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

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 4 zur Algebra I

Abgabe bis 13. Mai 2013, 17:00 Uhr

Aufgabe 1. *Lage der Lösungen von Polynomgleichungen*

Sei $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$ eine normierte Polynomgleichung mit komplexen Koeffizienten. Zeige, dass jede komplexe Lösung z höchstens die Entfernung $1 + \max\{|a_0|, \ldots, |a_{n-1}|\}$ zum Ursprung hat.

Lösung. Sei $R := \max\{|a_0|, \ldots, |a_{n-1}|\}$. Dann gilt für alle $z \in \mathbb{C}$ mit $|z| \geq R + 1$ folgende Hilfsüberlegung (wieso?):

$$\begin{aligned}\left|a_{n-1}\frac{1}{z} + \cdots + a_1\frac{1}{z^{n-1}} + a_0\frac{1}{z^n}\right| &\overset{\triangle}{\leq} |a_{n-1}|\frac{1}{|z|} + \cdots + |a_1|\frac{1}{|z|^{n-1}} + |a_0|\frac{1}{|z|^n} \\ &\leq R \cdot \frac{1}{|z|} \leq \underbrace{\frac{R}{R+1}}_{=:q} < 1\end{aligned}$$

Dabei haben wir $\frac{1}{|z|^i} \leq \frac{1}{|z|}$ verwendet (okay, da $|z| \geq 1$). Somit gilt (wieso?) für alle $|z| \geq R+1$

$$|f(z)| = |z|^n \left|1 + a_{n-1}\frac{1}{z} + \cdots + a_0\frac{1}{z^n}\right| \geq |z|^n (1 - q) > 0,$$

insbesondere also $f(z) \neq 0$.

Die Idee ist also: Über die Terme der Ordnung echt kleiner als n können wir wenig aussagen. Aber diese Terme werden vom Monom z^n dominiert – ausnutzen können wir das dadurch, indem wir es ausklammern.

Aufgabe 2. *Stetigkeit von Polynomfunktionen*

Sei $f : \mathbb{C} \to \mathbb{C}, z \mapsto a_nz^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0$ eine Polynomfunktion mit Koeffizienten $a_0, \ldots, a_n \in \mathbb{C}$. Zeige, dass f in folgendem starken Sinn stetig ist:

$$\forall R > 0\ \forall \epsilon > 0\ \exists \delta > 0\ \forall z, w \in \mathbb{C} \text{ mit } |z|, |w| \leq R\text{: } |z - w| < \delta \Longrightarrow |f(z) - f(w)| < \epsilon$$

Lösung. Sei $R > 0$ beliebig. Sei $\epsilon > 0$ beliebig. Wir setzen

$$\delta := \epsilon \cdot \left[nR^{n-1} \cdot \left(\sum_{i=0}^{n} |a_i| + 1\right)\right]^{-1}.$$

Ohne Einschränkung der Allgemeinheit sei außerdem $R \geq 1$ (dann ist die Funktion $t \mapsto R^t$ monoton steigend). Dann gilt für alle $z, w \in \mathbb{C}$ mit $|z|, |w| \leq R$ und $|z - w| < \delta$ zunächst die Abschätzung

$$\begin{aligned}|z^i - w^i| &= |z - w| \cdot |z^{i-1} + z^{i-2}w + z^{i-3}w^2 + \cdots + zw^{i-2} + w^{i-1}| \\ &\leq |z - w| \cdot (R^{i-1} + \cdots + R^{i-1}) \\ &\leq nR^{n-1}|z - w|\end{aligned}$$

für alle $i = 0, \ldots, n$ und daher folgt

$$\begin{aligned}|f(z) - f(w)| = \left|\sum_{i=0}^{n} a_i(z^i - w^i)\right| &\leq \sum_{i=0}^{n} |a_i||z^i - w^i| \\ &\leq \sum_{i=0}^{n} |a_i| \cdot nR^{n-1}|z - w| = nR^{n-1}\left(\sum_{i=0}^{n} |a_i|\right) \cdot |z - w| < \epsilon.\end{aligned}$$

Bemerkung: In Worten lautet die Behauptung, dass die Polynomfunktion f auf jeder abgeschlossenen Kreisscheibe um den Ursprung gleichmäßig stetig ist. Der Vorteil der hier gegebenen Lösung gegenüber einem Verweis auf eine Analysis-Vorlesung ist, dass wir die ϵ-Abhängigkeit von δ explizit angeben konnten.

