

## Übungsblatt 9 zur Algebra I

Abgabe bis 17. Juni 2013, 17:00 Uhr

### Aufgabe 1. Linearkombinationen

- Sei  $x$  eine Lösung der Gleichung  $X^4 - 3X^3 + 10X - 10 = 0$ . Drücke  $x^6$  als Linearkombination der Zahlen  $1, x, x^2, x^3$  mit rationalen Koeffizienten aus.
- Sei  $z := \sqrt{5} + \sqrt[3]{5}$  gegeben. Gib eine natürliche Zahl  $n$  und eine verschwindende nichttriviale Linearkombination von  $1, z, z^2, \dots, z^n$  mit rationalen Koeffizienten an.
- Finde zwei komplexe Zahlen, die über  $\mathbb{R}$  linear unabhängig und über  $\mathbb{C}$  linear abhängig sind.

### Lösung.

- Variante 1:* Wir rechnen unter Verwendung der Beziehung  $x^4 = 3x^3 - 10x + 10$ :

$$\begin{aligned}
 x^6 &= x^4 x^2 = (3x^3 - 10x + 10)x^2 \\
 &= 3x^4 x - 10x^3 + 10x^2 \\
 &= 3 \cdot (3x^3 - 10x + 10)x - 10x^3 + 10x^2 \\
 &= 9x^4 - 30x^2 + 30x - 10x^3 + 10x^2 \\
 &= 9 \cdot (3x^3 - 10x + 10) - 30x^2 + 30x - 10x^3 + 10x^2 \\
 &= 27x^3 - 90x + 90 - 30x^2 + 30x - 10x^3 + 10x^2 \\
 &= 17x^3 - 20x^2 - 60x + 90
 \end{aligned}$$

*Variante 2:* Wir führen in einem Schritt eine Polynomdivision durch:

$$X^6 = (X^4 - 3X^3 + 10X - 10) \cdot (X^2 + 3X + 9) + (17X^3 - 20X^2 - 60X + 90).$$

Setzt man nun  $x$  für  $X$  ein, erhält man dasselbe Ergebnis, da die erste Klammer verschwindet.

- Wir rechnen:

$$\begin{aligned}
 &z = \sqrt{5} + \sqrt[3]{5} \\
 \iff &\sqrt[3]{5} = z - \sqrt{5} \\
 \implies &5 = (z - \sqrt{5})^3 \\
 \iff &5 = z^3 - 3\sqrt{5}z^2 + 15z - 5\sqrt{5} \\
 \iff &5 - 15z - z^3 = -\sqrt{5} \cdot (5 + 3z^2) \\
 \implies &(5 - 15z - z^3)^2 = 5 \cdot (25 + 30z^2 + 9z^4) \\
 \iff &0 = z^6 - 15z^4 - 10z^3 + 75z^2 - 150z - 100
 \end{aligned}$$

Also können wir etwa  $n = 6$  setzen, die gesuchte nichttriviale und trotzdem verschwindende Linearkombination steht schon da.

*Bemerkung:* Tatsächlich ist der Ausdruck in der letzten Zeile (wenn man „ $X$ “ statt „ $z$ “ schreibt) schon das Minimalpolynom von  $z$  über  $\mathbb{Q}$ . Schmerzlos kann man durch eine schnelle Gradüberlegung erkennen: Da die Grade von  $\sqrt{5}$  und  $\sqrt[3]{5}$  teilerfremd sind (sie sind 2 bzw. 3), ist der Grad von  $\mathbb{Q}(\sqrt{5}, \sqrt[3]{5})$  gerade durch das Produkt der Grade, also durch  $2 \cdot 3 = 6$  gegeben; und  $z$  ist gerade ein primitives Element für diese Erweiterung.

