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

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 3 zur Algebra I

Abgabe bis 6. Mai 2013, 17:00 Uhr

Aufgabe 1. *Beispiele für algebraische Zahlen*

a) Ist die Zahl $\cos 10^\circ$ algebraisch?

b) Zeige, dass die Polynomgleichung $X^3 - 2X + 5 = 0$ genau eine reelle Lösung α besitzt.

c) Zeige, dass diese Lösung α invertierbar ist, und finde eine normierte Polynomgleichung mit rationalen Koeffizienten, die α^{-1} als Lösung besitzt.

Lösung.

a) Ja, denn die Zahl $\cos 10^\circ$ ist der Realteil der komplexen Zahl $e^{\pi \mathrm{i}/18}$, und diese ist algebraisch, da sie die Gleichung

$$X^{18} + 1 = 0$$

erfüllt (wieso?). Da Realteile algebraischer Zahlen selbst ebenfalls algebraisch sind, begründet das die Algebraizität von $\cos 10^\circ$.

b) Wir setzen $f := X^3 - 2X + 5$. Da $f(-3) = -16 < 0 < 1 = f(-2)$, besitzt die Gleichung $f(X) = 0$ nach Blatt 1, Aufgabe 2 mindestens eine reelle Lösung α im Intervall $(-3, -2)$. Mit einer Polynomdivision durch $(X - \alpha)$ kann man f faktorisieren:

$$f = (X - \alpha)(X^2 + \alpha X + \alpha^2 - 2).$$

Das verbleibende Polynom hat nun keine weiteren reellen Nullstellen, denn seine Diskriminante ist negativ:

$$D = \alpha^2 - 4(\alpha^2 - 2) = 8 - 3\alpha^2 \leq 8 - 3 \cdot 2^2 = -4 < 0.$$

c) Die Zahl α kann nicht Null sein, da Null keine Lösung der Gleichung $f(X) = 0$ ist:

$$f(0) = 0^3 - 2 \cdot 0 + 5 = 5 \neq 0.$$

Also ist α invertierbar. Für die Zahl α^{-1} gilt

$$(\alpha^{-1})^{-3} - 2(\alpha^{-1})^{-1} + 5 = 0;$$

das ist zwar eine Gleichung, aber keine Polynomgleichung für α^{-1}. Wenn wir mit $(\alpha^{-1})^3$ durchmultiplizieren, erhalten wir die äquivalente Gleichung

$$1 - 2(\alpha^{-1})^2 + 5(\alpha^{-1})^3 = 0.$$

Also ist α^{-1} Lösung der normierten Polynomgleichung mit rationalen Koeffizienten

$$X^3 - \frac{2}{5}X^2 + \frac{1}{5} = 0.$$

Aufgabe 2. *Produkt algebraischer Zahlen*

a) Seien x und y Zahlen mit $x^3 - x + 1 = 0$ und $y^2 - 2 = 0$. Finde eine normierte Polynomgleichung mit rationalen Koeffizienten, die die Zahl $x \cdot y$ als Lösung besitzt.

b) Der *Grad* einer algebraischen Zahl z ist der kleinstmögliche Grad einer normierten Polynomgleichung mit rationalen Koeffizienten, die z als Lösung besitzt. Finde eine Abschätzung für den Grad des Produkts zweier algebraischer Zahlen in Abhängigkeit der Grade der Faktoren.

Lösung.

a) Es ist unnötig, nach den Zahlen x und y aufzulösen. Stattdessen können wir direkt das Verfahren aus Proposition 1.3 des Skripts verwenden, wir setzen also $c_{ij} := x^i y^j$ für $i = 0, 1, 2$ und $j = 0, 1$ und rechnen:

$$\begin{aligned}
xy \cdot c_{00} &= xy \cdot x^0 y^0 = xy = c_{11} \\
xy \cdot c_{01} &= xy \cdot x^0 y^1 = xy^2 = 2x = 2c_{10} \\
xy \cdot c_{10} &= xy \cdot x^1 y^0 = x^2 y = c_{21} \\
xy \cdot c_{11} &= xy \cdot x^1 y^1 = x^2 y^2 = 2x^2 = 2c_{20} \\
xy \cdot c_{20} &= xy \cdot x^2 y^0 = x^3 y = (x-1)y = c_{11} - c_{01} \\
xy \cdot c_{21} &= xy \cdot x^2 y^1 = x^3 y^2 = 2x^3 = 2(x-1) = 2c_{10} - 2c_{00}
\end{aligned}$$

