Körpererweiterung

In der abstrakten Algebra ist ein *Unterkörper* K eines Körpers L eine Teilmenge $K \subseteq L$, die 0 und 1 enthält und mit den auf K eingeschränkten Verknüpfungen selbst ein Körper ist. L wird dann *Oberkörper* von K genannt. Das Paar L und K bezeichnet man als **Körpererweiterung** und schreibt es als L/K oder $L \mid K$, seltener als $L\colon K$ oder (L, K).

Zum Beispiel ist der Körper $\mathbb{C}$ der komplexen Zahlen ein Oberkörper des Körpers $\mathbb{R}$ der reellen Zahlen und daher $\mathbb{C}/\mathbb{R}$ eine Körpererweiterung.

Inhaltsverzeichnis

Definition und Schreibweisen

Sei L ein Körper, und sei K eine Teilmenge von L, die 0 und 1 enthält (die jeweiligen neutralen Elemente der Verknüpfungen) und mit den auf K eingeschränkten Verknüpfungen Addition und Multiplikation selbst ein Körper ist. In diesem Fall heißt K *Unterkörper* (oder *Teilkörper*) von L und L heißt *Oberkörper* (oder *Erweiterungskörper*) von K.

Eine Teilmenge $K \subseteq L$ ist genau dann ein Teilkörper von L, wenn sie 0 und 1 enthält und bezüglich der vier Verknüpfungen Addition, Multiplikation, Negation (also Übergang von x zu $-x$) und Kehrwertbildung (also Übergang von x zu x^{-1}) abgeschlossen ist, d. h. die Verknüpfung von Elementen von K liefert wieder ein Element von K.

Die verbreitetste Schreibweise für Körpererweiterungen ist L/K (nicht als Bruch, sondern nebeneinander mit Schrägstrich), manchmal findet man auch $L \mid K$, seltener die Schreibweise $L\colon K$. Einige Autoren schreiben auch lediglich $L \supset K$ und fügen in Worten an, dass es sich um eine Körpererweiterung handelt.

Die Schreibweise L/K entspricht am ehesten der Sprechweise "*L über K*", es besteht aber eine geringe Verwechslungsgefahr mit Faktorstrukturen wie Faktorgruppen oder Faktorräumen, die ebenfalls mit einem Schrägstrich geschrieben werden.

Etwas allgemeiner betrachtet man auch den folgenden Fall als Körpererweiterung: Es seien K_1, K_2 und L Körper, K_2 Teilkörper von L und K_1 isomorph zu K_2. Wenn es nicht zu Missverständnissen führt und der Isomorphismus aus dem Zusammenhang klar ist, kann man K_1 und K_2 identifizieren und so K_1 selbst als Teilkörper von L auffassen.

Ein Körper M heißt *Zwischenkörper* der Körpererweiterung L/K, wenn M ein Unterkörper von L und ein Oberkörper von K ist, also $K \subseteq M \subseteq L$ gilt.

Es sei im Folgenden stets L/K eine Körpererweiterung.

Erweiterungsgrad

Der Oberkörper L ist ein Vektorraum über K, wobei die Vektoraddition die Körper-Addition in L ist und die Skalarmultiplikation die Körper-Multiplikation von Elementen aus L mit Elementen aus K. Die Dimension dieses Vektorraums wird *Grad der Erweiterung* genannt und $[L\colon K]$ geschrieben. Die Erweiterung heißt *endlich* oder *unendlich*, je nachdem ob der Grad endlich oder unendlich ist.

Ein Beispiel für eine endliche Körpererweiterung ist die Erweiterung $\mathbb{C}/\mathbb{R}$ der reellen Zahlen zu den komplexen Zahlen. Der Grad $[\mathbb{C} : \mathbb{R}]$ dieser Erweiterung ist 2, da $\{1, i\}$ eine $\mathbb{R}$-Basis von $\mathbb{C}$ ist. Im Gegensatz dazu ist $[\mathbb{R} : \mathbb{Q}] = \infty$ (genauer gleich der Mächtigkeit $\mathfrak{c}$ des Kontinuums), also ist diese Erweiterung unendlich.

Sind M/L und L/K Körpererweiterungen, dann ist auch M/K eine Körpererweiterung, und es gilt der *Gradsatz*

$$[M : K] = [M : L] \cdot [L : K].$$

Dies gilt auch im Falle unendlicher Erweiterungen (als Gleichung von Kardinalzahlen, oder alternativ mit den üblichen Rechenregeln für das Symbol unendlich). L/K heißt dabei eine *Teilerweiterung* von M/K.