- c) Zum Beispiel 1 und  $i$ : Diese sind über  $\mathbb{R}$  sicherlich linear unabhängig, denn für reelle Zahlen  $a, b \in \mathbb{R}$  folgt aus

$$a \cdot 1 + b \cdot i = 0$$

sofort  $a = b = 0$ , da eine komplexe Zahl genau dann null ist, wenn ihr Real- und Imaginärteil null sind. Dagegen bezeugt die verschwindende und trotzdem nichttriviale Linearkombination

$$i \cdot 1 + (-1) \cdot i = 0,$$

dass die beiden Zahlen über  $\mathbb{C}$  linear abhängig sind.

*Bemerkung:* Letzteres muss auch so sein, denn  $\mathbb{C}$  ist als  $\mathbb{C}$ -Vektorraum nur eindimensional.

## Aufgabe 2. Grade algebraischer Zahlen

- Berechne den Grad von  $\sqrt{3} + i$  über  $\mathbb{Q}$ , über  $\mathbb{Q}(\sqrt{3})$  und über  $\mathbb{Q}(i)$ .
- Finde ein Polynom mit rationalen Koeffizienten, das über  $\mathbb{Q}$  irreduzibel ist, über  $\mathbb{Q}(\sqrt{3})$  in genau zwei und über  $\mathbb{Q}(\sqrt{3} + i)$  in genau vier irreduzible Polynome zerfällt.
- Seien  $a$  und  $d$  ganze Zahlen. Zeige, dass  $a + \sqrt{d}$  eine ganz algebraische Zahl ist und berechne ihren Grad in Abhängigkeit von  $a$  und  $d$ .
- Sei  $\zeta$  eine Lösung der Polynomgleichung  $X^4 + X^3 + X^2 + X + 1 = 0$ . Zeige, dass  $\zeta$  eine in  $\alpha := \exp(\pi i/5)$  rationale Zahl ist, und gib eine Basis von  $\mathbb{Q}(\alpha)$  über  $\mathbb{Q}(\zeta)$  an.

## Lösung.

- a) *Variante 1 (direkt, etwas länglich):* Sei  $z := \sqrt{3} + i$ . Wir wollen zunächst den Grad von  $z$  über  $\mathbb{Q}(\sqrt{3})$  bestimmen. Dazu suchen wir das Minimalpolynom:

$$\begin{aligned} z &= \sqrt{3} + i \\ \iff z - \sqrt{3} &= i \\ \implies (z - \sqrt{3})^2 &= -1 \\ \iff z^2 - 2\sqrt{3}z + 4 &= 0 \end{aligned}$$

Das Polynom  $X^2 - 2\sqrt{3}X + 4$  ist tatsächlich über  $\mathbb{Q}(\sqrt{3})$  irreduzibel: Es hat Grad 2 und seine Nullstellen  $\sqrt{3} \pm i$  sind echt komplex und liegen daher nicht in  $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ . Also ist es das Minimalpolynom von  $z$  über  $\mathbb{Q}(\sqrt{3})$ ; der Grad von  $z$  über  $\mathbb{Q}(\sqrt{3})$  ist also 2.

Nun wollen wir das Minimalpolynom über  $\mathbb{Q}(i)$  bestimmen. Dazu rechnen wir:

$$\begin{aligned} z &= \sqrt{3} + i \\ \iff z - i &= \sqrt{3} \\ \implies (z - i)^2 &= 3 \\ \iff z^2 - 2iz - 4 &= 0 \end{aligned}$$

Das Polynom  $X^2 - 2iX - 4$  ist tatsächlich über  $\mathbb{Q}(i)$  irreduzibel: Es hat Grad 2 und seine Nullstellen  $\pm\sqrt{3} + i$  liegen nicht in  $\mathbb{Q}(i)$ : Wenn doch, läge auch  $\sqrt{3}$  in  $\mathbb{Q}(i)$  (wieso?), also gäbe es rationale Zahlen  $a, b \in \mathbb{Q}$  mit  $\sqrt{3} = a + bi$ . Realteilvergleich würde dann  $\sqrt{3} = a \in \mathbb{Q}$  liefern, ein Widerspruch. Also ist das Polynom tatsächlich das Minimalpolynom von  $z$  über  $\mathbb{Q}(i)$ ; der Grad von  $z$  über  $\mathbb{Q}(i)$  ist also 2.