In Matrixform:

$$xy \cdot \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \\ c_{20} \\ c_{21} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 \\ -2 & 0 & 2 & 0 & 0 & 0 \end{pmatrix}}_{=: A} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \\ c_{20} \\ c_{21} \end{pmatrix}$$

Also ist xy als Eigenwert dieser Matrix Nullstelle ihres charakteristischen Polynoms

$$p(X) = \det(XI - A) = \cdots = X^6 - 4\,X^4 + 4\,X^2 - 8$$

und erfüllt somit die Gleichung $p(X) = 0$.

Bemerkung: Bei anderer Anordnung der c_{ij} erhält man die Beziehungen

$$xy \cdot \begin{pmatrix} c_{00} \\ c_{10} \\ c_{20} \\ c_{01} \\ c_{11} \\ c_{21} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ -2 & 2 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{10} \\ c_{20} \\ c_{01} \\ c_{11} \\ c_{21} \end{pmatrix}, \quad xy \cdot \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{20} \\ c_{11} \\ c_{21} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ -2 & 0 & 2 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{20} \\ c_{11} \\ c_{21} \end{pmatrix}.$$

Das charakteristische Polynom ist jeweils dasselbe.

b) Sei x eine algebraische Zahl vom Grad n und y eine algebraische Zahl vom Grad m. Nach Proposition 1.3 des Skripts erhält man eine Polynomgleichung für das Produkt xy, indem man aus den Zahlen $xy \cdot c_{ij}$, wobei $c_{ij} := x^i y^j$ und $i = 0, \ldots, n-1$, $j = 0, \ldots, m-1$, eine Matrix baut und deren charakteristisches Polynom bestimmt. Da diese Matrix eine $(nm \times nm)$-Matrix ist, hat das charakteristische Polynom Grad nm. Also ist der Grad des Produkts höchstens nm.

Bemerkung: Diese Abschätzung ist *scharf*, d. h. es gibt tatsächlich Fälle, bei denen der Grad des Produkts genau gleich dem Produkt der Grade der Faktoren ist (etwa bei $x = \sqrt{2}$, $y = \sqrt{3}$). Es gibt aber auch Fälle, bei denen der Produktgrad deutlich unter der Schranke aus der Abschätzung bleibt (etwa bei $x = \sqrt[71]{2}$, $y = 1/x$).

Bemerkung: Für den Grad der Summe algebraischer Zahlen gilt dieselbe Abschätzung.

Aufgabe 3. *Eigenschaften algebraischer Zahlen*

a) Zeige, dass das komplex Konjugierte einer jeden algebraischen Zahl algebraisch ist.

b) Zeige, dass der Betrag einer jeden algebraischen Zahl algebraisch ist.

c) Zeige, dass rationale ganz algebraische Zahlen schon ganzzahlig sind.

d) Sei f ein normiertes Polynom vom Grad mindestens 1 mit rationalen Koeffizienten und z eine transzendente Zahl. Zeige, dass dann auch $f(z)$ eine transzendente Zahl ist.

Lösung.

a) Da z algebraisch ist, ist z Lösung einer normierten Polynomgleichung

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$$

mit rationalen Koeffizienten, d. h. es gilt $z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0$. Damit folgt (wieso?)

$$0 = \overline{z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0} = \overline{z}^n + a_{n-1}\overline{z}^{n-1} + \cdots + a_1\overline{z} + a_0,$$

also ist $\overline{z}$ Lösung derselben Gleichung und damit als algebraisch entlarvt.