Algebraisch und transzendent

Ein Element ℓ von L, das Nullstelle eines Polynoms über K ist, das nicht das Nullpolynom ist, heißt *algebraisch* über K. Das normierte Polynom von kleinstem Grad mit dieser Nullstelleneigenschaft heißt Minimalpolynom von ℓ . Ist ein Element nicht algebraisch, dann heißt es *transzendent*. Der Fall $L = \mathbb{C}$ und $K = \mathbb{Q}$ ist dabei besonders wichtig. Siehe dazu algebraische Zahl, transzendente Zahl.

Ist jedes Element von L algebraisch über K, dann heißt L/K *algebraische Erweiterung*, andernfalls *transzendente Erweiterung*. Wenn jedes Element von $L \setminus K$ (also aus L ohne K) transzendent ist, dann heißt die Erweiterung *rein transzendent*.

Man kann zeigen, dass eine Erweiterung genau dann algebraisch ist, wenn sie die Vereinigung aller ihrer endlichen Teilerweiterungen ist. Damit ist jede endliche Erweiterung algebraisch; zum Beispiel trifft dies für $\mathbb{C}/\mathbb{R}$ zu. Die Körpererweiterung $\mathbb{R}/\mathbb{Q}$ ist dagegen transzendent, wenn auch nicht rein transzendent. Es gibt aber auch unendliche algebraische Erweiterungen. Beispiele sind die algebraischen Abschlüsse für den Körper der rationalen Zahlen $\mathbb{Q}$ und für die Restklassenkörper $\mathbb{Z}/p\mathbb{Z}$.

Körperadjunktion

Ist V eine Teilmenge von L, dann ist der Körper $K(V)$ ("K adjungiert V") definiert als der kleinste Teilkörper von L, der K und V enthält, mit anderen Worten, der Durchschnitt aller K und V enthaltenden Teilkörper von L. $K(V)$ besteht aus allen Elementen von L, die mit endlich vielen Verknüpfungen $+, -, \cdot, /$ aus den Elementen von K und V gebildet werden können. Ist $L = K(V)$, dann sagt man, L wird von V erzeugt.

Primkörper

Der Primkörper eines Körpers K ist der Durchschnitt aller Unterkörper von K. Als Primkörper bezeichnet man auch einen Körper K, der keine echten Teilkörper hat, der also selbst sein eigener Primkörper ist.

Jeder Primkörper ist zum Körper $\mathbb{Q}$ der rationalen Zahlen oder einem der Restklassenkörper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ isomorph (wobei p eine Primzahl ist).

Falls der Primkörper von K isomorph zu $\mathbb{Q}$ ist, so sagt man, K habe Charakteristik null. Ist der Primkörper von K isomorph zu $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, so sagt man, K habe Charakteristik p.

Einfache Erweiterung

Eine Körpererweiterung $K(a)/K$, die von einem einzelnen Element a erzeugt wird, heißt *einfach*. Eine einfache Erweiterung ist endlich, wenn sie von einem algebraischen Element erzeugt wird, und rein transzendent, wenn sie von einem transzendenten Element erzeugt wird. Ist a algebraisch, dann ist der Erweiterungsgrad $[K(a) : K]$ gleich dem Grad n des Minimalpolynoms von a. Eine K-Basis von $K(a)$ ist dann gegeben durch $\{1, a, a^2, \ldots, a^{n-1}\}$. Ist hingegen a transzendent, so ist $K(a)$ isomorph zum rationalen Funktionenkörper $K(X)$.

Zum Beispiel ist $\mathbb{C}$ eine einfache Erweiterung von $\mathbb{R}$, denn $\mathbb{C} = \mathbb{R}(i)$ mit $i^2 = -1$. Die Erweiterung $\mathbb{R}/\mathbb{Q}$ kann nicht einfach sein, da sie weder algebraisch noch rein transzendent ist. Jede endliche Erweiterung von $\mathbb{Q}$ ist einfach.

Allgemeiner gilt: Jede endliche Erweiterung eines Körpers mit Charakteristik 0 ist eine einfache Erweiterung. Dies folgt aus dem Satz vom primitiven Element, welcher ein hinreichendes Kriterium für einfache Erweiterungen liefert.

Kompositum

Sind K_1 und K_2 Teilkörper von L, dann heißt der kleinste gemeinsame Oberkörper $K_1(K_2) = K_2(K_1)$ das *Kompositum* von K_1 und K_2.

Sind K_1 und K_2 beides endlich erweiterte Oberkörper von K, dann ist auch $K_1(K_2)/K$ endlich.