Nun bleibt es, den Grad von  $z$  über  $\mathbb{Q}$  zu bestimmen. Dazu müssen wir unsere Rechnungen fortsetzen:

$$\begin{array}{rcl}
 & & z = \sqrt{3} + i \\
 \implies & & z^2 - 2iz - 4 = 0 \\
 \iff & & z^2 - 4 = 2iz \\
 \implies & & (z^2 - 4)^2 = -4z^2 \\
 \iff & & z^4 - 4z^2 + 16 = 0
 \end{array}$$

Nun kann man nachrechnen, dass das Polynom  $X^4 - 4X^2 + 16$  tatsächlich über den rationalen Zahlen irreduzibel ist. Das gelingt etwa über unseren numerischen Irreduzibilitätstest. Ist das getan, folgt, dass der Grad von  $z$  über  $\mathbb{Q}$  genau 4 ist.

*Variante 2 (schneller mit der Gradformel):* Sei  $z := \sqrt{3} + i$ . Die Zahl  $\sqrt{3}$  liegt in  $\mathbb{Q}(z)$ . Das kann man durch kurzes Knobeln erkennen (es gilt  $\sqrt{3} = z - z^3/8$ ) oder auch daran, dass nach dem Verfahren der Vorlesung  $z$  ein primitives Element von  $\sqrt{3}$  und  $i$  ist (die Ausnahmemenge  $S$  enthält nur 0 und  $\sqrt{3} \cdot i$ ) und daher sogar  $\mathbb{Q}(z) = \mathbb{Q}(\sqrt{3}, i)$  gilt.

Auf jeden Fall liegt daher der Rechenbereich  $\mathbb{Q}(\sqrt{3})$  in  $\mathbb{Q}(z)$  und wir können das Diagramm

$$\begin{array}{c}
 \mathbb{Q}(\sqrt{3} + i) \\
 | \\
 \mathbb{Q}(\sqrt{3}) \\
 | \\
 \mathbb{Q}
 \end{array}$$

zeichnen. Nach der Gradformel gilt also

$$[\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

Wie die erste Rechnung in Variante 1 gezeigt hat, ist der erste Faktor auf der rechten Seite gleich 2, und vom zweiten Faktor weiß man sowieso, dass er gleich 2 ist (Minimalpolynom ist  $X^2 - 3$ ). Folglich ist der Grad von  $z$  über  $\mathbb{Q}$  gleich 4.

Bleibt, den Grad von  $z$  über  $\mathbb{Q}(i)$  zu bestimmen. Da  $\mathbb{Q}(i) \subseteq \mathbb{Q}(z)$  (da  $i = z^3/8$ ), können wir dafür das Diagramm

$$\begin{array}{c}
 \mathbb{Q}(\sqrt{3} + i) \\
 | \\
 \mathbb{Q}(\sqrt{i}) \\
 | \\
 \mathbb{Q}
 \end{array}$$

zeichnen und daher die Gradformel verwenden:

$$[\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}(\sqrt{i})] \cdot [\mathbb{Q}(\sqrt{i}) : \mathbb{Q}].$$

Gesucht ist der erste Faktor auf der rechten Seite, die anderen Terme kennen wir. Aufgelöst ergibt sich  $[\mathbb{Q}(\sqrt{3} + i) : \mathbb{Q}(\sqrt{i})] = \deg_{\mathbb{Q}(i)} z = 2$ .

*Bemerkung:* Die beiden Varianten kann man auf mehrere Arten und Weisen miteinander kombinieren.