Aufgabe 3. *Rechenregeln*

a) Seien f und g Polynome mit komplexen Koeffizienten und $\deg f \leq n$ und $\deg g \leq m$. Zeige, dass $\deg(f + g) \leq \max\{n, m\}$ und $\deg(fg) \leq n + m$.

b) Beweise oder widerlege: Für alle Polynome f und Zahlen x, y gilt $f(xy) = f(x)f(y)$.

c) Sei q eine komplexe Zahl ungleich Eins. Zeige: $\sum_{k=0}^{n} q^k = (q^{n+1} - 1) / (q - 1)$.

Lösung.

a) Da $\deg f \leq n$, gibt es Koeffizienten $a_0, \ldots, a_n \in \mathbb{C}$ sodass $f = \sum_{i=0}^{n} a_i X^i$. Analog gibt es Koeffizienten $b_0, \ldots, b_m \in \mathbb{C}$ mit $g = \sum_{j=0}^{m} b_j X^j$. Dann sehen wir: In der Summe $f+g$ sind die Koeffizienten aller Monomome vom Grad $> \max\{n, m\}$ und im Produkt fg die aller Monome vom Grad $> nm$ null. Das zeigt die Behauptung.

Bemerkung: Abgerundet wird die Aufgabe durch Beispiele, wo man sieht, wie sich bei der Addition die höchsten Potenzen wegheben oder nicht wegheben.

Bemerkung: Wenn man von den Koeffizienten nicht entscheiden kann, ob sie null oder nicht null sind (wie bei allgemeinen reellen oder komplexen Zahlen der Fall), ist der Grad eines Polynoms keine wohldefinierte natürliche Zahl (wieso?). Dem zusammengesetzten Ausdruck „$\deg f \leq n$“ kann man aber trotzdem einen Sinn verleihen, nämlich dass alle Koeffizienten von f zu Monomen mit Grad echt größer als n null sind. In diesem Sinn ist die Aufgabe zu verstehen.

b) Die Behauptung gilt fast nie. Ein einfaches Gegenbeispiel ist

$$f(X) := X + 1, \quad x := 0, \quad y := 1,$$

denn dann ist

$$f(xy) = f(0) = 1 \neq 2 = 1 \cdot 2 = f(0)f(1).$$

Ein noch einfacheres Gegenbeispiel ist

$$f(X) := 2, \quad x := 0, \quad y := 1,$$

denn dann ist

$$f(xy) = f(0) = 2 \neq 4 = 2 \cdot 2 = f(0)f(1).$$

c) Wir rechnen:

$$\begin{aligned}(q-1)\cdot(1+q+q^2+\cdots+q^n) = \quad & q+q^2+q^3+\cdots+q^n+q^{n+1}\\ & -1-q-q^2-q^3-\cdots-q^n\\ & = q^{n+1}-1.\end{aligned}$$

Nach Division durch $q-1$ steht die zu zeigende Identität da.

Bemerkung: Wem die Auslassungszeichen unlieb sind, kann auch einen Induktionsbeweis führen.

Aufgabe 4. *Teiler von Polynomen*

a) Ist $X+\sqrt{2}$ ein Teiler von X^3-2X?

b) Besitzt $X^7+11\,X^3-33\,X+22$ einen Teiler der Form $(X-a)(X-b)$ mit $a,b\in\mathbb{Q}$?

c) Sei $f=3\,X^4-X^3+X^2-X+1$ und $g=X^3-2\,X+1$.
Finde Polynome q und r mit $f=qg+r$ und $\deg r<\deg g$.

d) Sei d ein gemeinsamer Teiler zweier Polynome f und g und seien p und q weitere Polynome. Zeige, dass d dann auch ein Teiler von $pf+qg$ ist.

e) Seien f, g und h Polynome mit ganzzahligen Koeffizienten und $f=g\cdot h$. Zeige, dass für jede ganze Zahl n die ganze Zahl $g(n)$ ein Teiler von $f(n)$ ist.

Lösung.

a) *Variante 1:* Ja, denn $-\sqrt{2}$ ist eine Nullstelle von X^3-2X (wieso?).

