WIKIPEDIA

Galoisgruppe

Die **Galoisgruppe** (nach Évariste Galois) ist eine Gruppe, mit deren Hilfe Körpererweiterungen in der Algebra untersucht werden können.

Die Zwischenkörper einer Körpererweiterung lassen sich gewissen Untergruppen der Galoisgruppe zuordnen. Damit kann man Strukturuntersuchungen von Körpererweiterungen mit gruppentheoretischen Untersuchungen in Verbindung bringen. Da zu endlichdimensionalen Körpererweiterungen endliche Galoisgruppen gehören, können damit solche Strukturuntersuchungen oft stark vereinfacht werden.

Historisch bedeutsam war, dass die klassischen Fragen der Konstruierbarkeit – mit Zirkel und Lineal – gewisser algebraischer Zahlen damit in eine gruppentheoretische Formulierung übersetzt werden konnten. Einzelheiten zur klassischen Fragestellung der Konstruierbarkeit mit Zirkel und Lineal, Beispiele und deren moderne Lösung siehe unter → Konstruierbares Polygon

Inhaltsverzeichnis

Definition

Sei F/K (lies: „F über K“) eine Körpererweiterung. Das heißt: K und F sind Körper und der Körper K ist als Unterring in F enthalten. Damit ist F zugleich ein (nicht notwendig endlichdimensionaler) K-Vektorraum.

In dieser Situation heißt die Gruppe aller Körperautomorphismen des Erweiterungskörpers F, die den Grundkörper K elementweise festlassen, die *Galoisgruppe* von F über K und wird mit $\mathrm{Gal}(F/K)$ bezeichnet, formal

$$\mathrm{Gal}(F/K) = \{\varphi \in \mathrm{Aut}(F) \mid \forall k \in K : \varphi(k) = k\}.$$

Dies kann auch so formuliert werden: Die Galoisgruppe von F über K besteht genau aus den Körperautomorphismen von F, die zugleich Vektorraumendomorphismen von F als K-Vektorraum sind.

Galoisgruppe eines Polynoms

Sei K ein Körper. Als *Galoisgruppe des Polynoms* f im Polynomring $K[x]$ wird die Gruppe $\mathrm{Gal}(F/K)$ bezeichnet, wobei F ein Zerfällungskörper des Polynoms f ist. Man spricht in diesem Fall auch von *dem* Zerfällungskörper, da Zerfällungskörper – und damit *die* Galoisgruppe eines Polynoms – bis auf Isomorphie eindeutig bestimmt sind.

Der Zerfällungskörper F eines Polynoms ist *normal* über dem Grundkörper K. In diesem Fall ist die – hier endlichdimensionale – Körpererweiterung F/K bereits dann galoissch, wenn die über K irreduziblen Faktoren von f separabel sind. Der Artikel Galoistheorie behandelt den Begriff der Galoisgruppe eines Polynoms, für diesen Fall genügt die unten genannte erste Fassung des Hauptsatzes – der Hauptsatz für endliche Galoiserweiterungen.

Abweichende Bedeutungen des Begriffs

Besonders nützlich ist die Galoisgruppe, wenn die Körpererweiterung F/K eine Galoiserweiterung (s. u.) ist. In der Literatur wird oft nur in diesem Falle von „Galoisgruppe“ gesprochen. Die in diesem Artikel verwendete Gruppe der K-Automorphismen von F wird dann mit $\mathrm{Aut}_K(F)$ bezeichnet.

Eigenschaften

- Die Galoisgruppe ist eine Untergruppe der Automorphismengruppe von F.

- Ist die Körpererweiterung F/K endlich, d. h. ist F endlichdimensional über K, so ist die Gruppenordnung von $\mathrm{Gal}(F/K)$ kleiner gleich dem Erweiterungsgrad $[F:K]$. In diesem Fall existiert für jedes Körperelement $\alpha \in F$ das Minimalpolynom $f = m_{K,\alpha}$ von α über K. Ist F/K eine endliche Galoiserweiterung, dann gilt $|\mathrm{Gal}(F/K)| = [F:K]$.
- Sei F ein Zerfällungskörper des Polynoms f über K. Jeder Automorphismus aus der Galoisgruppe $\mathrm{Gal}(F/K)$ des Polynoms f bildet eine Nullstelle von f wieder auf eine Nullstelle ab. Die Galoisgruppe operiert also auf der Menge der Nullstellen von f im Körper F, $N = \{u_1, u_2, \ldots u_n\}$ als Permutationsgruppe und ist damit isomorph zu einer Untergruppe der symmetrischen Gruppe S_n. Für ein separables, über K irreduzibles Polynom f ist diese Operation sogar transitiv, das heißt zu zwei verschiedenen Nullstellen $u_j \neq u_k$ gibt es ein Element φ der Galoisgruppe, das u_j auf u_k abbildet: $\varphi(u_j) = u_k$.

