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

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

a) Seien die Polynome $f = X^3 + 2X^2 + 2X + 4$ und $g = X^2 + 3X + 2$ 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) Wir verwenden natürlich den euklidischen Algorithmus:

$$\begin{aligned} f &= (X-1)\cdot g + (3X+6) \\ g &= \frac{1}{3}(X+1)\cdot(3X+6) + 0 \end{aligned}$$

Dann noch rückwärts auflösen: $3X + 6 = f - (X-1)\cdot g$, also $X + 2 = \frac{1}{3}f + \frac{1}{3}(-X+1)g$.

Variante: Man kann die Neu-Normierung auch schon in jedem Schritt des Algorithmus vornehmen (diese Variante verwendet der Beweis im Skript):

$$\begin{aligned} f &= (X-1)\cdot g + 3(X+2) \\ g &= (X+1)\cdot(X+2) + 0 \end{aligned}$$

Dann noch rückwärts auflösen: $X + 2 = \frac{1}{3}f + \frac{1}{3}(-X+1)g$.

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 $d = \widetilde{d}$ (wieso?).

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

$$\begin{aligned} f &= \prod_i p_i^{a_i} \\ g &= \prod_i p_i^{b_i} \end{aligned}$$

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 $\widetilde{d} \mid d$.

Implizit haben wir dabei folgendes allgemeines Lemma verwendet: Sei p ein irreduzibles Polynom und gelte $f \mid g$ (also $g = \widetilde{g} \cdot f$ für ein Polynom $\widetilde{g}$). Dann ist die Vielfachheit von p in f höchstens gleich der Vielfachheit von p in g. Diese Beobachtung folgt sofort aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren (wieso?).

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: $k \mid \widetilde{k}$.

Konstruieren können wir es zum Beispiel durch die Setzung

$$k := \prod_i p_i^{e_i},$$

wobei wir die Bezeichnungen der Lösung von Teilaufgabe c) weiterverwenden, jetzt aber $e_i := \max\{a_i, b_i\}$ setzen. Der Beweis, dass dieses Polynom tatsächlich ein kleinstes gemeinsames Vielfaches von f und g ist, verläuft völlig analog.

Konstruktionsvariante: Man kann auch $k := f \cdot g/d$ setzen. Dabei geht die Polynomdivision auf, denn da d größter gemeinsamer Teiler ist, gibt es Polynome $\widetilde{f}, \widetilde{g}, p, q$ mit

$$\begin{aligned} f &= \widetilde{f} \cdot d, \\ g &= \widetilde{g} \cdot d, \\ d &= pf + qg, \end{aligned}$$

weshalb die Darstellungen $k = \widetilde{f} \cdot g = f \cdot \widetilde{g}$ folgen. Über diese ist auch klar, dass k tatsächlich ein gemeinsames Vielfaches von f und g ist. Sei zum Nachweis der Kleinstheit ein weiteres gemeinsames Vielfaches $\widehat{k}$ gegeben. Dann gibt es Polynome $\widehat{f}, \widehat{g}$ mit $\widehat{k} = \widehat{f} \cdot f$ und $\widehat{k} = \widehat{g} \cdot g$. Mit der Bézoutdarstellung von d folgt

$$\widehat{k} = \widehat{f} \cdot f = \widehat{f} \cdot \widetilde{f} d = \widehat{f}\widetilde{f} pf + \widehat{f}\widetilde{f} qg = \widehat{g}\widetilde{g} pf + \widehat{f} q \cdot k = (\widehat{g} p + \widehat{f} q) \cdot k,$$

also ist k in der Tat ein Teiler von $\widehat{k}$.

Definitionsvariante: Folgende Definition funktioniert ebenfalls, ist aber weniger schön (da sie nicht nur über Teilbarkeit spricht): 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: $\deg k \leq \deg \widetilde{k}$.

Bemerkung für Leute, die wissen, was eine Kategorie ist: Die eleganten Definitionen von ggT und kgV sind Beispiele für Definitionen durch sog. *universelle Eigenschaften*. Tatsächlich kann man ggT und kgV als Produkt bzw. Koprodukt in einer geeigneten Kategorie von Polynomen realisieren (in der zwischen zwei Polynomen genau dann ein Morphismus verläuft, falls das erste das zweite teilt).