Zerfällungskörper

→ *Hauptartikel: Zerfällungskörper*

Der *Zerfällungskörper* eines Polynoms ist eine spezielle Körpererweiterung.

K sei weiterhin ein Körper, $p \in K[X]$ ein nicht konstantes Polynom über K. L/K ist ein *Zerfällungskörper* von p, wenn alle Nullstellen von p in L liegen und L diesbezüglich minimal ist. Man sagt auch, dass L durch Adjunktion aller Wurzeln von p an K entsteht. Dieser Körper heißt Zerfällungskörper, da p über L in Linearfaktoren *zerfällt*. Jedes nicht konstante Polynom besitzt einen bis auf Isomorphie eindeutigen Zerfällungskörper

Zum Beispiel hat $X^3 - 2 \in \mathbb{Q}[X]$ den Zerfällungskörper $\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$.

Allgemeiner definiert man den Zerfällungskörper bezüglich einer Menge von Polynomen: Dieser enthält alle Nullstellen aller Polynome dieser Menge und entsteht durch Adjunktion aller dieser Nullstellen an K. Auch in diesem Fall kann man die Existenz eines bis auf Isomorphie eindeutigen Zerfällungskörpers beweisen. Nimmt man die Menge aller Polynome über K, so erhält man den

algebraischen Abschluss

Normale Erweiterungen

L/K heißt *normale Erweiterung*, wenn alle Minimalpolynome über K von Elementen aus L in L vollständig in Linearfaktoren zerfallen. Ist a in L und f sein Minimalpolynom über K, dann heißen die Nullstellen von f in L die Konjugierten von a. Sie sind genau die Bilder von a unter K-Automorphismen von L.

Eine Körpererweiterung ist genau dann normal, wenn sie Zerfällungskörper einer Familie von Polynomen mit Koeffizienten aus dem Grundkörper ist.

Ist L nicht normal über K, dann gibt es jedoch einen Oberkörper von L, der normal über K ist. Er heißt die *normale Hülle* von L/K.

Ein Beispiel für eine nicht normale Körpererweiterung ist $L = \mathbb{Q}(\sqrt[3]{2})$: Das Minimalpolynom des erzeugenden Elements ist $X^3 - 2$ und hat komplexe, also nicht in L liegende, Nullstellen: $\{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}$. Hierbei bezeichne ζ_3 die dritte Einheitswurzel.

Separabilität

Separable Polynome

Ein Polynom f über K heißt *separabel*, wenn es in seinem Zerfällungskörper nur einfache Nullstellen hat. Es ist genau dann separabel, wenn es teilerfremd zu seiner formalen Ableitung f' ist. Ist f irreduzibel, dann ist es genau dann separabel, wenn f' nicht das Nullpolynom ist.

Es gibt aber auch eine abweichende Definition, der zufolge ein Polynom separabel heißt, wenn jeder seiner irreduziblen Teiler im obigen Sinn separabel ist. Für irreduzible Polynome und damit insbesondere für Minimalpolynome stimmen beide Definitionen überein, für reduzible Polynome unterscheiden sie sich jedoch.

Separable Erweiterungen

Ein algebraisches Element von L heißt *separabel* über K, wenn sein Minimalpolynom über K separabel ist. Eine algebraische Erweiterung L/K heißt *separable Erweiterung*, wenn alle Elemente von L separabel sind.

Ein Beispiel für eine inseparable Körpererweiterung ist $L = \mathbb{F}_p(X),\ K = \mathbb{F}_p(X^p) \subset L$, denn das Minimalpolynom $T^p - X^p \in K[T]$ des Erzeugers X zerfällt über L in $(T - X)^p$ und hat somit X als p-fache Nullstelle.

Der Separabilitätsgrad $[L : K]_s$ einer algebraischen Körpererweiterung L/K wird definiert als die Anzahl der K-Homomorphismen von L in den L enthaltenden algebraischen Abschluss von K, die auf K die Identität sind. Für $L = K(a)$ und ein Minimalpolynom f von a über K ist $[L : K]_s$ die Anzahl der verschiedenen Nullstellen von f im algebraischen Abschluss von K. Für einen Turm algebraischer Körpererweiterungen $M/L/K$ gilt die Produktformel $[M : K]_s = [M : L]_s \cdot [L : K]_s$.

Vollkommene Körper

Für viele Körper K, über denen Körpererweiterungen untersucht werden, sind irreduzible Polynome immer separabel und man muss sich bei diesen Körpern nicht um die Bedingung der Separabilität kümmern. Man nennt diese Körper *vollkommen* oder *perfekt*.