Galoiskorrespondenz, Abgeschlossene Untergruppen und Zwischenkörper

Man kann jedem Zwischenkörper L der Erweiterung F/K die Untergruppe der Galoisgruppe $G = \mathrm{Gal}(F/K)$ zuordnen, deren Elemente L elementweise fest lässt, und umgekehrt jeder Untergruppe H von $\mathrm{Gal}(F/K)$ den Zwischenkörper, den sie fixiert. Nach Hungerford (1981) wird hier für beide Zuordnungen, die beide auch als *Galoiskorrespondenz* bezeichnet werden, die „Priming-Notation“ verwendet:

$$L' := \mathrm{Gal}(F/L) := \{\varphi \in \mathrm{Gal}(F/K) \,|\, \forall l \in L : \varphi(l) = l\}$$
$$H' := \{f \in F \,|\, \forall \eta \in H : \eta(f) = f\}$$

Für Zwischenkörper L und M der Erweiterung, Untergruppen H und J von G gelten folgende Beziehungen:

1. $F' = 1$ und $K' = G$,
2. $1' = F$,
3. $L \subset M \Rightarrow M' < L'$,
4. $H < J \Rightarrow J' \subset H'$,
5. $L \subset L''$ und $H < H''$,
6. $L' = L'''$ und $H' = H'''$.

Die Körpererweiterung F/K heißt hier *Galoiserweiterung*, wenn sie normal und separabel ist. Dies ist genau dann der Fall, wenn $G' = K$ gilt, wenn also die Galoisgruppe außer dem Grundkörper keine weiteren Elemente von F fixiert. Da in allen Fällen $K' = G$ gilt, ist die Erweiterung genau dann galoissch, wenn $K = K''$ ist. Dieselbe Bedingung gilt für Zwischenkörper L: Die Erweiterung F/L ist genau dann eine Galoiserweiterung, wenn $L = L''$ gilt. Die Begriffe *normal* und *separabel* werden im Artikel Körpererweiterung unabhängig von den hier verwendeten Zuordnungen definiert. Dort wird im Abschnitt Galoiserweiterung dieselbe für den Fall definiert, dass die Erweiterung algebraisch ist. Die hier verwendete Definition lässt nach Emil Artin und Hungerford (1981) auch nicht algebraische Erweiterungen zu.

Abgeschlossenheit

Nach Hungerford (1981) heißt eine Untergruppe X der Galoisgruppe oder ein Zwischenkörper X der Erweiterung *abgeschlossen*, wenn $X = X''$ gilt.

- Alle Objekte $X = Y'$, die als Bilder der oben beschriebenen Korrespondenzen auftreten, sind abgeschlossen (nach 6.).
- Die triviale Untergruppe 1, G und F sind abgeschlossen.
- Die Erweiterung F/K ist genau dann eine Galoiserweiterung, wenn K abgeschlossen ist.

Mit den am Anfang des Abschnitts vereinbarten Bezeichnungen gilt:

- Wenn L abgeschlossen ist und $[L:M]$ endlich ist, dann ist M abgeschlossen und es gilt $[L':M'] = [M:L]$.
- Wenn H abgeschlossen ist und $[J:H]$ endlich ist, dann ist J abgeschlossen und $[H':J'] = [J:H]$.
- Speziell gilt (für $H = 1$): Jede *endliche* Untergruppe der Galoisgruppe ist abgeschlossen.
- Wenn F eine endlichdimensionale Galoiserweiterung von K ist, dann sind alle Zwischenkörper und alle Untergruppen der Galoisgruppe abgeschlossen und die Galoisgruppe hat die Ordnung $[F:K]$.