Bemerkung: Die Erkenntnis aus dieser Aufgabe kann man als griffige Merkregel formulieren: Lösungen von Polynomgleichungen mit reellen Koeffizienten treten stets in komplex-konjugierten Paaren auf. Für allgemeine Polynomgleichungen stimmt das nicht.

b) Sei z eine algebraische Zahl. Dann gilt

$$|z|^2 = z\overline{z}.$$

Da mit z auch $\overline{z}$ algebraisch ist und das Produkt algebraischer Zahlen algebraisch ist, ist die rechte Seite dieser Identität algebraisch. Der Betrag von z ist also als eine der Lösungen der Gleichung mit algebraischen Koeffizienten

$$X^2 - z\overline{z} = 0$$

ebenfalls algebraisch.

c) Sei z eine rationale ganz-algebraische Zahl. Dann erfüllt z also eine normierte Polynomgleichung mit ganzzahligen Koeffizienten. Nach Blatt 0, Aufgabe 3b) ist z daher schon ganzzahlig.

d) Angenommen, $y := f(z)$ wäre algebraisch. Dann gibt es ein normiertes Polynom g mit rationalen Koeffizienten, sodass y die Gleichung

$$g(Y) = 0$$

erfüllt, sodass also $g(f(z)) = 0$ ist. Setzt man $h := g \circ f$ – das ist wieder ein normiertes Polynom mit rationalen Koeffizienten (wieso?) – sieht man, dass z Lösung der Gleichung $h(X) = 0$ ist. Das ist ein Widerspruch zur Transzendenz von z.

Explizitere Variante: Angenommen, $y := f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0$ wäre algebraisch. Dann erfüllt y eine normierte Polynomgleichung mit rationalen Koeffizienten:

$$y^m + b_{m-1}y^{m-1} + \cdots + b_1y + b_0 = 0.$$

Setzt man obige Darstellung von y in diese Gleichung ein, erhält man eine normierte Polynomgleichung mit rationalen Koeffizienten, die z als Lösung hat. Das ist ein Widerspruch zur Transzendenz von z.

Aufgabe 4. *Spielen mit Einheitswurzeln*

a) Finde alle komplexen Lösungen der Gleichung $X^6 + 1 = 0$.

b) Finde eine Polynomgleichung, deren Lösungen genau die Ecken desjenigen regelmäßigen Siebenecks in der komplexen Zahlenebene sind, dessen Zentrum der Ursprung der Ebene ist und das deine Lieblingszahl als eine Ecke besitzt.

c) Zeige, dass die Gleichung $X^{n-1} + X^{n-2} + \cdots + X + 1 = 0$ genau $n - 1$ Lösungen besitzt, und zwar alle n-ten Einheitswurzeln bis auf die 1.

d) Sei ζ eine n-te und ϑ eine m-te Einheitswurzel. Zeige, dass $\zeta \cdot \vartheta$ eine k-te Einheitswurzel ist, wobei k das kleinste gemeinsame Vielfache von n und m ist.

Lösung.

a) Bezeichne ξ eine primitive sechste Einheitswurzel, etwa $\xi = e^{2\pi \mathrm{i}/6}$. Eine Lösung der Gleichung ist i. Daher sind die insgesamt sechs Lösungen der Gleichung durch

$$\mathrm{i}, \quad \xi\mathrm{i}, \quad \xi^2\mathrm{i}, \quad \xi^3\mathrm{i}, \quad \xi^4\mathrm{i}, \quad \xi^5\mathrm{i}$$

gegeben (wieso?).

Bemerkung: Man kann auch die Faktorisierung $X^{12} - 1 = (X^6 - 1) \cdot (X^6 + 1)$ ausnutzen. An dieser kann erkennt man nämlich sofort, dass die Lösungen von $X^6 + 1 = 0$ einfach genau die zwölften Einheitswurzeln sind, die keine sechsten Einheitswurzeln sind.

b) Sei $\heartsuit$ meine Lieblingszahl. Dann tut's die Gleichung $X^7 - \heartsuit^7 = 0$ (wieso?).