- b) Von dem Polynom  $f(X) = X^4 - 4X^2 + 16 \in \mathbb{Q}[X]$  haben wir schon gesehen, dass es über  $\mathbb{Q}$  irreduzibel ist. Seine vier Nullstellen sind die Zahlen

$$x_1 = \sqrt{3} + i, \quad x_2 = \sqrt{3} - i, \quad x_3 = -\sqrt{3} + i, \quad x_4 = -\sqrt{3} - i,$$

welche alle in  $\mathbb{Q}(\sqrt{3} + i)$  liegen, da  $\sqrt{3} + i$  ein primitives Element für  $\mathbb{Q}(\sqrt{3}, i)$  ist. Also zerfällt  $f(X)$  über  $\mathbb{Q}(\sqrt{3} + i)$  in die vier Linearfaktoren

$$f(X) = (X - x_1) \cdot (X - x_2) \cdot (X - x_3) \cdot (X - x_4).$$

Über  $\mathbb{Q}(\sqrt{3})$  erhalten wir die Zerlegung

$$f(X) = (X - x_1)(X - x_2) \cdot (X - x_3)(X - x_4) = (X^2 - 2\sqrt{3}X + 4) \cdot (X^2 + 2\sqrt{3}X + 4).$$

Dabei sind die beiden auftretenden Faktoren sicherlich über  $\mathbb{Q}(\sqrt{3})$  irreduzibel, da sie vom Grad 2 sind und ihre Nullstellen nicht in  $\mathbb{Q}(\sqrt{3})$  liegen, da sie echt komplex sind, aber  $\mathbb{Q}(\sqrt{3})$  nur reelle Zahlen enthält.

- c) Wir setzen  $z := a + \sqrt{d}$  und rechnen:

$$\begin{aligned} z &= a + \sqrt{d} \\ \iff z - a &= \sqrt{d} \\ \implies (z - a)^2 &= d \\ \iff z^2 - 2az + a^2 - d &= 0 \end{aligned}$$

Die Zahl  $z$  ist also als Lösung der Polynomgleichung  $X^2 - 2aX + a^2 - d = 0$  mit ganzzahligen Koeffizienten ganz algebraisch. Außerdem ist damit klar, dass der Grad von  $z$  höchstens 2 ist. Er ist genau dann 1, wenn dieses Polynom reduzibel ist. Das ist genau dann der Fall, wenn eine seiner beiden Nullstellen, etwa  $z$ , schon ganzzahlig ist. Das wiederum ist genau dann der Fall, wenn  $\sqrt{d}$  in  $\mathbb{Z}$  liegt; das ist äquivalent dazu, dass  $d$  eine Quadratzahl ist.

- d) Nach Aufgabe 4c) von Blatt 3 ist  $\zeta$  eine fünfte Einheitswurzel (aber nicht die 1). Insbesondere ist  $\zeta$  damit auch eine zehnte Einheitswurzel (denn  $\zeta^{10} = (\zeta^5)^2 = 1^2 = 1$ ). Die Zahl  $\alpha = \exp(\pi i/5) = \exp(2\pi i/10)$  ist eine primitive zehnte Einheitswurzel, daher muss es einen Exponent  $k \in \mathbb{Z}$  mit  $\alpha^k = \zeta$  geben. Also ist  $\zeta$  in  $\alpha$  rational, d. h. es gilt  $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\alpha)$ .

Umgekehrt gilt auch  $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta)$ : Die Zahl  $(-\zeta)$  ist nämlich eine primitive zehnte Einheitswurzel (siehe unten). Da  $\alpha$  (irgend-)eine zehnte Einheitswurzel ist, gibt es daher einen Exponent  $\ell \in \mathbb{Z}$  mit  $(-\zeta)^\ell = \alpha$ . Also ist  $\alpha$  in  $\zeta$  rational, d. h. es gilt  $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta)$ .

Zusammengenommen gilt somit  $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$ . Daher ist der Grad der Erweiterung 1 und eine mögliche Basis ist durch die Familie (1) der Länge 1 gegeben.