Hauptsätze der Galoistheorie

Endlichdimensionale Körpererweitung

Ist F eine endlichdimensionale Galoiserweiterung von K, dann vermittelt die Galoiskorrespondenz eine Bijektion zwischen der Menge der Zwischenkörper und der Menge der Untergruppen der Galoisgruppe. Diese Korrespondenz bildet den Teilmengenverband der Zwischenkörper (mit der Ordnung $\subset$) auf den Verband der Untergruppen (mit der Ordnung $>$) ordnungstreu ab, wobei die Teilmengenbeziehung umgekehrt wird. Dabei gilt:

1. Die relative Dimension von zwei Zwischenkörpern ist gleich dem relativen Index der korrespondierenden Untergruppen.
2. F ist galoissch über jedem Zwischenkörper L. Die Galoisgruppe $\mathrm{Gal}(F/L)$ stimmt mit der Untergruppe L' überein.
3. Ein Zwischenkörper L ist galoissch über K genau dann, wenn die korrespondierende Untergruppe L' ein Normalteiler der Galoisgruppe $G = \mathrm{Gal}(F/K)$ ist. In diesem Fall ist die Faktorgruppe G/L' isomorph zur Galoisgruppe $\mathrm{Gal}(L/K)$ des Körpers L über K.

Unendlichdimensionale algebraische Erweiterung

Ist F eine algebraische, nicht notwendig endlichdimensionale Galoiserweiterung von K, dann vermittelt die Galoiskorrespondenz eine Bijektion zwischen der Menge *aller* Zwischenkörper und der Menge der *abgeschlossenen* Untergruppen der Galoisgruppe. Diese Korrespondenz bildet den Teilmengenverband der Zwischenkörper (mit der Ordnung $\subset$) auf den Verband der abgeschlossenen Untergruppen (mit der Ordnung $>$) ordnungstreu ab, wobei die Teilmengenbeziehung umgekehrt wird. Dabei gilt:

1. F ist galoissch über jedem Zwischenkörper L. Die Galoisgruppe $\mathrm{Gal}(F/L)$ stimmt mit der Untergruppe L' überein.
2. Ein Zwischenkörper L ist galoissch über K genau dann, wenn die korrespondierende Untergruppe L' ein Normalteiler der Galoisgruppe $G = \mathrm{Gal}(F/K)$ ist. In diesem Fall ist die Faktorgruppe G/L' isomorph zur Galoisgruppe $\mathrm{Gal}(L/K)$ des Körpers L über K.

Beispiele

- Die komplexen Zahlen sind ein Körper und enthalten den Körper der reellen Zahlen. Also ist $\mathbb{C}/\mathbb{R}$ eine Körpererweiterung. Da $\mathbb{C}$ ein Vektorraum der Dimension 2 über $\mathbb{R}$ ist ($(1, i)$ ist eine Basis), gilt $[\mathbb{C} : \mathbb{R}] = 2$. Die Galoisgruppe enthält die Identität und die komplexe Konjugation. Die Wurzelmenge des Minimalpolynoms $f = X^2 + 1$ ist $\{i, -i\}$. Die Identität bildet diese beiden Elemente wieder auf sich selbst ab, während sie von der komplexen Konjugation permutiert werden. Also ist die Galoisgruppe eingeschränkt auf die Wurzelmenge isomorph zur symmetrischen Gruppe S_2.
- Sei $F = K(x)$, der Körper der rationalen Funktionen ρ über *K*. Dann ist für jede Zahl $a \in K \setminus \{0\}$ die durch $\varphi_a : \rho(x) \mapsto \rho(ax)$ definierte Abbildung ein *K*-Automorphismus. Ist der Körper *K* unendlich, so gibt es unendlich viele dieser Automorphismen und die Galoisgruppe $G = \mathrm{Gal}(F/K)$ ist eine unendliche Gruppe. Ist das Element $a \neq 0$ selbst keine Einheitswurzel, dann ist die von dem Automorphismus φ_a erzeugte Untergruppe von *G* nicht abgeschlossen.
- Der Körper der reellen Zahlen lässt keine nichttrivialen Automorphismen zu, denn seine Anordnung ist eine *algebraische* Invariante: Es ist $r \leq s$ für zwei reelle Zahlen genau dann, wenn $s - r$ ein Quadrat ist. Daher ist der Körper der reellen Zahlen über keinem seiner echten Teilkörper galoissch, dasselbe gilt für den Körper der reellen algebraischen Zahlen.
- Allgemeiner trifft das auf alle euklidischen Körper zu: die Galoisgruppe eines euklidischen Körpers über einem seiner Teilkörper ist immer die triviale Gruppe.

