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

Sommersemester 2013
Ingo Blechschmidt
Robert Gelb

Übungsblatt 7 zur Algebra I

Abgabe bis 3. Juni 2013, 17:00 Uhr

Wird noch vervollständigt.

Aufgabe 1. *Größte gemeinsame Teiler und kleinste gemeinsame Vielfache*

a) Seien die Polynome $f = X^3 + 2\,X^2 + 2\,X + 4$ und $g = X^2 + 3\,X + 2$ gegeben. Finde Polynome p und q mit $X + 2 = pf + qg$.

b) Seien f und g zwei normierte Polynome mit rationalen Koeffizienten. Zeige, dass *genau ein normiertes* Polynom existiert, welches ein größter gemeinsamer Teiler von f und g ist.

c) Seien f und g wie in b). Gib ein Verfahren zur Berechnung des größten gemeinsamen Teilers von f und g über die Zerlegung von f und g in ihre irreduziblen Faktoren an.

d) Seien f und g wie in b) und c). Definiere, was man unter einem *kleinsten gemeinsamen Vielfachen* von f und g verstehen sollte, und gib eine Konstruktionsvorschrift für es an.

Lösung.

a)

b) *Existenz (kurz auch im Skript abgehandelt):* Dank des euklidischen Algorithmus gibt es ein normiertes Polynom d, welches ein gemeinsamer Teiler von f und g ist und für gewisse weitere Polynome p und q die Beziehung

$$d = p \cdot f + q \cdot g$$

erfüllt. Aus dieser folgt, dass d sogar ein größter gemeinsamer Teiler ist, d. h. ein Vielfaches jedes anderen gemeinsamen Teilers ist: Ist e ein beliebiger gemeinsamer Teiler von f und g, so ist er auch ein Teiler von pf und qg und somit auch ein Teiler der rechten Seite der Gleichung, also von d.

Eindeutigkeit: Seien d und $\widetilde{d}$ beides normierte größte gemeinsame Teiler von f und g. Da d ein größer gemeinsamer Teiler ist, folgt $\widetilde{d} \mid d$. Umgekehrt folgt $d \mid \widetilde{d}$, da $\widetilde{d}$ ein größter gemeinsamer Teiler ist. Da d und $\widetilde{d}$ beide normiert sind, folgt $d = \widetilde{d}$.

c) Wir können f und g in ihre irreduziblen Faktoren p_i zerlegen:

$$f = \prod_i p_i^{a_i}$$
$$g = \prod_i p_i^{b_i}$$

Dabei dürfen die Exponenten auch null sein – damit tragen wir, ohne die Notation verkomplizieren zu müssen, dem Umstand Rechnung, dass manche Faktoren vielleicht nur in einem der beiden Polynome vorkommen. Als Vorschlag für den größten gemeinsamen Teiler definieren wir

$$d = \prod_i p_i^{c_i}$$

mit $c_i := \min\{a_i, b_i\}$ für alle Indizes i. Klar ist zumindest, dass dieses Polynom ein gemeinsamer Teiler von f und g ist. Zum Nachweis, dass d wirklich größter gemeinsamer

Teiler ist, sei ein beliebiger gemeinsamer Teiler $\widetilde{d}$ von f und g gegeben. Dann folgt (siehe unten), dass in $\widetilde{d}$ nur die Faktoren p_i (und keine anderen) vorkommen, und dass diese höchstens mit Vielfachheit a_i (wegen $\widetilde{d} \mid f$) und zugleich höchstens mit Vielfachheit b_i (wegen $\widetilde{d} \mid g$) vorkommen. Unter'm Strich kommen sie also höchstens mit Vielfachheit c_i vor, also gilt $\widetilde{d} \mid$.

Implizit haben wir dabei folgendes allgemeines Lemma benutzt: Sei p ein irreduzibles Polynom und gelte $f \mid g$. Dann ist die Vielfachheit von p in f höchstens gleich der Vielfachheit von p in g.

d) Folgende Definition ist sinnvoll: Ein Polynom k heißt genau dann *kleinstes gemeinsames Vielfaches* von f und g, wenn k ein gemeinsames Vielfaches von f und g ist und für jedes gemeinsame Vielfache $\widetilde{k}$ von f und g gilt: $k \mid \widetilde{k}$.

