Universität Augsburg
Lehrstuhl für Algebra und Zahlentheorie
Prof. Marc Nieper-Wißkirchen

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 9 zur Algebra I

Abgabe bis 17. Juni 2013, 17:00 Uhr

Aufgabe 1. *Linearkombinationen*

a) Sei x eine Lösung der Gleichung $X^4 - 3\,X^3 + 10\,X - 10 = 0$. Drücke x^6 als Linearkombination der Zahlen $1, x, x^2, x^3$ mit rationalen Koeffizienten aus.

b) Sei $z := \sqrt{5} + \sqrt[3]{5}$ gegeben. Gib eine natürliche Zahl n und eine verschwindende nichttriviale Linearkombination von $1, z, z^2, \ldots, z^n$ mit rationalen Koeffizienten an.

c) Finde zwei komplexe Zahlen, die über $\mathbb{R}$ linear unabhängig und über $\mathbb{C}$ linear abhängig sind.

Lösung.

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

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

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

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

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

b) …

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

$$a \cdot 1 + b \cdot \mathrm{i} = 0$$

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

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

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*

a) Berechne den Grad von $\sqrt{3} + \mathrm{i}$ über $\mathbb{Q}$, über $\mathbb{Q}(\sqrt{3})$ und über $\mathbb{Q}(\mathrm{i})$.

b) Finde ein Polynom mit rationalen Koeffizienten, das über $\mathbb{Q}$ irreduzibel ist, über $\mathbb{Q}(\sqrt{3})$ in genau zwei und über $\mathbb{Q}(\sqrt{3}+\mathrm{i})$ in genau vier irreduzible Polynome zerfällt.

c) 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.

d) Sei ζ eine Lösung der Polynomgleichung $X^4+X^3+X^2+X+1=0$. Zeige, dass ζ eine in $\alpha := \exp(\pi\mathrm{i}/5)$ rationale Zahl ist, und gib eine Basis von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}(\zeta)$ an.

Lösung.

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

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

Das Polynom $X^2-2\sqrt{3}\,X+4$ ist tatsächlich über $\mathbb{Q}(\sqrt{3})$ irreduzibel: Es hat Grad 2 und seine Nullstellen $\sqrt{3}\pm\mathrm{i}$ 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 $\mathbb{Q}(\mathrm{i})$ bestimmen. Dazu rechnen wir:

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

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

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

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

Nun kann man nachrechnen, dass das Polynom $X^4-4\,X^2+16$ 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 $z := \sqrt{3}+\mathrm{i}$. 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 $\sqrt{3}\cdot\mathrm{i}$) und daher sogar $\mathbb{Q}(z)=\mathbb{Q}(\sqrt{3},\mathrm{i})$ gilt.

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

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

zeichnen. Nach der Gradformel gilt also

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

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

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

zeichnen und daher die Gradformel verwenden:

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

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

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

Aufgabe 3. *Spiel und Spaß mit der Gradformel*

a) 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?

b) Seien x, y, z wie in a). Zeige, dass $\deg_{\mathbb{Q}(z)} y$ ein Teiler von $\deg_{\mathbb{Q}(z)} x$ ist.

c) Sei f ein normiertes und irreduzibles Polynom vom Grad ≥ 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.

a) 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.

b) Folgt sofort aus der in a) hergeleiteten Beziehung.

c) 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 einer Teiler vom Grad von a. Wegen $\deg f \geq 2$ ist das ein Widerspruch zur Teilerfremdheitsvoraussetzung.

Aufgabe 4. *Primitive Elemente*

a) Finde ein primitives Element zu i und $\sqrt[3]{2}$.

b) Drücke $\sqrt{2}$ und $\sqrt{3}$ als Polynome in $\sqrt{2} + \sqrt{3}$ mit rationalen Koeffizienten aus.

c) Seien $z_1, \ldots, z_n$ algebraische Zahlen. Zeige, dass es eine algebraische Zahl z mit $\mathbb{Q}(z) = \mathbb{Q}(z_1, \ldots, z_n)$ gibt.

d) 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 $x := \mathrm{i}$ und $y := \sqrt[3]{2}$ sind $f(X) = X^2 + 1$ bzw. $g(X) = X^3 - 2$ mit den Nullstellen $\pm\mathrm{i}$ bzw. $\omega^k \cdot \sqrt[3]{2}$, $k = 0, 1, 2$. Die Ausnahmemenge S ist daher gleich

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

Näherungsweise ergibt sich

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

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

Variante 2 (durch stundenlanges Knobeln): Wir vermuten, dass $z := \mathrm{i} + \sqrt[3]{2}$ 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 $\mathbb{Q}(z) \subseteq \mathbb{Q}(\mathrm{i}, \sqrt[3]{2})$ gilt. Umgekehrt kann man durch Vergleich verschiedener z-Potenzen auf die Beziehungen

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

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

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 mit z^1 und z^3 können wir geeignet gegeneinander ausspielen:

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

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

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

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 $\mathbb{Q}(x_1, \ldots, x_n)$ vollständig in Linearfaktoren. Nach Teilaufgabe c) 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:

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

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.