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

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 6 zur Algebra I

Abgabe bis 27. Mai 2013, 17:00 Uhr

Aufgabe 1. *Anwendungen der Diskriminante*

a) Sei $X^3 + pX + q = 0$ eine reduzierte kubische Gleichung mit ganzzahligen Koeffizienten p und q. Zeige, dass die Gleichung drei *paarweise verschiedene* Lösungen (in den komplexen Zahlen) besitzt, wenn q ungerade ist.

b) Sei $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$ eine normierte Polynomgleichung mit rationalen Koeffizienten. Zeige, dass sie mindestens eine nicht reelle Nullstelle besitzt, wenn ihre Diskriminante negativ ist.

Lösung.

a) Die Diskriminante $\Delta = -4p^3 - 27q^2$ ist nicht null, da der Term $-4p^3$ gerade, aber $27q^2$ ungerade ist.

b) Wenn $x_1, \ldots, x_n$ die Lösungen der Gleichungen mit Vielfachheiten sind, so ist $\Delta = \prod_{i<j}(x_i - x_j)^2$. Wenn nun alle x_i reell wären, wäre $\Delta \geq 0$.

Aufgabe 2. *Diskriminanten allgemeiner kubischer Gleichungen*

a) Berechne die Diskriminante der allgemeinen kubischen Gleichung $X^3+aX^2+bX+c = 0$.

b) Zeige, dass $X^3 - 5\,X^2 + 7\,X - 3 = 0$ höchstens zwei verschiedene Lösungen hat.

Lösung.

a) Wenn wir $Y := X + \frac{a}{3}$ und

$$p := b - \frac{a^2}{3} \qquad\qquad q := \frac{2a^3 - 9ab + 27c}{27}$$

setzen, lässt sich die gegebene Gleichung äquivalent als

$$Y^3 + pY + q = 0$$

schreiben. Die Lösungen für Y dieser Gleichung sind von den Lösungen der originalen Gleichung um $a/3$ verschoben – das ändert aber die Diskriminante nicht, da in ihr nur die Differenzen der Lösungen eingehen. Somit ist die Diskriminante der gegebenen Gleichung gleich der Diskriminante der reduzierten Gleichung, also gleich

$$\Delta = -4p^3 - 27q^2 = \cdots = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

b) Die Diskriminante dieser Gleichung ist null:

$$\Delta = (-5)^2 \cdot 7^2 - 4 \cdot 7^3 - 4 \cdot (-5)^3 \cdot (-3) - 27 \cdot (-3)^2 + 18 \cdot (-5) \cdot 7 \cdot (-3) = 0.$$

Variante: Man errät die Lösung 1 und findet dann nach einer Polynomdivision die weiteren Nullstellen. Dann ergibt sich die Faktorisierung $X^3 - 5\,X^2 + 7\,X - 3 = (X-1)^2 \cdot (X-3)$.

Aufgabe 3. *Transzendente Zahlen*

a) Sei (z_n) eine konvergente komplexe Zahlenfolge mit Grenzwert z und seien alle Folgenglieder z_n algebraisch. Ist dann auch z algebraisch?

b) Ist $\sqrt[3]{\pi}$ eine algebraische Zahl? Ist π^3 algebraisch?

c) Finde eine Folge paarweise verschiedener transzendenter Zahlen.

Lösung.

a) Das ist in den seltensten Fällen der Fall. Etwa kann man

$$z_n := 3,\text{die ersten } n \text{ Nachkommaziffern von } \pi$$

setzen. Dann sind alle Folgenglieder algebraisch (sogar rational), aber der Grenzwert π ist nicht algebraisch.

Ein anderes Beispiel ist
$$z_n := \left(1 + \frac{1}{n}\right)^n.$$

Dann sind ebenfalls alle Folgenglieder algebraisch (sogar rational), aber der Grenzwert e ist nicht algebraisch.

Bemerkung: Tatsächlich gilt [in klassischer Logik] eine Art Umkehrung der Aufgabe: Jede komplexe Zahl ist Grenzwert einer Folge algebraischer Zahlen. (Es ist sogar jede komplexe Zahl Grenzwert einer Folge von Zahlen der Form $x + \mathrm{i}y$ mit $x, y \in \mathbb{Q}$.) Man sagt auch, dass die algebraischen Zahlen *dicht* in $\mathbb{C}$ liegen.

b) Nein: Wäre $\sqrt[3]{\pi}$ algebraisch, so wäre auch $(\sqrt[3]{\pi})^3 = \pi$ algebraisch.

