Erweiterungen der rationalen Zahlen

Vereinfachung der Beschreibung durch Erzeuger

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

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

zu vereinfachen (wieso gelten die Regeln?):

a) Die Reihenfolge der Erzeuger (damit sind die x_i gemeint) spielt keine Rolle.

b) Erzeuger, die in $\mathbb{Q}$ liegen, kann man weglassen.

c) Man kann beliebige Elemente aus $\mathbb{Q}$ zu Erzeugern addieren und subtrahieren, sowie (falls nicht null) multiplizieren und dividieren.

d) Man kann beliebige $\mathbb{Q}$-Vielfache eines Erzeugers auf einen anderen addieren und subtrahieren, sowieso (falls nicht null) multiplizieren und dividieren.

Beispiele

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

Anwendungen

Die Darstellung zu vereinfachen ist hilfreich, wenn man…

- …Erweiterungen von $\mathbb{Q}$ in knapper Form angeben möchte.
- …den Grad einer Erweiterung bestimmen möchte.

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

  Beispiel: Ein primitives Element für die Zahlen $\zeta^0, \ldots, \zeta^5$ aus Beispiel 3 ist $\sqrt{3}\,\mathrm{i}$. 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 $\widetilde{F}$ 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) $\mathbb{Q}[x] = \mathbb{Q}(x)$ genau dann, wenn x algebraisch ist.

c) $\mathbb{Q}(x_1, \dots, x_n) \subseteq F$ genau dann, wenn $x_1, \dots, x_n \in F$.

d) $\mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_1)$ genau dann, wenn $x_2 \in \mathbb{Q}(x_1)$ (wie folgt das aus c)?).

e) Gelte $F \subseteq \widetilde{F}$. Dann gilt genau dann $F = \widetilde{F}$, wenn $[F : \mathbb{Q}] = [\widetilde{F} : \mathbb{Q}]$.
Ohne die Zusatzvoraussetzung $F \subseteq \widetilde{F}$ 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 $[\mathbb{Q}(x_1, \dots, x_n) : \mathbb{Q}] = [\mathbb{Q}(t) : \mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}}(x_1, \dots, x_n)|$. Dies folgt aus der fundamentalen 1:1–Korrespondenz zwischen den Elementen der Galoisgruppe und den galoissch Konjugierten von t (Proposition 4.8).

Basen

Eine mögliche $\mathbb{Q}$-Basis der Erweiterung $\mathbb{Q}(\alpha)$ ist durch

$$1, \quad \alpha, \quad \alpha^2, \quad \dots, \quad \alpha^{n-1}$$

gegeben, wobei n der Grad von α sei. Ausbuchstabiert bedeutet das: *Jede* Zahl aus $\mathbb{Q}(\alpha)$ lässt sich auf *eindeutige* Art und Weise als rationale Linearkombination in den Zahlen $\alpha^0, \dots, \alpha^{n-1}$ schreiben.

Beispiel: Der Grad von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist 3 (wieso?). Daher gibt es für jede Zahl x aus $\mathbb{Q}(\sqrt[3]{2})$ genau einen Satz von rationalen Koeffizienten a, b, c mit

$$x = a \cdot 1 + b \cdot \sqrt[3]{2} + c \cdot \sqrt[3]{2}^2.$$