Variante 2: Ja, denn es gilt: $X^3-2X=X(X^2-2)=X(X-\sqrt{2})(X+\sqrt{2})$.

Variante 3: Ja, denn eine Nebenrechnung zeigt, dass die Polynomdivision von X^3-2X durch $X+\sqrt{2}$ keinen Rest lässt.

b) Nach Blatt 0, Aufgabe 3b) und Blatt 1, Aufgabe 1 können rationale Nullstellen des gegebenen Polynoms nur Teiler von 22 sein. Einsetzen zeigt aber, dass keine der Zahlen

$$\pm1,\quad \pm2,\quad \pm11,\quad \pm22$$

Nullstellen sind. Also besitzt das Polynom keinerlei rationale Nullstellen und daher auch keine Teiler der Form $(X-a)(X-b)$ mit $a,b\in\mathbb{Q}$.

c) Polynomdivision liefert

$$\begin{aligned}q &= 3X-1,\\ r &= 7X^2-6X+2.\end{aligned}$$

d) Nach Voraussetzung gibt es Polynome $\tilde{f}$ und $\tilde{g}$ mit $f=d\tilde{f}$ und $g=d\tilde{g}$. Damit folgt

$$pf+qg=pf\tilde{f}+qd\tilde{g}=d\cdot(p\tilde{f}+q\tilde{g}),$$

also ist d tatsächlich ein Teiler von $pf+qg$.

e) Für jede ganze Zahl n folgt $f(n)=g(n)\cdot h(n)$ (wieso?). Da $h(n)$ eine ganze Zahl ist (wieso?), zeigt das schon die Behauptung.

Aufgabe 5. *Polynomielle Ausdrücke*

a) Schreibe $\frac{1}{\sqrt{2}+5\sqrt{3}}$ als polynomiellen Ausdruck in $\sqrt{2}$ und $\sqrt{3}$ mit rationalen Koeffizienten.

b) Sei z eine komplexe Zahl mit $\mathbb{Q}(z) = \mathbb{Q}[z]$. Zeige, dass z algebraisch ist.

c) Inwiefern kann man ein Polynom in zwei Unbestimmten X und Y als Polynom in einer einzigen Unbestimmten Y, dessen Koeffizienten Polynome in X sind, auffassen?

Lösung.

a) Wir bedienen uns desselben Tricks, den man auch beim Dividieren durch komplexe Zahlen verwendet:

$$\frac{1}{\sqrt{2}+5\sqrt{3}} = \frac{\sqrt{2}-5\sqrt{3}}{(\sqrt{2}+5\sqrt{3})(\sqrt{2}-5\sqrt{3})} = \frac{\sqrt{2}-5\sqrt{3}}{2-25\cdot 3} = \frac{-1}{73}\sqrt{2} + \frac{5}{73}\sqrt{3}.$$

Bemerkung: Im neunjährigen Gymnasium war diese Technik unter dem Titel *Nenner rational machen* bekannt.

Bemerkung: Mit ein wenig Galoistheorie kann man verstehen, wie man bei komplizierteren Nennern verfahren kann: Der Nenner x ist in diesem Fall Element einer gewissen endlichen Erweiterung von $\mathbb{Q}$. Wenn wir die Elemente ihrer Galoisgruppe mit $\sigma_1, \ldots, \sigma_n$ bezeichnen, wobei wir $\sigma_1 = \mathrm{id}$ setzen, so können wir den Bruch mit $\sigma_2(x)\cdots\sigma_n(x)$ erweitern. Der erweiterte Nenner ist dann

$$\sigma_1(x)\cdots\sigma_n(x),$$

augenscheinlich invariant unter der Wirkung der σ_i, und somit tatsächlich rational.

b) Wir beweisen die Behauptung zunächst für den Fall, dass $z \neq 0$. Dann ist nämlich $1/z$ ein Element von $\mathbb{Q}(z)$ und daher auch von $\mathbb{Q}[z]$; also gibt es ein Polynom $f(X)$ mit rationalen Koeffizienten und $\frac{1}{z} = f(z)$. Dieses Polynom kann nicht das Nullpolynom sein (wieso?) und hat daher mindestens Grad 0. Die Zahl z ist also Lösung der Polynomgleichung

$$f(X)\cdot X - 1 = 0$$

mit rationalen Koeffizienten. Diese ist nichttrivial (wegen der Multiplikation mit X ist ihr Grad mindestens 1) und enttarnt daher nach Normierung z als algebraisch.