Galoisgruppe eines kubischen Polynoms

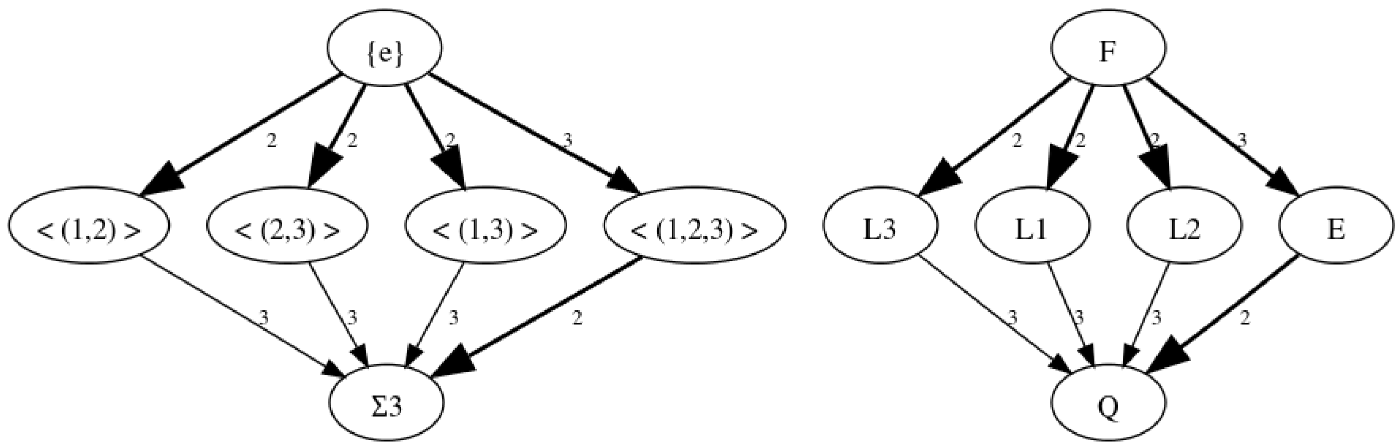
Das folgende, ausführliche Beispiel zeigt am Polynom $f(x) = x^3 - 2$, wie mit Hilfe der Galoisgruppe Zwischenkörper bestimmt werden können.

Der von der reellen Zahl $\xi_1 = \sqrt[3]{2}$ über $\mathbb{Q}$ erzeugte Zahlkörper $L_1 = \mathbb{Q}\left(\sqrt[3]{2}\right)$ hat die Galoisgruppe 1, da keine weiteren Nullstellen des Minimalpolynoms $f(x) = x^3 - 2$ von ξ_1 im (reellen!) Zahlkörper L_1 liegen. Diese Erweiterung ist also nicht galoissch. Ihr Grad ist 3, da L_1 isomorph zu dem Faktorring $\mathbb{Q}(x)/(f)$ ist (siehe Faktorring). Dasselbe gilt für die beiden Zahlkörper $L_2 = \mathbb{Q}(\xi_2)$ und $L_3 = \mathbb{Q}(\xi_3)$, die von den beiden nichtreellen Wurzeln $\xi_2 = \sqrt[3]{2} \cdot \exp\left(\frac{2\pi i}{3}\right)$ und $\xi_3 = \sqrt[3]{2} \cdot \exp\left(\frac{4\pi i}{3}\right)$ von f über $\mathbb{Q}$ erzeugt werden. Alle drei Körper sind isomorphe Zwischenkörper des Zerfällungskörpers F des Polynoms f.

Da der Grundkörper $\mathbb{Q}$ als Körper mit der Charakteristik 0 perfekt ist, ist der gesuchte Zerfällungskörper $F = \mathbb{Q}(\xi_1, \xi_2, \xi_3)$ eine Galoiserweiterung von $\mathbb{Q}$ und die Galoisgruppe G muss transitiv auf den Nullstellen von f operieren. Die einzige echte Untergruppe der symmetrischen Gruppe S_3, die transitiv auf $\{1, 2, 3\}$ operiert, ist der von dem 3-Zyklus $(1, 2, 3)$ erzeugte Normalteiler der S_3, die alternierende Gruppe A_3. Da wir bereits drei echte Zwischenkörper identifiziert haben und die A_3 keine echten Untergruppen hat, kann es sich noch nicht um die volle Galoisgruppe handeln. Diese kann also nur die volle symmetrische Gruppe sein, es gilt also