Ebenso ist π^3 nicht algebraisch: Wäre π^3 algebraisch, so wäre auch $\sqrt[3]{\pi^3} = \pi$ algebraisch (da Wurzeln algebraischer Zahlen stets algebraisch sind).

c) Man kann etwa $z_n := \pi + n$ setzen. Die Folgenglieder sind paarweise verschieden (klar) und jeweils transzendent (wieso?).

Aufgabe 4. *Triangulatur des Kreises*

Ist folgendes Problem lösbar? Gegeben ein Kreis. Konstruiere nur mit Zirkel und Lineal ein gleichseitiges Dreieck mit demselben Flächeninhalt.

Lösung. Sei r der Radius des Kreises und a die Seitenlänge eines flächengleichen gleichseitigen Dreiecks. Da nach dem Satz des Pythagoras die Höhe des Dreiecks durch $h = \frac{\sqrt{3}}{2}a$ gegeben ist, gilt dann also die Beziehung

$$A_{\bigcirc} = \pi r^2 = \frac{\sqrt{3}}{4}a^2 = A_{\triangle}.$$

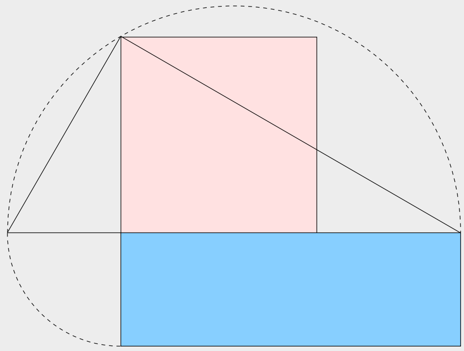
Somit ist die Seitenlänge a die Zahl

$$a = \sqrt{\frac{4}{\sqrt{3}}\pi} \cdot r.$$

Für die meisten Werte von r, etwa $r = 1$, ist die Seitenlänge a daher nicht algebraisch (wieso?) und somit nicht konstruierbar: Wäre sie es, könnte man die Strecke beim Ursprung abtragen und so die Zahl a konstruieren – aber transzendente Zahlen sind nicht konstruierbar. Im Allgemeinen ist das Problem also nicht lösbar.

Geometrische Alternativlösung: Aus jedem gleichseitigen Dreieck kann man ein flächengleiches Rechteck konstruieren, indem man es längs einer Höhe aufschneidet und eine der entstehenden Hälften längs der Diagonale mit der anderen Hälfte verklebt (Skizze!).

Ferner kann man aus jedem Rechteck ein flächengleiches Quadrat konstruieren:



Dabei garantiert der Höhensatz, dass das konstruierte Quadrat tatsächlich denselben Flächeninhalt hat wie das Rechteck.

Wäre also das gegebene Problem immer lösbar, wäre auch das Problem der Quadratur des Kreises immer möglich. Das ist bekanntermaßen aber nicht der Fall.

Aufgabe 5. *Die Resultante zweier Polynome*

a) Seien $f(X)$ und $g(Y)$ zwei normierte Polynome mit Nullstellen (mit Vielfachheiten) $x_1, \ldots, x_n$ bzw. $y_1, \ldots, y_m$. Zeige, dass der Ausdruck $R := \prod_{i,j}(x_i - y_j)$ ein Polynom in den Koeffizienten von $f(X)$ und den Koeffizienten von $g(Y)$ ist.

b) Seien $X^2 + aX + b = 0$ und $Y^2 + cY + d = 0$ zwei quadratische Gleichungen. Gib einen in a, b, c und d polynomiellen Ausdruck an, der genau dann verschwindet, wenn die beiden Gleichungen eine gemeinsame Lösung besitzen.

Lösung.

a) Die Grundidee ist einfach: Der gegebene Ausdruck R ist symmetrisch in den x_i und separat symmetrisch in den y_j. Mit zweimaliger Anwendung des Hauptsatzes über die symmetrischen Funktionen folgt daher, dass R ein polynomieller Ausdruck in den elementarsymmetrischen Funktionen der x_i und in denen der y_j ist. Diese sind nach dem Satz von Vieta bis auf Vorzeichen durch die Koeffizienten von f bzw. g gegeben.

   Wenn man etwas präziser verstehen möchte, auf welche Polynome man den Hauptsatz anwendet, muss man etwas ausholen.