Nun wollen wir den allgemeinen Fall behandeln. In klassischer Logik ist das einfach, denn da ist z null oder nicht null; im ersten Fall ist z sowieso algebraisch, im zweiten Fall haben wir das gerade gesehen. Intuitionistisch ist diese Fallunterscheidung nicht zulässig, trotzdem können wir den Beweis retten: Denn auch konstruktiv gilt

$$|z| > 0 \quad \text{oder} \quad |z| < 1.$$

Im ersten Fall folgt $z \neq 0$ und daher die Algebraizität nach obigem Argument. Im zweiten Fall ist $z' := z + 1$ nicht null; wegen $\mathbb{Q}(z) = \mathbb{Q}(z')$ und $\mathbb{Q}[z] = \mathbb{Q}[z']$ (wieso?) zeigt obige Argumentation, dass z' algebraisch ist. Also ist auch $z = z' - 1$ algebraisch.

Bemerkung: Die Inklusion $\mathbb{Q}[z] \subseteq \mathbb{Q}(z)$ besteht stets. Die Umkehrung der Behauptung der Aufgabe gilt ebenfalls und wird im Skript unmittelbar vor Folgerung 2.3 bewiesen. Zusammengefasst ist die Beweisidee dort folgende: Die Nenner x von Zahlen aus $\mathbb{Q}(z)$ sind algebraisch, daher sind ihre Inversen polynomielle Ausdrücke in x und damit auch in z.

c) Ein Polynom aus $\mathbb{Q}[X,Y]$ kann man einfach dadurch als Polynom in $(\mathbb{Q}[X])[Y]$ auffassen, indem man seine Terme nach Y-Potenzen umgruppiert, zum Beispiel so:

$$3\,X^2Y - 5\,XY - 8\,X + 4\,Y + 5 = (3\,X^2 - 5\,X + 4)Y^1 + (-8\,X + 5)Y^0.$$

Bemerkung: Etwas präziser kann man mittels dieser Idee einen *Ringisomorphismus* $\mathbb{Q}[X,Y] \to (\mathbb{Q}[X])[Y]$ angeben. Für formale Potenzreihen stimmt die analoge Aussage ebenfalls.

Aufgabe 6. *Beweis des Fundamentalsatzes*

Im Beweis des Fundamentalsatzes der Algebra tritt die Zahl 3 immer wieder auf. Kann sie durch eine kleinere Zahl $3 - \epsilon$ ersetzt werden?

Lösung. Wir erinnern an die grobe Struktur des Beweises des Fundamentalsatzes: Ausgehend von der (möglicherweise sehr schlechten) Näherung 0 als Lösung der Polynomgleichung

$$f(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 = 0$$

konstruieren wir eine erste bessere Näherung z. Diese ist insofern besser, als dass sie die Abschätzung

$$|z^n + b_{n-1}z^{n-1} + \cdots + b_1z + b_0| \leq q|b_0| \tag{1}$$

erfüllt, wobei $q := 1 - \frac{1}{2} \cdot 3^{1-n^2}$ ein fester Faktor kleiner als Eins ist. (Zum Vergleich: Für die Näherung 0 ergibt sich als Abstand $|f(0)| = |b_0|$.) Aus dieser besseren Näherung konstruieren wir dann eine abermals verbesserte Näherung; sukzessive erhalten wir so eine Folge immer besser werdender Näherungslösungen, deren Grenzwert eine tatsächliche Lösung der Gleichung ist.

Wenn man nun die Zahl 3 in der Definition von q durch eine kleinere Zahl ersetzen könnte, hätte das folgenden Vorteil: Der Faktor q wäre dann kleiner (wieso?) und damit die Konvergenz schneller – zumindest, wenn die Abschätzung (1) nicht zu pessimistisch ist, sondern ein realistisches Bild der Konvergenzgeschwindigkeit vermittelt. (Manche numerische Verfahren konvergieren in der Realität viel schneller als naive Abschätzungen vermuten lassen.)

