

Erweiterungen der rationalen Zahlen

Vereinfachung der Beschreibung durch Erzeuger

Folgende Regeln kann man verwenden, um Darstellungen von Erweiterungen der Form

$$\mathbb{Q}(x_1, \dots, x_n)$$

zu vereinfachen (wieso gelten die Regeln?):

- Die Reihenfolge der Erzeuger (damit sind die x_i gemeint) spielt keine Rolle.
- Erzeuger, die in \mathbb{Q} liegen, kann man weglassen.
- Man kann beliebige Elemente aus \mathbb{Q} zu Erzeugern addieren und subtrahieren, sowie (falls nicht null) multiplizieren und dividieren.
- Man kann beliebige \mathbb{Q} -Vielfache eines Erzeugers auf einen anderen addieren und subtrahieren, sowieso (falls nicht null) multiplizieren und dividieren.

Beispiele

- $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$
- $\mathbb{Q}(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}) = \mathbb{Q}(1 + \sqrt{5}, 1 - \sqrt{5}) = \mathbb{Q}(\sqrt{5}, -\sqrt{5}) = \mathbb{Q}(\sqrt{5})$
- $\mathbb{Q}(\zeta^0, \zeta^1, \dots, \zeta^5) = \mathbb{Q}(\zeta) = \mathbb{Q}(1 + \sqrt{3}i) = \mathbb{Q}(\sqrt{3}i),$
für $\zeta := e^{2\pi i/6} = \cos 60^\circ + i \sin 60^\circ = \frac{1}{2}(1 + \sqrt{3}i).$
- $\mathbb{Q}(\sqrt{3})(\zeta^0, \dots, \zeta^5) = \mathbb{Q}(\sqrt{3})(\sqrt{3}i) = \mathbb{Q}(\sqrt{3}, \sqrt{3}i) = \mathbb{Q}(\sqrt{3}, i),$
für ζ wie in Beispiel 3.
- $\mathbb{Q}(\sqrt[8]{2}\zeta^0, \dots, \sqrt[8]{2}\zeta^7) = \mathbb{Q}(\sqrt[8]{2}, \zeta, \zeta^2, \dots, \zeta^7) = \mathbb{Q}(\sqrt[8]{2}, \zeta) = \mathbb{Q}(\sqrt[8]{2}, 1 + i) = \mathbb{Q}(\sqrt[8]{2}, i),$
für $\zeta := e^{2\pi i/8} = \frac{1}{\sqrt{2}}(1 + i).$
- $\mathbb{Q}(\text{alle sechs Nullstellen von } (X^4 - 2)(X^2 + 1)) = \mathbb{Q}(\sqrt[4]{2}, i)$

Anwendungen

Die Darstellung zu vereinfachen ist hilfreich, wenn man...

- ...den Grad einer Körpererweiterung bestimmen möchte.

Beispiel: Die Erweiterung von Beispiel 3 hat über \mathbb{Q} den Grad 2, denn das Minimalpolynom von $\sqrt{3}i$ über \mathbb{Q} ist $X^2 + 3$ (wieso?). In der Ausgangsformulierung $\mathbb{Q}(\zeta^0, \zeta^1, \dots, \zeta^5)$ erkennt man den Grad dagegen nicht so schnell.

- ...Erweiterungen von \mathbb{Q} in knapper Form angeben möchte.
- ...primitive Elemente bestimmen möchte.

Beispiel: Ein primitives Element für die Zahlen ζ^0, \dots, ζ^5 aus Beispiel 3 ist $\sqrt{3}i$. Dank der Vereinfachungsregeln sieht man das ganz mühelos, ohne langwierige wiederholte Anwendung des Verfahrens aus der Vorlesung.

- ...Galoisgruppen bestimmen möchte (denn dazu benötigt man ja diese Dinge).

Nachweis von Rechenbereichsinklusionen

Seien F und \tilde{F} beliebige weitere Erweiterungen von \mathbb{Q} . Dann gilt (wieso?):

- a) $\mathbb{Q}(x_1, \dots, x_n)(y_1, \dots, y_m) = \mathbb{Q}(x_1, \dots, x_n, y_1, \dots, y_m)$
- b) $\mathbb{Q}(x_1, \dots, x_n) \subseteq F$ genau dann, wenn $x_1, \dots, x_n \in F$.
- c) $\mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_1)$ genau dann, wenn $x_2 \in \mathbb{Q}(x_1)$.
- d) Gelte $F \subseteq \tilde{F}$. Dann gilt genau dann $F = \tilde{F}$, wenn $[F : \mathbb{Q}] = [\tilde{F} : \mathbb{Q}]$.

Ohne die Zusatzvoraussetzung $F \subseteq \tilde{F}$ ist das Quatsch!

Im Allgemeinen gilt nicht, dass $\mathbb{Q}(x, y) = \mathbb{Q}(x + y)$.

Gradbestimmung

- a) Seien w und u algebraische Zahlen. Dann gilt

$$\begin{aligned} \deg_{\mathbb{Q}(u)} w &= \text{Grad von } w \text{ über } \mathbb{Q}(u) \\ &= \text{Grad des Minimalpolynoms von } w \text{ über } \mathbb{Q}(u) \\ &= [\mathbb{Q}(u, w) : \mathbb{Q}(u)]. \end{aligned}$$

Falls außerdem $u \in \mathbb{Q}(w)$ gelten sollte, gilt ferner $\mathbb{Q}(u, w) = \mathbb{Q}(w)$, sodass man in diesem Fall die Formel noch weiter vereinfachen kann:

$$= [\mathbb{Q}(w) : \mathbb{Q}(u)].$$

Für den Grad über \mathbb{Q} folgt daraus (mit $u := 1$):

$$\deg_{\mathbb{Q}} w = (\text{Grad des Minimalpolynoms von } w \text{ über } \mathbb{Q}) = [\mathbb{Q}(w) : \mathbb{Q}].$$

- b) Gelte $F \subseteq F' \subseteq F''$. Dann gilt die *Gradformel*:

$$[F'' : F] = [F'' : F'] \cdot [F' : F].$$

- c) Verbindung zur Galoistheorie: Sind x_1, \dots, x_n die Nullstellen eines normierten separablen Polynoms mit rationalen Koeffizienten und ist t ein primitives Element für diese Nullstellen, so gilt $[\mathbb{Q}(x_1, \dots, x_n) : \mathbb{Q}] = [\mathbb{Q}(t) : \mathbb{Q}] = |\text{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)|$. Dies folgt aus fundamentalen 1:1-Korrespondenz zwischen den Elementen der Galoisgruppe und den galoissch Konjugierten von t (Proposition 4.8).