Aufgabe 2. *Separable Polynome*

a) Finde eine Polynomgleichung mit rationalen Koeffizienten, die dieselben Lösungen wie die Gleichung $X^7 - X^6 + 4\,X^4 - 4\,X^3 + 4\,X - 4 = 0$ besitzt, jedoch alle mit Vielfachheit 1.

b) Konstruiere eine Polynomgleichung, die genau dann von einer algebraischen Zahl a erfüllt wird, wenn das Polynom $f_a(X) := X^3 + 2a^2X - a + 6$ nicht separabel ist.

c) Zeige, dass ein normiertes Polynom f mit rationalen Koeffizienten genau dann separabel ist, wenn der größte gemeinsame Teiler von f und f' das konstante Polynom 1 ist.

Lösung.

a) Wir befolgen das Verfahren des Skripts und berechnen daher zunächst die normierte Ableitung des Polynoms $f = X^7 - X^6 + 4\,X^4 - 4\,X^3 + 4\,X - 4$:

$$\frac{1}{7}f'(X) = X^6 - \frac{6}{7}X^5 + \frac{16}{7}X^3 - \frac{12}{7}X^2 + \frac{4}{7}.$$

Der eindeutig bestimmte normierte größte gemeinsame Teiler von f und $f'/7$ ist das Polynom $d(X) = X^3 + 2$, wie eine Nebenrechnung mit dem euklidischen Algorithmus zeigt, und es gilt $f(X) = d(X) \cdot \widetilde{f}(X)$ mit $\widetilde{f}(X) = X^4 - X^3 + 2\,X - 2$. Die gesuchte Gleichung ist also

$$X^4 - X^3 + 2\,X - 2 = 0.$$

Variante: Vielleicht schafft man es auch irgendwie, das gegebene Polynom f zu faktorisieren: Es gilt $f(X) = (X-1) \cdot (X^3+2)^2$. Dann sieht man sofort, dass

$$(X-1) \cdot (X^3 + 2) = 0$$

die gesuchte Gleichung ist. Diese stimmt mit obiger überein.

b) Das Polynom f_a ist genau dann nicht separabel, wenn seine Diskriminante null ist:

$$\Delta_{f_a} = -4p^3 - 27q^2 = \cdots = -32 \cdot a^6 - 27a^2 + 324a - 972 \stackrel{!}{=} 0.$$

Damit haben wir die geforderte Polynomgleichung gefunden.

c) Sei $d(X)$ der normierte größte gemeinsame Teiler von f und f'. Dann sind die Nullstellen von $d(X)$ (in den algebraischen Zahlen) genau die mehrfachen Nullstellen von $f(X)$, d. h. diejenigen mit Vielfachheit ≥ 2.

„$\Longrightarrow$“: Da $f(X)$ nach Voraussetzung keine mehrfachen Nullstellen besitzt, besitzt $d(X)$ also keine einzige Nullstelle. Da es normiert ist, muss es daher gleich dem Einspolynom sein.

„$\Longleftarrow$“: Da $d(X)$ nach Voraussetzung keine Nullstellen besitzt, besitzt $f(X)$ keinerlei mehrfache Nullstellen.

Aufgabe 3. *Irreduzible Polynome*

a) Sind normierte Polynome vom Grad 1 stets irreduzibel über den rationalen Zahlen?

b) Zeige, dass normierte Polynome vom Grad 2 oder 3 über den rationalen Zahlen genau dann reduzibel sind, wenn sie mindestens eine rationale Nullstelle besitzen.

c) Finde ein Polynom mit rationalen Koeffizienten, das keine rationale Nullstelle besitzt und trotzdem über den rationalen Zahlen reduzibel ist.

d) Zeige, dass das Polynom $X^3 - \frac{3}{2}X^2 + X - \frac{6}{5}$ über den rationalen Zahlen irreduzibel ist.

Lösung.

a) Ja!

b) Sei $f(X)$ ein normiertes Polynom vom Grad 2 oder 3 mit rationalen Koeffizienten. Die Rückrichtung ist klar: Wenn f eine rationale Nullstelle x besitzt, geht die Division von f durch den Linearfaktor $X - x$ auf – also ist f zerlegbar.