Nun müssen wir noch zu begründen, wieso  $(-\zeta)$  eine primitive zehnte Einheitswurzel ist. Klar ist zumindest, dass  $(-\zeta)$  überhaupt eine zehnte Einheitswurzel ist, denn es gilt  $(-\zeta)^{10} = \zeta^{10} = (\zeta^5)^2 = 1$ . Um die Primitivität nachzuweisen, zeigen wir, dass  $(-\zeta)^j$  erst für  $j = 10$  (und nicht schon für  $j = 1, 2, \dots, 9$ ) wieder 1 ist:

Gelte  $(-\zeta)^j = (-1)^j \zeta^j = 1$ , also  $\zeta^j = (-1)^j$ . Dann kann  $j$  nicht ungerade sein, denn dann gälte  $\zeta^j = -1$ , aber  $(-1)$  ist keine fünfte Einheitswurzel. Also ist  $j$  gerade und es gilt  $\zeta^j = 1$ . Da  $\zeta$  eine *primitive* fünfte Einheitswurzel ist, muss  $j$  ein Vielfaches von 5 sein. Da es außerdem gerade ist, muss  $j$  sogar ein Vielfaches von 10 sein.

*Variante für den zweiten Teil, wenn man Kreisteilungspolynome kennt:* Wir wollen zeigen, dass  $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta)$ . Da sicher die Inklusion „ $\supseteq$ “ gilt, genügt es zu zeigen, dass beide Vektorräume dieselbe Dimension über  $\mathbb{Q}$  haben, dass also  $\deg_{\mathbb{Q}} \alpha = \deg_{\mathbb{Q}} \zeta$  gilt. Das Minimalpolynom von  $\zeta$  ist das fünfte Kreisteilungspolynom,  $\Phi_5 = X^4 + X^3 + X^2 + X + 1$ , das

von  $\alpha$  ist das zehnte Kreisteilungspolynom,  $\Phi_{10} = X^4 - X^3 + X^2 - X + 1$ . Also haben beide Zahlen in der Tat denselben Grad, nämlich 4.

*Explizite Variante für beide Teile:* Wir gehen alle vier Möglichkeiten für  $\zeta$  durch und drücken jeweils  $\zeta$  durch  $\alpha$  und umgekehrt  $\alpha$  durch  $\zeta$  aus:

$$\begin{array}{lll} \zeta = \exp(2\pi i/5), \text{ dann:} & \zeta = \alpha^2, & \alpha = -\zeta^3. \\ \zeta = \exp(4\pi i/5), \text{ dann:} & \zeta = \alpha^4, & \alpha = -\zeta^4. \\ \zeta = \exp(6\pi i/5), \text{ dann:} & \zeta = \alpha^6, & \alpha = -\zeta. \\ \zeta = \exp(8\pi i/5), \text{ dann:} & \zeta = \alpha^8, & \alpha = -\zeta^2. \end{array}$$

In jedem Fall gilt also  $\mathbb{Q}(\zeta) = \mathbb{Q}(\alpha)$ , eine Basis ist also durch (1) gegeben.

### Aufgabe 3. Spiel und Spaß mit der Gradformel

- Seien  $x \in \overline{\mathbb{Q}}$ ,  $y \in \mathbb{Q}(x)$  und  $z \in \mathbb{Q}(y)$ . Wie lässt sich  $\deg_{\mathbb{Q}(z)} x$  aus  $\deg_{\mathbb{Q}(y)} x$  und  $\deg_{\mathbb{Q}(z)} y$  berechnen?
- Seien  $x, y, z$  wie in a). Zeige, dass  $\deg_{\mathbb{Q}(z)} y$  ein Teiler von  $\deg_{\mathbb{Q}(z)} x$  ist.
- Sei  $f$  ein normiertes und irreduzibles Polynom vom Grad  $\geq 2$  mit rationalen Koeffizienten. Sei  $a$  eine algebraische Zahl, deren Grad teilerfremd zum Grad von  $f$  ist. Zeige, dass keine Zahl aus  $\mathbb{Q}(a)$  Nullstelle von  $f$  sein kann.

### Lösung.

- Da  $\mathbb{Q}(z) \subseteq \mathbb{Q}(y) \subseteq \mathbb{Q}(x)$ , ist die Gradformel anwendbar:

$$\deg_{\mathbb{Q}(z)} x = [\mathbb{Q}(x) : \mathbb{Q}(z)] = [\mathbb{Q}(x) : \mathbb{Q}(y)] \cdot [\mathbb{Q}(y) : \mathbb{Q}(z)] = \deg_{\mathbb{Q}(y)} x \cdot \deg_{\mathbb{Q}(z)} y.$$

Auf diese Weise lässt sich also der gesuchte Grad berechnen.