   Zunächst betrachten wir noch nicht speziell die gegebenen Polynome f und g. Stattdessen definieren wir allgemein ein Polynom

$$P := \prod_{i,j}(X_i - Y_j),$$

   man beachte die Großbuchstaben auf der rechten Seite. Dieses Polynom ist offenkundig in den X_i und separat in den Y_j symmetrisch. Unser Ziel ist es nun, dieses

Polynom als Polynom in den elementarsymmetrischen Funktionen $e_i(X_1, \ldots, X_n)$ und $\widetilde{e}_j(Y_1, \ldots, Y_m)$ zu schreiben. Das erreichen wir in zwei Schritten. Zur besseren Lesbarkeit verwenden wir die Abkürzung „$\vec{X}$“ für $X_1, \ldots, X_n$ und analog für $Y_1, \ldots, Y_m$.

Schritt 1: Wir fassen P als Polynom in $(\mathbb{Z}[\vec{Y}]_{\text{symm}})[\vec{X}]$ auf. Dabei meinen wir mit „$\mathbb{Z}[\vec{Y}]_{\text{symm}}$“ den Rechenbereich der in $Y_1, \ldots, Y_m$ *symmetrischen* Polynome. So aufgefasst, ist es symmetrisch (in seinen nunmehr einzigen Variablen, den X_i), womit Satz 2.12 der Vorlesung uns garantiert, dass es genau ein Polynom $H \in (\mathbb{Z}[\vec{Y}]_{\text{symm}})[E_1, \ldots, E_n]$ mit

$$P = H(e_1(\vec{X}), \ldots, e_n(\vec{X}))$$

gibt. Die Koeffizienten von H stammen dabei aus demselben Rechenbereich wie die von P, nach unserer Auffassung also $\mathbb{Z}[\vec{Y}]_{\text{symm}}$; konkret handelt es sich bei den Koeffizienten von H also um in den Y_j symmetrische Polynome.

Schritt 2: Das Polynom H können wir auch als Polynom aus $(\mathbb{Z}[E_1, \ldots, E_n])[\vec{Y}]$ auffassen; so aufgefasst, ist es in seinen nunmehr einzigen Variablen, den Y_j, symmetrisch. Damit können wir abermals Satz 2.12 der Vorlesung anwenden: Es gibt genau ein Polynom $L \in (\mathbb{Z}[E_1, \ldots, E_n])[\widetilde{E}_1, \ldots, \widetilde{E}_m]$ mit

$$H = L(\widetilde{e}_1(\vec{Y}), \ldots, \widetilde{e}_m(\vec{Y})).$$

Dabei bezeichnen wir zur besseren Unterscheidung die elementarsymmetrischen Funktionen in den Y_j mit $\widetilde{e}_1(\vec{Y}), \ldots, \widetilde{e}_m(\vec{Y})$.

Zwischenfazit: Zusammenfassend gilt

$$P(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = L(e_1(\vec{X}), \ldots, e_n(\vec{X}), \widetilde{e}_1(\vec{Y}), \ldots, \widetilde{e}_m(\vec{Y})). \tag{1}$$

Die Notation auf der rechten Seite bedeutet dabei, dass wir in L für die Variablen E_i jeweils die $e_i(\vec{X})$ und für die Variablen $\widetilde{E}_j$ jeweils die $\widetilde{e}_j(\vec{Y})$ einsetzen. Unser obiges Ziel ist also erreicht.

Jetzt betrachten wir speziell die Polynome $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ und $g = Y^m + b_{m-1}Y^{m-1} + \cdots + b_1 Y + b_0$ mit ihren Nullstellen $x_1, \ldots, y_n$ bzw. $y_1, \ldots, y_m$. Nach dem Vietaschen Satz gelten die Beziehungen

$$e_i(x_1, \ldots, x_n) = (-1)^i a_{n-i}$$
$$\widetilde{e}_j(y_1, \ldots, y_m) = (-1)^j b_{m-j}.$$

Setzen wir also in Gleichung (1) für die Platzhalter $X_1, \ldots, X_n$ die tatsächlichen Nullstellen $x_1, \ldots, x_n$ und für $Y_1, \ldots, Y_m$ die Nullstellen $y_1, \ldots, y_m$ ein, erhalten wir

$$R = P(x_1, \ldots, x_n, y_1, \ldots, y_m) = L(\pm a_{n-1}, \ldots, \pm a_0, \pm b_{m-1}, \ldots, \pm b_0).$$

Also ist R in der Tat ein in den Koeffizienten von f und g polynomieller Ausdruck.