Etwas formaler kann ein vollkommener Körper durch eine der folgenden gleichwertigen Eigenschaften des Körpers K bzw. des Polynomrings $K[X]$ charakterisiert werden:

1. Jedes irreduzible Polynom in $K[X]$ ist separabel.

2. Jeder algebraische Abschluss $\overline{K}$ von K ist eine Galoiserweiterung (im weiteren Sinn, der im Artikel Galoisgruppe erläutert wird: auch unendlichdimensionale Erweiterungen können Galoiserweiterungen sein) von K.
3. Jede algebraische Körpererweiterung von K ist separabel über K (und ist überdies auch wieder vollkommen).
4. Der Körper K hat entweder die Charakteristik 0 oder er hat Primzahlcharakteristik p und es gilt $K = K^p$, d. h., der Frobeniusendomorphismus ist bijektiv.
5. Der Körper K hat entweder die Charakteristik 0 oder er hat Primzahlcharakteristik p und jedes Element aus K hat eine p-te Wurzel.

Insbesondere sind Körper der Charakteristik 0, endliche Körper und algebraisch abgeschlossene Körper vollkommen. Ein Beispiel für einen nicht vollkommenen Körper ist $L = \mathbb{F}_p(X)$ – dort hat das Körperelement X keine p-te Wurzel.

K-Automorphismen

Die Gruppe $\mathbf{Aut}(L)$ aller Automorphismen von L nennt man die Automorphismengruppe von L.

Für jeden Automorphismus $\sigma \in \mathbf{Aut}(L)$ definiert man den *Fixkörper* $\mathbf{Fix}(\sigma) := L^\sigma := \{x \in L : \sigma(x) = x\}$ aller Elemente von L, die von σ festgehalten werden. Man rechnet leicht nach, dass das ein Teilkörper von L ist. Der Fixkörper $\mathbf{Fix}(G)$ (auch geschrieben als L^G) einer ganzen Gruppe G von Automorphismen in L ist definiert durch:

$$\mathbf{Fix}(G) := L^G := \bigcap_{\sigma \in G} \mathbf{Fix}(\sigma)$$

Die Automorphismen von L, die mindestens K punktweise fest lassen, bilden eine Untergruppe von $\mathbf{Aut}(L)$, die Gruppe der K-Automorphismen von L, die mit $\mathbf{Aut}(L/K)$ oder auch $\mathbf{Aut}_K(L)$ bezeichnet wird.

Galoiserweiterung

→ *Hauptartikel: Galoistheorie*

Galoisgruppen

Ist die Erweiterung L/K algebraisch, normal und separabel, dann heißt die Erweiterung *galoissch* ([galoa:ʃ], nach Évariste Galois). Eine algebraische Erweiterung ist genau dann galoissch, wenn der Fixkörper $\mathbf{Fix}(\mathbf{Aut}(L/K))$ der K-Automorphismengruppe gleich K ist.

Man nennt $\mathbf{Aut}(L/K)$ in diesem Fall die *Galoisgruppe* der Erweiterung und schreibt sie als $\mathbf{G}(L/K), \mathbf{G}_{L/K}$, oder $\mathbf{Gal}(L/K)$. Abweichend von der im vorliegenden Artikel benutzten Sprachregelung wird im Artikel „Galoisgruppe“ die Gruppe $\mathbf{Aut}(L/K)$ stets als *Galoisgruppe* bezeichnet, auch wenn die Erweiterung L/K nicht galoissch ist.

Ist die Galoisgruppe einer Galoiserweiterung abelsch, dann heißt diese *abelsche Erweiterung*, ist sie zyklisch, dann heißt die Erweiterung *zyklisch*. Zum Beispiel ist $\mathbb{C}/\mathbb{R}$ abelsch und zyklisch, denn ihre Galoisgruppe ist zweielementig und besteht aus der Identität und der komplexen Konjugation

Der Körper der reellen Zahlen ist – wie allgemeiner jeder reell abgeschlossene oder auch nur euklidische Körper – über *keinem* seiner echten Teilkörper galoissch, weil durch die dort einzig mögliche Körperanordnung die identische Abbildung der einzig mögliche Körperautomorphismus ist.