- Folgt sofort aus der in a) hergeleiteten Beziehung.
- Sei  $w \in \mathbb{Q}(a)$  eine hypothetische Zahl mit  $f(w) = 0$ . Da  $f$  normiert ist, rationale Koeffizienten hat und über den rationalen Zahlen irreduzibel ist, ist  $f$  daher Minimalpolynom von  $z$ , es gilt also  $\deg_{\mathbb{Q}} w = \deg f$ . Somit folgt

$$\deg_{\mathbb{Q}} a = [\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(w)] \cdot [\mathbb{Q}(w) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(w)] \cdot \deg f,$$

also ist der Grad von  $f$  ein Teiler vom Grad von  $a$ . Wegen  $\deg f \geq 2$  ist das ein Widerspruch zur Teilerfremdheitsvoraussetzung.

### Aufgabe 4. Primitive Elemente

- Finde ein primitives Element zu  $i$  und  $\sqrt[3]{2}$ .
- Drücke  $\sqrt{2}$  und  $\sqrt{3}$  als Polynome in  $\sqrt{2} + \sqrt{3}$  mit rationalen Koeffizienten aus.
- Seien  $z_1, \dots, z_n$  algebraische Zahlen. Zeige, dass es eine algebraische Zahl  $z$  mit  $\mathbb{Q}(z) = \mathbb{Q}(z_1, \dots, z_n)$  gibt.
- Sei  $f(X)$  ein Polynom mit rationalen Koeffizienten. Zeige, dass eine algebraische Zahl  $a$  existiert, sodass  $f(X)$  über  $\mathbb{Q}(a)$  vollständig in Linearfaktoren zerfällt.

## Lösung.

- a) *Variante 1 (Verfahren aus der Vorlesung):* Die Minimalpolynome von  $x := i$  und  $y := \sqrt[3]{2}$  sind  $f(X) = X^2 + 1$  bzw.  $g(X) = X^3 - 2$  mit den Nullstellen  $\pm i$  bzw.  $\omega^k \cdot \sqrt[3]{2}$ ,  $k = 0, 1, 2$ . Die Ausnahmemenge  $S$  ist daher gleich

$$\begin{aligned} S &= \left\{ \frac{x' - x}{y - y'} \mid f(x') = 0, g(y') = 0, y \neq y' \right\} \\ &= \left\{ 0, \frac{-2i}{\sqrt[3]{2} - \omega \sqrt[3]{2}}, \frac{-2i}{\sqrt[3]{2} - \omega^2 \sqrt[3]{2}} \right\}. \end{aligned}$$

Näherungsweise ergibt sich

$$\begin{aligned} \frac{-2i}{\sqrt[3]{2} - \omega \sqrt[3]{2}} &\approx 0,46 - 0,79i, \\ \frac{-2i}{\sqrt[3]{2} - \omega^2 \sqrt[3]{2}} &\approx -0,46 - 0,79i, \end{aligned}$$

also ist zum Beispiel die Wahl  $\lambda := 1 \notin S$  erlaubt und  $i + \sqrt[3]{2}$  daher ein primitives Element.

*Variante 2 (durch stundenlanges Knobeln):* Wir vermuten, dass  $z := i + \sqrt[3]{2}$  ein primitives Element ist und wollen diese Vermutung nur noch bestätigen. Klar ist zumindest, dass  $z$  in  $i$  und  $\sqrt[3]{2}$  rational ist, dass also  $\mathbb{Q}(z) \subseteq \mathbb{Q}(i, \sqrt[3]{2})$  gilt. Umgekehrt kann man durch Vergleich verschiedener  $z$ -Potenzen auf die Beziehungen

$$\begin{aligned} i &= -\frac{91}{22} - \frac{39}{11}z + \frac{39}{11}z^2 - \frac{20}{11}z^3 + \frac{9}{22}z^4 - \frac{6}{11}z^5, \\ \sqrt[3]{2} &= \frac{91}{22} + \frac{50}{11}z - \frac{39}{11}z^2 + \frac{20}{11}z^3 - \frac{9}{22}z^4 + \frac{6}{11}z^5 \end{aligned}$$

kommen; diese bezeugen, dass  $\mathbb{Q}(i)$  und  $\mathbb{Q}(\sqrt[3]{2})$  jeweils Teilmengen von  $\mathbb{Q}(z)$  sind.