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: Man kann auch über die Faktorisierung von f gehen: 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, denn die beiden Faktoren haben jeweils nur einfache Nullstellen und sie überlappen nicht mit denen des anderen Faktors (das ist nach dem Abelschen Irreduzibilitätssatz auch allgemein klar). Diese Gleichung stimmt mit obiger überein.

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

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

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. Dieser Umstand ist im Skript auf Seite 74 festgehalten: Gilt $f(X) = \prod_i (X - x_i)^{a_i}$, so ist $\mathrm{ggT}(f, f') = \prod_i (X - x_i)^{a_i - 1}$.

„$\Longrightarrow$“: 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.

Variante für die Rückrichtung: Nach Vorlesung ist $f_0 := f / \mathrm{ggT}(f, f')$ ein separables Polynom. Da nach Voraussetzung der Nenner das Einspolynom ist, ist also $f_0 = f$ ein separables Polynom.

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 $X^3 - \frac{5}{2}X^2 + \frac{4}{3}$ über den rationalen Zahlen irreduzibel ist.

Lösung.

a) Ja!

Bemerkung: Über den ganzen Zahlen ist die Situation komplizierter, wenn man die Forderung nach Normiertheit fallen lässt: Etwa gilt das Polynom $2\,X - 2 = 2 \cdot (X - 1)$ dort als reduzibel. Die verfeinerte Regel lautet: Ein Polynom vom Grad 1 ist genau dann irreduzibel über den ganzen Zahlen, wenn es primitiv ist.

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.

Bemerkung: Im Skript auf Seite 76 wird eine *Zerlegung* eines normierten Polynoms f als ein Produkt der Form $f = f_1 \cdots f_n$ definiert, wobei die f_i jeweils normiert und mindestens vom Grad 1 sein sollen.

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 6 durchmultiplizierte Polynom

$$6\,X^3 - 15\,X^2 + 8$$

keine rationalen Nullstellen besitzt. In vollständig gekürzter Darstellung müssen Zähler und Nenner solcher Nullstellen Teiler von 8 bzw. 6 sein. Also kommen nur die Möglichkeiten

$$\begin{aligned} \text{Zähler} &\in \{\pm 1, \pm 2, \pm 4, \pm 8\}, \\ \text{Nenner} &\in \{\pm 1, \pm 2, \pm 3, \pm 6\}, \end{aligned}$$

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

Variante: Man kann auch das allgemeine Verfahren zur Irreduzibilitätsprüfung einsetzen (wie in Beispiel 3.17 des Skripts vorgeführt). Der Inhalt des Polynoms ist $\frac{1}{6}$. Da es vom Grad 3 ist, genügt es, einelementige Auswahlen der Nullstellen zu untersuchen – wir müssen also prüfen, ob mindestens eine der Nullstellen mit 6 multipliziert eine ganze Zahl gibt. Das ist nicht der Fall:

$x_1 \approx -0{,}651$	$x_2 \approx 0{,}916$	$x_3 \approx \ \ 2{,}232$
$6x_1 \approx -3{,}9$	$6x_2 \approx 5{,}5$	$x_3 \approx 13{,}4$

Wenn man Zugriff auf Näherungswerte der Nullstellen hat (und man weiß, dass man ihnen vertrauen kann), ist dieses Verfahren in der Praxis schneller als obige Methode über Nullstellenkandidaten.

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. Zunächst müssen wir zeigen, dass $f(X) = f(X)$ eine Zerlegung ist. Nach Definition von *Zerlegung* müssen wir dazu nur anmerken, dass f mindestens Grad 1 hat; das ist erfüllt, da f nicht das Einspolynom ist.

Dann bleibt nur noch 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 f 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.

Variante: Wir können die Polynome g_i jeweils in ihre irreduziblen Faktoren zerlegen. Wegen der Eindeutigkeit der Zerlegung muss dann einer dieser vielen Faktoren gleich f sein. Also teilt f dasjenige g_i, zu dem dieser Faktor gehört.

