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 dem *kleinsten gemeinsamen Vielfachen* von f und g verstehen sollte, und gib eine Konstruktionsvorschrift für es an.

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) ...

b) ...

c) 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.

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) 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.

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

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. Dann folgt insbesondere $f \mid gh$, also nach Voraussetzung $f \mid g$ oder $f \mid h$.

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.