen p-adisch entwickeln zu können, braucht man eine unendlich Summe. Dies bringt uns zu folgendem Kapitel:

A.0.2 p-adische Zahlen

Definition A.0.2. Eine *ganze p-adische Zahl* ist eine formale unendliche Reihe $\sum_{i=0}^{\infty} a_i p^i$ mit $0 \leq a_i < p$ für alle i. Eine *p-adische Zahl* ist eine formale unendliche Reihe $\sum_{i=-m}^{\infty} a_i p^i$ mit $m \in \mathbb{Z}$ und $0 \leq a_i < p$ für alle i.
Die Menge aller ganzen p-adischen Zahlen ist überabzählbar und wird mit $\mathbb{Z}_p$ bezeichnet.
Die Menge aller p-adischen Zahlen wird mit $\mathbb{Q}_p$ bezeichnet.

Satz 13. *Für die Restklassen $a \mod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ existiert eine eindeutige Darstellung*

$$a \equiv \sum_{i=0}^{n-1} a_i p^i \mod p^n$$

mit $0 \leq a_i < p$ für alle i.

Beweis. Der Beweis erfolt per vollständige Induktion: Für $n = 1$ ist die Darstellung offensichtlich. Gelte nun die Behauptung für $n - 1$:

$$a \equiv \sum_{i=0}^{n-2} a_i p^i \mod p^{n-1}$$

Dies ist gleichbedeutend mit

$$a = \sum_{i=0}^{n-1} a_i p^i + g p^{n-1}$$

mit $g \in \mathbb{Z}$. Falls nun $g \equiv a_{n-1} \mod p$ mit $0 \leq a_{n-1} < p$, dann ist a_{n-1} eindeutig bestimmt und $g = a_{n-1} + kp$ mit $k \in \mathbb{Z}$. Nun lässt sich die a umschreiben als

$$\begin{aligned} & a = \sum_{i=0}^{n-1} a_i p^i + (a_{n-1} + kp) p^{n-1} \\ \iff & \text{a} = \sum_{i=0}^{n-1} a_i p^i + a_{n-1} p^{n-1} + kp^n \end{aligned}$$

Hiermit ist nun die Kongruenz im Satz gezeigt. □

Nun lassen sich die p-adischen Zahlen auch algebraisch, über den projektiven Limes, konstruieren. Dazu folgender Satz, welcher direkt aus Satz 13 folgt:

Satz 14. *Die Abbildung*

$$\begin{aligned} \mathbb{Z}_p &\to \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ f = \sum_{i=0}^{\infty} a_i p^i &\mapsto (\bar{s}_n)_{n \in \mathbb{N}} \end{aligned}$$

mit $\bar{s}_n = \sum_{i=0}^{n-1} a_i p^i \ mod\ p^n \in \mathbb{Z}/p^n\mathbb{Z}$ ist eine Bijektion.

$\mathbb{Q}_p$ ist der Quotientenkörper von $\mathbb{Z}_p$.

Beispiel A.0.2. Das vorherige Beispiel: 247=2,31(13) lässt sich in $\varprojlim \mathbb{Z}/13^n\mathbb{Z}$ schreiben als $(0, 78, 247, 247, ...)$,
weil $(247 \mod 13, 247 \mod 13^2, 247 \mod 13^3, ...) = (0, 78, 247, 247, ...)$

$\mathbb{Z} \ni 35 = 1, 10001(2) \in \mathbb{Z}_2$
$= (1, 3, 3, 3, 3, 35, 35, ...) \in \varprojlim \mathbb{Z}/2^n\mathbb{Z}$

Man kann die p-adischen Zahlen und die Mengen $\mathbb{Z}_p$ und $\mathbb{Q}_p$ auch analytisch definieren. Dazu zunächst folgende Definitionen:

Definition A.0.3. Die *p-adische Bewertung* auf $\mathbb{Q}$ ist definiert als Funktion $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Sei $x \in \mathbb{Q}$ mit $x \neq 0$. Falls $x \in \mathbb{Z}$, sei $v_p(x)$ die eindeutige ganze positive Zahl, welche

$$x = p^{v_p(x)}x' \text{ mit } p \nmid x'$$

erfüllt. Für alle $x \in \mathbb{Q}$ mit $x \neq 0$ lässt sich x schreiben als $x = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$. Definiere nun $v_p(x) = v_p(a) - v_p(b)$ und $v_p(0) = +\infty$.

Definition A.0.4. Definiere den *p-adischen Betrag* als Funktion $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ mit

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{wenn } x \neq 0 \\ 0 & \text{wenn } x = 0. \end{cases}$$

Der p-adische Betrag induziert die *p-adische Metrik* d_p.

Satz 15. *Sei $\mathbb{K}$ ein Körper mit Betragsfunktions $|\cdot|$. Dann existiert ein vollständiger Körper $\mathbb{K}'$ (i.e. jede Cauchyfolge konvergiert) mit Betragsfunktion $|\cdot|'$ welcher $\mathbb{K}$ erweitert. Die Vervollständigung $\mathbb{K}'$ ist, bis auf Isomorphismus, eindeutig. Ausserdem ist $|\cdot|$ die Einschränkung von $|\cdot|'$ auf $\mathbb{K}$. Schlussendlich liegt $\mathbb{K}$ dicht in $\mathbb{K}'$.*

Definition A.0.5. Der *Körper der p-adischen Zahlen* $\mathbb{Q}_p$ ist definiert als die Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Metrik. Satz 15 gibt die Existenz und Eindeutigkeit einer solchen Vervollständigung.

Definition A.0.6. Der *Körper der ganzen p-adischen Zahlen* $\mathbb{Z}_p$ ist definiert wie folgt:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p, |\cdot|_p \leq 1\}$$

$\mathbb{Z}_p$ ist die Vervollständigung von $\mathbb{Z}$ bezüglich der p-adischen Metrik.