Beispiele

- $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ ist eine Galoiserweiterung. Die Automorphismengruppe besteht genau aus der Identität und dem Automorphismus, der $\mathbb{Q}$ konstant lässt, aber $\sqrt{2}$ und $-\sqrt{2}$ vertauscht. Der Fixkörper davon ist $\mathbb{Q}$.
- $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ ist *keine* Galoiserweiterung, denn die Automorphismengruppe A besteht nur aus der Identität. Ein Automorphismus auf dieser Erweiterung, der $\sqrt[3]{2}$ nicht fix lässt, müsste $\sqrt[3]{2}$ auf eine andere dritte Wurzel aus 2

abbilden, jedoch enthält $\mathbb{Q}(\sqrt[3]{2})$ keine weiteren dritten Wurzeln aus 2. Da es sich um keine Galoiserweiterung handelt, heißt sie auch weder abelsch noch zyklisch, obwohl die Gruppe $\mathcal{A}$ (als triviale Gruppe) natürlich zyklisch und abelsch ist.
- Ein algebraischer Abschluss $\bar{K}$ eines beliebigen Körpers K ist genau dann galoissch über K, wenn K ein vollkommener Körper ist.

Konstruierbarkeitsfragen

Die klassischen Probleme der antiken Mathematik, bei denen es um die Konstruierbarkeit einer bestimmten *Zahl* (als Streckenlänge) allein mit Zirkel und Lineal aus rationalen Zahlen geht, konnten mit der Galoistheorie in gruppentheoretische Fragen umformuliert werden. Mit dem Grundgedanken von René Descartes, dass die Punkte auf Geraden (Lineal) und Kreisen (Zirkel) durch analytische Gleichungen darstellbar sind, lässt sich zeigen, dass die konstruierbaren Zahlen (Koordinaten von endlichen Schnittmengen von zwei dieser Figuren in der rationalen Zahlenebene bzw. auf der Basis bereits konstruierter Zahlen) genau die folgenden sind:

- Die rationalen Zahlen,
- die Quadratwurzeln aus konstruierbaren Zahlen,
- Summe, Differenz und Produkt von zwei konstruierbaren Zahlen,
- der Kehrwert jeder von 0 verschiedenen konstruierbaren Zahl.

Damit kann man zeigen, dass jede konstruierbare reelle Zahl

1. algebraisch und
2. vom Grad einer Zweierpotenz 2^n über dem Körper $\mathbb{Q}$ der rationalen Zahlen ist.

Dies bedeutet, dass für eine konstruierbare Zahl c die Körpererweiterung $\mathbb{Q}(c)/\mathbb{Q}$ eine endliche, algebraische Erweiterung vom Grad 2^n ($n \in \mathbb{N}$) sein muss. Dies ist noch keine hinreichende Bedingung, genügt aber in den klassischen Fragen für einen Unmöglichkeitsbeweis.

1. Quadratur des Kreises Unmöglich, da die Kreiszahl π nicht algebraisch ist.
2. Verdoppelung des Würfels Unmöglich: Im Verhältnis zum konstruierten Ausgangswürfel (etwa ein Würfel mit der Kantenlänge 1) hätte der neue Würfel die Kantenlänge $\alpha = \sqrt[3]{2}$. Die Körpererweiterung $\mathbb{Q}(\alpha)/\mathbb{Q}$ hat den Grad 3 – keine Zweierpotenz.
3. Dreiteilung des Winkels Ein Winkel mit dem Gradmaß 60° kann mit Zirkel und Lineal nicht in drei gleiche Teile geteilt werden. Wäre dieser Winkel – also 20° – konstruierbar, dann könnte man auch die reelle Zahl $\xi = \cos 20°$ konstruieren. Für jeden Winkel α gilt das Additionstheorem $\cos(3\alpha) = 4(\cos(\alpha))^3 - 3\cos(\alpha)$. Also löst unsere Zahl ξ die Gleichung $\frac{1}{2} = 4x^3 - 3x$ und ist daher eine Nullstelle von $8x^3 - 6x - 1$. Da dieses Polynom über $\mathbb{Q}$ irreduzibel ist, hat ξ über $\mathbb{Q}$ den Grad 3.

→ Im Artikel Euklidischer Körper wird dargestellt, wie eine Körpererweiterung von $\mathbb{Q}$ beschaffen sein muss, damit genau die mit Zirkel und Lineal konstruierbaren Zahlen im Erweiterungskörper vorhanden sind.

Weblinks

Wikiversity: Vorlesung über Körper- und Galoistheorie – Kursmaterialien, Forschungsprojekte und wissenschaftlicher Austausch

Literatur

- Thomas W. Hungerford: *Algebra* (Graduate Texts in Mathematics; Bd. 73). 5. Aufl. Springer-Verlag, New York 1989, ISBN 0-387-90518-9 (englisch)
- Siegfried Bosch: *Algebra*. 7. Aufl. Springer-Verlag, Berlin 2009, ISBN 3-540-40388-4