*Variante 3 (ein anderes primitives Element):* Wir vermuten, dass  $z := i \cdot \sqrt[3]{2}$  ein primitives Element ist. Klar ist zumindest, dass  $z$  in  $i$  und  $\sqrt[3]{2}$  rational ist, dass also  $\mathbb{Q}(z) \subseteq \mathbb{Q}(i, \sqrt[3]{2})$  gilt. Die umgekehrte Inklusion zeigen die Beziehungen

$$\begin{aligned} i &= -z^3/2, \\ \sqrt[3]{2} &= z^4/2. \end{aligned}$$

- b) Sei  $z := \sqrt{2} + \sqrt{3}$ . Dann rechnen wir ein paar  $z$ -Potenzen aus:

$$\begin{aligned} z &= \sqrt{2} + \sqrt{3} \\ z^2 &= 5 + 2\sqrt{6} \\ z^3 &= 11\sqrt{2} + 9\sqrt{3} \end{aligned}$$

Die Darstellung der Potenz  $z^2$  hilft uns nicht weiter, da in ihr nicht nur die Zahlen  $\sqrt{2}$  und  $\sqrt{3}$  vorkommen, sondern auch die für uns nicht weiter relevante Zahl  $\sqrt{6}$ . Aber  $z^1$  und  $z^3$  können wir geeignet gegeneinander ausspielen:

$$\begin{aligned} \sqrt{2} &= (z^3 - 9z)/2 \\ \sqrt{3} &= (z^3 - 11z)/(-2) \end{aligned}$$

*Bemerkung:* Die explizite Rechnung zeigt, dass  $\sqrt{2} + \sqrt{3}$  ein primitives Element für  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  ist: Denn  $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$  gilt sowieso, und die umgekehrte Inklusion gilt gerade deswegen, weil  $\sqrt{2}$  und  $\sqrt{3}$  in  $\sqrt{2} + \sqrt{3}$  rational sind.

- c) Wir führen einen Induktionsbeweis. Der Induktionsanfang  $n = 1$  ist klar. Für den Induktionsschritt  $n \rightarrow n + 1$  seien algebraische Zahlen  $z_1, \dots, z_{n+1}$  gegeben. Nach Induktionsvoraussetzung gibt es dann ein primitives Element der Zahlen  $z_1, \dots, z_n$ , d. h. eine algebraische Zahl  $t$  mit  $\mathbb{Q}(t) = \mathbb{Q}(z_1, \dots, z_n)$ . Ferner können wir ein primitives Element  $t'$  zu  $t$  und  $z_{n+1}$  finden, also eine Zahl mit

$$\mathbb{Q}(t') = \mathbb{Q}(t, z_{n+1}) = \mathbb{Q}(t)(z_{n+1}) = \mathbb{Q}(z_1, \dots, z_n)(z_{n+1}) = \mathbb{Q}(z_1, \dots, z_{n+1}).$$

Das beschließt den Beweis des Induktionsschritts.

- d) Über den algebraischen Zahlen zerfällt  $f$  vollständig in Linearfaktoren:  $f = (X - x_1) \cdots (X - x_n)$ . Etwas genauer zerfällt  $f$  aber auch schon in dem kleineren Rechenbereich  $\mathbb{Q}(x_1, \dots, x_n)$  vollständig in Linearfaktoren. Nach Teilaufgabe c) (anwendbar, da alle  $x_i$  algebraisch) ist dieser von der geforderten Form  $\mathbb{Q}(a)$  für eine geeignete algebraische Zahl  $a$ .