Sei für den Beweis der Hinrichtung eine Zerlegung $f = g \cdot h$ gegeben. Nach der Gradvoraussetzung an f hat dann g oder h Grad 1 und ist daher von der Form $X - x$ für eine gewisse rationale Zahl x. Also besitzt f eine rationale Nullstelle, nämlich x.

c) Das Polynom $(X^2 + 1)^2$ ist eines von unzähligen Beispielen.

d) Nach Teilaufgabe b) genügt es, nachzuweisen, dass das gegebene Polynom keine rationalen Nullstellen besitzt. Äquivalent ist zu zeigen, dass das mit 10 durchmultiplizierte Polynom

$$10\,X^3 - 15\,X^2 + 10\,X - 12$$

keine rationalen Nullstellen besitzt. In vollständig gekürzter Darstellung müssen Zähler und Nenner solcher Nullstellen Teiler von -12 bzw. 10 sein. Also kommen nur die Möglichkeiten

$$\begin{aligned} \text{Zähler} &\in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}, \\ \text{Nenner} &\in \{\pm 1, \pm 2, \pm 5, \pm 10\}, \end{aligned}$$

in Betracht. Probiert man diese Möglichkeiten alle durch (ein paar fallen wegen fehlender Teilerfremdheit wieder weg), sieht man: Das Polynom hat keine rationalen Nullstellen.

Aufgabe 4. *Prime Polynome*

a) Ein normiertes Polynom f mit rationalen Koeffizienten heißt genau dann *prim*, wenn es nicht das Einspolynom ist und folgende Eigenschaft hat: Immer, wenn f ein Produkt $g \cdot h$ zweier Polynome mit rationalen Koeffizienten teilt, so teilt f schon mindestens einen der beiden Faktoren. Zeige, dass jedes prime Polynom irreduzibel ist.

b) Teile ein über den rationalen Zahlen irreduzibles Polynom f ein Produkt $g_1 \cdots g_n$ von Polynomen mit rationalen Koeffizienten. Zeige, dass f dann schon eines der g_i teilt.

Lösung.

a) Sei $f(X)$ ein primes Polynom. Da f nicht das Einspolynom ist, hat es mindestens Grad 1 (wieso?). Es bleibt also nur zu zeigen, dass $f(X) = f(X)$ die *einzige* Zerlegung von f ist. Sei dazu $f = g \cdot h$ mit normierten nichtkonstanten Polynomen $g(X), h(X)$ mit rationalen Koeffizienten eine hypothetische Zerlegung. Dann folgt insbesondere $f \mid gh$, also wegen der Primalität $f \mid g$ oder $f \mid h$.

Im ersten Fall folgt $g = f \cdot \widetilde{g}$ für ein Polynom $\widetilde{g}$. Dieses Polynom muss normiert sein, da g und h es sind. Eingesetzt ergibt sich $f = f\widetilde{g}h$; ein Gradvergleich zeigt, dass dann h doch konstant ist – das ist ein Widerspruch. Analog verfährt man im zweiten Fall.

b) Wir führen einen Induktionsbeweis. Der Induktionsanfang $n = 0$ ist witzig: Für ihn müssen wir zeigen, dass aus der Voraussetzung $f \mid 1$ (leeres Produkt) eine unmögliche Aussage folgt (nämlich, dass es ein $i \in \emptyset$ gibt). Da die Voraussetzung $f \mid 1$ nie erfüllt ist (irreduzible Polynome haben mindestens Grad 1), ist diese Implikation trivialerweise erfüllt.

Wenn man mag, kann man die Induktion auch erst bei $n = 1$ beginnen: Dann ist der Induktionsanfang klar und bereit weniger Kopfschmerzen.

Für den Beweis des Induktionsschritts $n \to n + 1$ gelte $f \mid g_1 \cdots g_{n+1} = (g_1 \cdots g_n) \cdot g_{n+1}$. Nach Folgerung 3.11 folgt dann $f \mid g_1 \cdots g_n$ oder $f \mid g_{n+1}$. Im zweiten Fall sind wir sofort fertig, im ersten Fall nach Anwendung der Induktionsvoraussetzung.

Aufgabe 5. *Euklidischer Algorithmus für ganze Zahlen*

Seien a und b ganze Zahlen. Zeige, dass es eine ganze Zahl $d \geq 0$ gibt, welche ein gemeinsamer Teiler von a und b ist, und für die es weitere ganze Zahlen r und s mit $d = r \cdot a + s \cdot b$ gibt.