Bemerkung: Wenn man möchte, kann man die Gleichung auch ausfaktorisiert hinschreiben. Sei dazu ξ eine primitive siebte Einheitswurzel, etwa $\xi = e^{2\pi \mathrm{i}/7}$. Dann ist obige Gleichung äquivalent zu

$$\prod_{k=0}^{6} (X - \xi^k \cdot \heartsuit) = 0.$$

Bemerkung: Für die meisten Wahlen von $\heartsuit$ kann es keine Polynomgleichung mit *reellen* Koeffizienten geben, die genau die sieben Ecken als Lösungen besitzt. Denn jede solche Gleichung würde mit $\heartsuit$ auch das komplex Konjugierte $\overline{\heartsuit}$ als Lösung besitzen, das ist aber im Allgemeinen keine der Ecken.

c) Sei x eine beliebige komplexe Zahl. Dann gilt:

$$\begin{aligned}
& x^{n-1} + x^{n-2} + \cdots + x + 1 = 0 \\
\overset{?}{\iff} \quad & x^{n-1} + x^{n-2} + \cdots + x + 1 = 0 \ \wedge \ x \neq 1 \\
\iff \quad & (x-1) \cdot (x^{n-1} + x^{n-2} + \cdots + x + 1) = 0 \ \wedge \ x \neq 1 \\
\iff \quad & x^n - 1 = 0 \ \wedge \ x \neq 1 \\
\iff \quad & x \text{ ist eine der } n\text{-ten Einheitswurzeln, aber nicht die 1.}
\end{aligned}$$

Da wir durchgängig Äquivalenzumformungen verwendet haben, zeigt diese Überlegung tatsächlich die Behauptung.

Bemerkung: Bei einem „⇒"-Schritt können Scheinlösungen entstehen, bei einem „⇐"-Schritt können Lösungen verloren gehen.

d) Da k ein Vielfaches von n ist, gilt $\zeta^k = 1$. Analog gilt $\vartheta^k = 1$. Daher folgt:

$$(\zeta \cdot \vartheta)^k = \zeta^k \cdot \vartheta^k = 1 \cdot 1 = 1.$$

Aufgabe 5. *Primitive Einheitswurzeln*

Eine n-te Einheitswurzel ζ heißt genau dann *primitiv*, wenn *jede* n-te Einheitswurzel eine ganzzahlige Potenz von ζ ist. Sei $\Phi(n)$ die Anzahl der zu n teilerfremden Zahlen in $\{1, \dots, n\}$.

a) Kläre ohne Verwendung von b): Welche der vierten Einheitswurzeln sind primitiv?

b) Zeige, dass es genau $\Phi(n)$ primitive n-te Einheitswurzeln gibt.

Lösung.

a) Insgesamt gibt es vier vierte Einheitswurzeln:

$$1, \quad \mathrm{i}, \quad -1, \quad -\mathrm{i}.$$

Von diesen sind i und $-\mathrm{i}$ primitiv: Denn die Potenzen von i geben gerade diese vier Zahlen, und für $-\mathrm{i}$ stimmt es auch. Die anderen beiden Wurzeln sind aber nicht primitiv: Denn die Potenzen von 1 sind nur 1 selbst, und die von -1 sind nur ± 1.

b) Sei $\xi := e^{2\pi \mathrm{i}/n}$. Dann wollen wir untersuchen, wann eine beliebige n-te Einheitswurzel ξ^a primitiv ist:

$$\begin{aligned}
& \xi^a \text{ primitiv} \\
\iff & \text{jede } n\text{-te Einheitswurzel ist Potenz von } \xi^a \\
\iff & \text{speziell } \xi \text{ ist Potenz von } \xi^a \\
\iff & \exists m \in \mathbb{Z}\colon (\xi^a)^m = \xi \\
\iff & \exists m \in \mathbb{Z}\colon am \equiv 1 \mod n \\
\iff & a \text{ und } n \text{ sind zueinander teilerfremd}
\end{aligned}$$

Das zeigt die Behauptung. (Wieso gelten die Äquivalenzaussagen?)

Bemerkung: Eine abstraktere Argumentation ist folgende. Die Gruppe der n-ten Einheitswurzeln (bzgl. der Multiplikation) ist (unkanonisch) isomorph zu $\mathbb{Z}/(n)$ (bzgl. der Addition). Die Teilmenge der (doch bzgl. der Multiplikation) invertierbaren Elemente in $\mathbb{Z}/(n)$ entspricht unter dieser Korrespondenz gerade der Menge der primitiven n-ten Einheitswurzeln. Da es bekanntlich genau $\Phi(n)$ invertierbare Elemente in $\mathbb{Z}/(n)$ gibt, zeigt das die Behauptung.