Bemerkung: Der Ausdruck ist sogar *universell* – das Polynom L, das die Form des Ausdrucks vorgibt, hängt nur von den Graden n und m, aber nicht von den konkreten Koeffizienten a_i, b_j ab.

b) In Erinnerung an Teilaufgabe a) definieren wir

$$R := (x_1 - y_1) \cdot (x_1 - y_2) \cdot (x_2 - y_1) \cdot (x_2 - y_2),$$

wobei x_1, x_2 und y_1, y_2 die Lösungen der ersten bzw. zweiten Gleichung seien. Dieser Ausdruck ist genau dann null, wenn die beiden Gleichungen gemeinsame Lösungen besitzen. Jetzt müssen wir ihn noch als Polynom in den Koeffizienten schreiben – Teilaufgabe a) verleiht uns die Gewissheit, dass das möglich ist. Zur konkreten Ausführung nutzen wir die Beziehungen aus dem Vietaschen Satz,

$$\begin{aligned} b &= x_1 x_2 & d &= y_1 y_2, \\ a &= -(x_1 + x_2) & c &= -(y_1 + y_2), \end{aligned}$$

und rechnen:

$$\begin{aligned} R &= (x_1 - y_1)(x_1 - y_2)(x_2 - y_1)(x_2 - y_2) \\ &= (x_1^2 - x_1 y_2 - x_1 y_1 + y_1 y_2)(x_2^2 - x_2 y_2 - x_2 y_1 + y_1 y_2) \\ &= (x_1^2 + c x_1 + d)(x_2^2 + c x_2 + d) \\ &= x_1^2 x_2^2 + c x_1^2 x_2 + d x_1^2 + c x_1 x_2^2 + c^2 x_1 x_2 + c d x_1 + d x_2^2 + c d x_2 + d^2 \\ &= b^2 + b c x_1 + d x_1^2 + b c x_2 + c^2 b + c d x_1 + d x_2^2 + c d x_2 + d^2 \\ &= b^2 - abc + d(x_1^2 + x_2^2 + 2 x_1 x_2) - 2 x_1 x_2 d - acd + c^2 b + d^2 \\ &= a^2 d - abc - acd + b^2 + bc^2 - 2bd + d^2. \end{aligned}$$

Variante: Statt der Beziehungen aus dem Satz von Vieta kann man auch die explizite Darstellung der Lösungen durch die Mitternachtsformel verwenden und dann die Ausmultipliziererei beginnen. Man erhält dasselbe Ergebnis.

Variante, die zu wenig zeigt: Man kann mit der Mitternachtsformel die Lösungen der beiden Gleichungen angeben und diese gleichsetzen – die beiden „±"-Zeichen sollen dabei unabhängig voneinander sein:

$$\begin{aligned} & & x_{1,2} &= y_{1,2} \\ \iff & & -a \pm_1 \sqrt{a^2 - 4b} &= -c \pm_2 \sqrt{c^2 - 4d} \\ \iff & & \pm_1 \sqrt{a^2 - 4b} \mp_2 \sqrt{c^2 - 4d} &= a - c \\ \implies & & a^2 - 4b + 2 \pm_1 \mp_2 \sqrt{a^2 - 4b}\sqrt{c^2 - 4d} + c^2 - 4d &= a^2 - 2ac + c^2 \\ \iff & & \pm_1 \mp_2 \sqrt{a^2 - 4b}\sqrt{c^2 - 4d} &= 2b + 2d - ac \\ \implies & & (a^2 - 4b) \cdot (c^2 - 4d) &= (2b + 2d - ac)^2 \\ \iff & & a^2 d - abc - acd + b^2 + bc^2 - 2bd + d^2 &= 0 \end{aligned}$$

Dann erhält man zwar denselben Ausdruck wie oben, kann sich jedoch nicht sicher sein, dass er *nur* dann verschwindet, wenn die beiden Gleichungen eine gemeinsame Lösung besitzen: Denn in der Herleitung kamen nicht ausschließlich „⇔"-Pfeile vor. Man kann sich aber sicher sein, dass der Ausdruck *zumindest* dann verschwindet, wenn es gemeinsame Lösungen gibt, denn jeder Schritt funktionierte zumindest in der Richtung „⇒".

Bemerkung, die Neugierde wecken soll: Man kann den gesuchten Ausdruck auch als Determinante einer gewissen Matrix schreiben:

$$R = \det \begin{pmatrix} 1 & a & b & 0 \\ 0 & 1 & a & b \\ 1 & c & d & 0 \\ 0 & 1 & c & d \end{pmatrix}.$$

Das hat einen tieferen Grund.

Nicht verpassen: **Gauß-Vorlesung** über Muster bei Primzahlen am 28. Mai ab 17:00 Uhr im Parktheater Göggingen, mehr Informationen auf `http://xrl.us/gauss2013`.