### Aufgabe 5. Irrationale Zahlen für Fortgeschrittene

Zeige mit elementaren Methoden direkt über den Ansatz  $\sqrt{2} = a + b\sqrt{3}$  mit rationalen Zahlen  $a$  und  $b$ , dass  $\sqrt{2}$  kein Element von  $\mathbb{Q}(\sqrt{3})$  ist, also keine in  $\sqrt{3}$  rationale Zahl ist. Welchen Grad hat  $\sqrt{2}$  daher über  $\mathbb{Q}(\sqrt{3})$ ?

**Lösung.** *Variante 1 (über Primfaktoren):* Angenommen,  $\sqrt{2} = a + b\sqrt{3}$  für gewisse rationale Zahlen  $a = x/y$ ,  $b = u/v \in \mathbb{Q}$  mit  $x, y, u, v \in \mathbb{Z}$ . Dann rechnen wir:

$$\begin{aligned} \sqrt{2} &= a + b\sqrt{3} \\ \iff \sqrt{2}yv &= xv + uy\sqrt{3} \\ \implies 2y^2v^2 &= x^2v^2 + 2xyuv\sqrt{3} + 3u^2y^2 \\ \iff 2y^2v^2 - x^2v^2 - 3u^2y^2 &= 2xyuv\sqrt{3} \\ \implies (2y^2v^2 - x^2v^2 - 3u^2y^2)^2 &= 12 \cdot (xyuv)^2 \end{aligned}$$

Auf der linken Seite kommt der Primfaktor 3 eine gerade Anzahl von Malen vor, auf der rechten Seite dagegen eine ungerade Anzahl von Malen (da er in  $(xyuv)^2$  gerade oft und dann noch einmal im Vorfaktor 12 vorkommt), das ist ein Widerspruch.

*Variante 2 (mit Fallunterscheidungen):* Angenommen,  $\sqrt{2} = a + b\sqrt{3}$  für gewisse rationale Zahlen  $a, b \in \mathbb{Q}$ . Dann folgt

$$2 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

Falls  $ab \neq 0$ , ist das ein Widerspruch, denn dann können wir nach  $\sqrt{3}$  auflösen und so als rationale Zahl ausdrücken. Nach Aufgabe 1a) von Blatt 0 ist  $\sqrt{3}$  aber irrational.

Falls  $ab = 0$ , gibt es zwei Unterfälle: Falls  $b = 0$ , gilt  $\sqrt{2} = a \in \mathbb{Q}$  im Widerspruch zur Irrationalität von  $\sqrt{2}$ . Falls  $b \neq 0$ , folgt  $a = 0$  und daher  $\sqrt{2/3} = b \in \mathbb{Q}$ . Das kann aber nicht sein: Ist  $b = x/y$  mit  $x, y \in \mathbb{Z}$ , folgt  $2/3 = x^2/y^2$ , also  $2y^2 = 3x^2$ . In der linken Seite tritt der Primfaktor 2 ungerade oft auf (wieso?), rechts aber gerade oft.

*Variante 3 (mit anderen Fallunterscheidungen):* Angenommen,  $\sqrt{2} = a + b\sqrt{3}$  für gewisse rationale Zahlen  $a, b \in \mathbb{Q}$ . Dann kann man nach  $a$  auflösen, quadrieren und umstellen, sodass

$$2b\sqrt{6} = 2 - 3b^2 - a^2$$

folgt. Falls  $b \neq 0$ , kann man weiter nach  $\sqrt{6}$  auflösen und damit  $\sqrt{6}$  als rational erkennen – ein Widerspruch. Falls  $b = 0$ , folgt direkt aus der Ursprungsgleichung, dass  $\sqrt{2}$  rational ist – ebenfalls ein Widerspruch.

*Folgerung über den Grad:* Wegen  $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$  ist der Grad von  $\sqrt{2}$  über  $\mathbb{Q}(\sqrt{3})$  mehr als 1. (Tatsächlich ist er genau 2, denn das Polynom  $X^2 - 2 \in \mathbb{Q}(\sqrt{3})[X]$  ist ein annullierendes Polynom für  $\sqrt{2}$ .)