Zum Satz über das primitive Element

Der abstrakte Satz lautet:

Satz. *Sei $L|K$ eine endliche und separable Körpererweiterung. Dann gibt es ein sog.* primitives Element $z \in L$ *mit*

$$L = K(z).$$

Dass dieser Satz stimmt, ist sehr erstaunlich: Wenn die Voraussetzungen erfüllt sind, kann man also gegebene Erzeuger einer Körpererweiterung stets durch ein einzelnes bestimmtes Element ersetzen.

Beispiele:

1. Da $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$, ist $\sqrt{2}$ ein primitives Element für die Körpererweiterung $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) \mid \mathbb{Q}$.
2. Da $\mathbb{Q}(\sqrt{2}, \mathrm{i}) = \mathbb{Q}(\sqrt{2} + \mathrm{i})$, ist $\sqrt{2} + \mathrm{i}$ ein primitives Elment für die Erweiterung $\mathbb{Q}(\sqrt{2}, \mathrm{i}) \mid \mathbb{Q}$.

Anwendungen

Der Satz vom primitiven Element ist für die Theorie sehr wichtig. Beispielsweise wird er für die Beweise folgender Sätze genutzt:

- Hauptsatz der Galoistheorie
- Zu jeder endlichen und separablen Erweiterung $E|K$ lässt sich ein Oberkörper $L \supseteq E \supseteq K$ finden, sodass $L|K$ normal ist. (Übungsaufgabe!)

Arturoverfahren zur Bestimmung eines primitiven Elements

Sei eine endliche und separable Körpererweiterung $L|K$ gegeben. Wenn man schon die Galoisgruppe G der Erweiterung kennt, kann man folgende Schritte durchführen, um ein primitives Element zu finden:

1. Zunächst rät man ein Element $z \in L$ von dem man hofft, dass $L = K(z)$ gelten könnte.

   Wenn $L = K(x, y)$, sollte man $z := x + y$ und dann $z := x + 2y$ versuchen.
2. Dann bestimmt man die Anzahl der Element der Menge

   $$H := \{\sigma(z) \mid \sigma \in G\}.$$

   Das ist nicht ganz einfach, weil man Teilergebnissen $\sigma_1(z), \sigma_2(z)$ nicht ansieht, ob sie gleich oder verschieden sind. Dazu schreibt man die Ergebnisse am besten in einer K-Basis von L aus, dann genügt es, Koeffizienten zu vergleichen.
3. Wenn $|H| = [L : K]$, ist z in der Tat ein primitives Element. Falls aber $|H| < [L : K]$, war die Vermutung leider falsch. Der Fall $|H| > [L : K]$ kann nicht eintreten.

Beispiel

Sei $L := \mathbb{Q}(\sqrt{2}, \mathrm{i})$ über $K := \mathbb{Q}$. Die zugehörige Galoisgruppe haben wir in einer Beispielrechnung zum Hauptsatz der Galoistheorie schonmal berechnet; wir halten uns an die Notation von dort.

1. Vermutung: $z := \sqrt{2} + \mathrm{i}$
2. $H := \{\sigma_1(z), \dots, \sigma_4(z)\} = \{\sqrt{2} + \mathrm{i},\ \sqrt{2} - \mathrm{i},\ -\sqrt{2} + \mathrm{i},\ -\sqrt{2} - \mathrm{i}\}$

   Da $1, \sqrt{2}, \mathrm{i}, \sqrt{2}\,\mathrm{i}$ eine $\mathbb{Q}$-Basis von L ist, sind diese vier Elemente in der Tat verschieden.
3. Da $[L : K] = 4 = |H|$, ist also z in der Tat ein primitives Element.