$$\mathrm{Gal}(F/\mathbb{Q}) = S_3.$$

Neben den Zwischenkörpern, die wir schon identifiziert haben, muss noch ein normaler Zwischenkörper E vorhanden sein, der zweidimensional über $\mathbb{Q}$ ist (Index von A_3). Dieser bleibt fix unter zyklischen Vertauschungen der Nullstellen, das trifft nur auf den Kreisteilungskörper der dritten Einheitswurzeln zu, der durch die Einheitswurzel $\omega = \exp\left(\frac{2\pi i}{3}\right) = \frac{\xi_2}{\xi_1} = \frac{\xi_3}{\xi_2} = \frac{\xi_1}{\xi_3}$ erzeugt wird. Alle Ergebnisse werden in dem Diagramm unten gezeigt.



Untergruppenverband der Galoisgruppe und Zwischenkörperverband der Körpererweiterung F im Beispiel. Die Pfeile im linken Diagramm sind als „ist Untergruppe von“ (dünn) bzw. „ist Normalteiler von“ (dick) zu lesen, im rechten Diagramm als „ist Erweiterung von“ (dünn) bzw. „ist Galoiserweiterung von“ (dick). Die Zahlen an den Pfeilen bedeuten im linken Diagramm relative Indizes, im rechten Diagramm die relative Dimension der Erweiterung. Schiebt man die beiden Graphen übereinander, so kommen die Objekte aufeinander zu liegen, die einander bei der Galoiskorrespondenz entsprechen. So wird z. B. der reelle Körper L1 durch die Gruppe <(2,3)> fixiert, der erzeugende Automorphismus, der die beiden nichtreellen Wurzeln von *f* vertauscht, ist auf *F* die Einschränkung der komplexen Konjugation.

Die Zwischenkörper können nun unter anderem dazu verwendet werden, verschiedene Darstellungen des Zerfällungskörpers zu gewinnen:

- $F = \mathbb{Q}(\xi_1, \xi_2, \xi_3)$, dies folgt – ganz ohne Galoistheorie – aus seiner Definition als Zerfällungskörper
- $F = \mathbb{Q}(\xi_1, \xi_2)$: Dass zwei Nullstellen zur Erzeugung genügen, folgt aus der Tatsache, dass zwischen den Körpern, die durch eine Nullstelle erzeugt werden und F keine weiteren Körper liegen.

- $F = E(\xi_1) = \mathbb{Q}(\omega, \xi_1)$: Hier wird die (in diesem Fall einzige maximale) Subnormalreihe der Galoisgruppe nachgebildet (in der Graphik der Pfad rechts außen). Die relativen Erweiterungen in $\mathbb{Q} \subset E \subset E(\xi_1)$ sind alle galoissch und ihre Galoisgruppen sind einfache abelsche Gruppen.
- F lässt sich auch als einfache Körpererweiterung darstellen: $\omega + \xi_1$ ist sicher ein Element von F und wird von keinem nichttrivialen Element der Galoisgruppe fixiert. Daher ist $F = \mathbb{Q}(\omega + \xi_1)$.

Natürlich können in allen genannten Darstellungen die Nullstellen ξ_k beliebig ausgetauscht werden.

Literatur

- Thomas W. Hungerford: *Algebra*. 5. Auflage. Springer, 1989, ISBN 0-387-90518-9.

Abgerufen von „https://de.wikipedia.org/w/index.php?title=Galoisgruppe&oldid=158551088"

Diese Seite wurde zuletzt am 7. Oktober 2016 um 16:39 Uhr bearbeitet.

Der Text ist unter der Lizenz „Creative Commons Attribution/Share Alike" verfügbar; Informationen zu den Urhebern und zum Lizenzstatus eingebundener Mediendateien (etwa Bilder oder Videos) können im Regelfall durch Anklicken dieser abgerufen werden. Möglicherweise unterliegen die Inhalte jeweils zusätzlichen Bedingungen. Durch die Nutzung dieser Website erklären Sie sich mit den Nutzungsbedingungen und der Datenschutzrichtlinie einverstanden.
Wikipedia® ist eine eingetragene Marke der Wikimedia Foundation Inc.