Um nun die Frage zu klären, ob man 3 durch eine kleinere Zahl ersetzen kann, müssen wir den gesamten Beweis des Fundamentalsatzes durchgehen und bei jedem Vorkommen von 3 prüfen, ob der jeweilige Schritt auch bei einer kleineren Zahl durchgeht. Bei einer solchen Analyse stellt man fest: Für den Großteil des Beweises spielt der Wert dieser Konstanten keine Rolle (solange er nur positiv ist), erst bei den Abschätzungen (1.47), (1.48), (1.49) und der finalen Abschätzung (auf Seite 41) wird es kritisch.

Wir wollen unseren kleineren Ersatz für die Zahl 3 mit „$\widetilde{3}$“ bezeichnen. Entsprechend setzen wir $\widetilde{2} := \widetilde{3} - 1$. Die veränderten Abschätzungen lauten dann:

$$m(r) \geq \widetilde{3}^{k^2-n^2}|b_0| \tag{1.47}$$

$$\sum_{i=1}^{k-1} f_i(r) \leq \frac{1 - \widetilde{3}^{1-k}}{\widetilde{2}} f_k(r) \tag{1.48}$$

$$\sum_{i=k+1}^{n} f_i(r) \leq \frac{1 - \widetilde{3}^{k-n}}{\widetilde{2}} f_k(r) \tag{1.49}$$

$$\sum_{i\neq 0,k} f_i(r) \leq \left(\frac{2}{\widetilde{2}} - \frac{\widetilde{3}^{1-k}}{\widetilde{2}}\right) f_k(r)$$

Interessant wird es, wenn wir uns der finalen Abschätzung zuwenden:

$$|f(z)| \leq |b_0| - \left(\frac{\widetilde{3}^{1-k}}{\widetilde{2}} + 1 - \frac{2}{\widetilde{2}} \right) m(r) \tag{2}$$

Auf der rechten Seite wollen wir nun mittels Abschätzung (1.47) weiter nach oben abschätzen. Dazu muss aber der Vorfaktor $(\cdots)$ positiv sein; eine kleine Nebenrechung zeigt, dass das genau dann der Fall ist, wenn

$$3 - \widetilde{3} < \widetilde{3}^{1-k} \tag{3}$$

für alle $k \in J \subseteq \{1, \ldots, n\}$. Da unsere neue Konstante $\widetilde{3}$ schon unabhängig von J sein soll (denn diese Menge kann sich in jedem Iterationsschritt des Näherungsverfahrens ändern), müssen wir daher fordern, dass die Abschätzung sogar im schlimmstmöglichen Fall $k = n$ gilt:

$$3 - \widetilde{3} < \widetilde{3}^{1-n}. \tag{4}$$

Denn für $k = n$ ist die rechte Seite der Ungleichung (3) am kleinsten. Wenn wir unsere neue Konstante $\widetilde{3}$ also so einschränken, dass sie Abschätzung (4) erfüllt, können wir Ungleichung (2) fortführen:

$$|f(z)| \leq |b_0| \cdot \left(1 - \frac{\widetilde{3}^{1-k+k^2-n^2}}{\widetilde{2}} + \frac{\widetilde{3}^{k^2-n^2}}{\widetilde{2}} \cdot (3 - \widetilde{3}) \right).$$

Für jedes k muss nun der Faktor $(\cdots)$ auf der rechten Seite echt kleiner als 1 sein (er wird unser neues q). Eine Nebenrechnung zeigt, dass das genau dann der Fall ist, wenn $\widetilde{3}$ die Abschätzung (4) erfüllt, was wir ja sowieso voraussetzten mussten.

Als Fazit können wir also festhalten: Für festen Polynomgrad n kann die Konstante 3 in der Tat durch jede kleinere positive Zahl $\widetilde{3}$ ersetzt werden, die noch Abschätzung (4) erfüllt. Konkret ergeben sich folgende Möglichkeiten (aufgerundete Werte):

n	kleinstmögliche Konstante $\widetilde{3}$
1	beliebig wenig mehr als exakt 2
2	2,619
3	2,880
4	2,962
5	2,988
6	2,996

Es gibt aber keine bessere Konstante, die für alle Polynomgrade n gleichmäßig funktionieren würde: Denn im Grenzwert $n \to \infty$ lautet Abschätzung (4)

$$3 - \widetilde{3} \leq 0.$$