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.

Lösung. Wir führen sukzessive Divisionen mit Rest durch, sodass wir folgende Gleichungen erhalten:

$$\begin{aligned} a &= p_1 \cdot b + r_1 \\ b &= p_2 \cdot r_1 + r_2 \\ r_1 &= p_3 \cdot r_2 + r_3 \\ r_2 &= p_4 \cdot r_3 + r_4 \\ &\vdots \\ r_{n-3} &= p_{n-1} \cdot r_{n-2} + r_{n-1} \\ r_{n-2} &= p_n \cdot r_{n-1} + r_n \\ r_{n-1} &= p_{n+1} \cdot r_n + 0 \end{aligned}$$

Dabei soll jeweils $0 \leq r_i < |r_{i-1}|$ gelten, wobei wir der Übersichtlichkeit halber $r_0 := b$ setzen. Wir hören auf, wenn sich als Rest 0 ergibt; den vorletzten Rest r_n nennen wir kurz „d“. Nun sind noch drei Dinge zu tun:

1. Wir müssen zeigen, dass das Verfahren *terminiert*, also irgendwann zu einem Ende kommt. (Wenn nicht, hätten wir d nicht wirklich gefunden!)
2. Wir müssen zeigen, dass der vorletzte Rest d tatsächlich ein gemeinsamer Teiler von a und b ist.
3. Wir müssen zeigen, dass es wirklich die geforderte Bézoutdarstellung gibt.

Für Punkt 1 müssen wir nur beobachten, dass die Reste r_i mit jedem Schritt echt abnehmen, aber nach unten durch 0 beschränkt sind. Daher muss irgendwann (genauer: nach spätestens $|b|$ Schritten) der Rest 0 erreicht werden.

Für Punkt 2 können wir die Gleichungen rückwärts betrachten: Die letzte Gleichung sagt uns, dass $d = r_n$ ein Teiler von r_{n-1} ist. Aus der vorletzten Gleichung folgt daher, dass d auch ein Teiler von r_{n-2} ist. Analog folgt dann aus der drittletzten Gleichung, dass d ein Teiler von r_{n-3} ist (wieso?). Wenn wir auf dieselbe Art und Weise fortfahren, erkennen wir schließlich, dass d ein Teiler von b und von a ist.

Für Punkt 3 lösen wir die Gleichungen rückwärts auf: Mithilfe der vorletzten Gleichung können wir d als Linearkombination von r_{n-2} und r_{n-1} ausdrücken. Die drittletzte Gleichung erlaubt uns wiederum, die Zahl r_{n-1} als Linearkombinaton von r_{n-3} und r_{n-2} zu schreiben; als Zwischenfazit können wir daher d als Linearkombination von r_{n-3} und r_{n-2} schreiben. Wenn wir auf diese Art und Weise fortfahren, können wir schlussendlich d als Linearkombination von a und b ausdrücken.

Bemerkung: Sollte $|b| > |a|$ sein, funktioniert das hier gegebene Verfahren trotzdem: Im ersten Schritt stellt sich die gewohnte Situation von selbst ein (siehe Beispiel).

Bemerkung: Gute Beispiele zum Vorführen bzw. Üben des euklidischen Algorithmus geben Fibonaccizahlen ab (wieso?), ggf. multipliziert mit einer gemeinsamen Konstante, damit der größte gemeinsamer Teiler keine langweilige 1 wird. Etwa ergibt sich für $a = 2 \cdot 21$, $b = 2 \cdot 34$:

$$\begin{aligned} a = 42 &= 0 \cdot 68 + 42 \\ b = 68 &= 1 \cdot 42 + 26 \\ 42 &= 1 \cdot 26 + 16 \\ 26 &= 1 \cdot 16 + 10 \\ 16 &= 1 \cdot 10 + \ \ 6 \\ 10 &= 1 \cdot \ \ 6 + \ \ 4 \\ 6 &= 1 \cdot \ \ 4 + \ \ 2 \\ 4 &= 2 \cdot \ \ 2 + \ \ 0. \end{aligned}$$