

Übungsblatt 7 zur Algebra I

Abgabe bis 3. Juni 2013, 17:00 Uhr

Aufgabe 1. Größte gemeinsame Teiler und kleinste gemeinsame Vielfache

- Seien die Polynome $f = X^3 - 2X^2 + 2X - 4$ und $g = X^2 - 3X + 2$ gegeben. Finde Polynome p und q mit $X - 2 = pf + qg$.
- Seien $f(X)$ und $g(X)$ zwei normierte Polynome mit rationalen Koeffizienten. Gib ein Verfahren zur Berechnung des größten gemeinsamen Teilers von $f(X)$ und $g(X)$ über die Zerlegung von $f(X)$ und $g(X)$ in ihre irreduziblen Faktoren an.
- Seien $f(X)$ und $g(X)$ wie in b). Definiere, was man unter dem *kleinsten gemeinsamen Vielfachen* von $f(X)$ und $g(X)$ verstehen sollte, und gib eine Konstruktionsvorschrift für es an.

Aufgabe 2. Separabilität

- 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.
- Finde eine normierte Polynomgleichung mit rationalen Koeffizienten, die dieselben Lösungen wie die Gleichung $X^7 + X^6 - 4X^4 - 4X^3 + 4X + 4 = 0$ besitzt, jedoch alle mit Vielfachheit 1.
- Konstruiere eine Polynomgleichung mit rationalen Koeffizienten, die genau dann von einer algebraischen Zahl a erfüllt wird, wenn das Polynom $f_a(X) := X^3 + 2a^2X - a + 5$ nicht separabel ist.

Lösung.

- ...
- ...
- Das Polynom f_a ist genau dann nicht separabel, wenn seine Diskriminante null ist:

$$\Delta_{f_a} = -4p^3 - 27q^2 = \dots = -32 \cdot a^6 - 27a^2 + 270a - 675 \stackrel{!}{=} 0.$$

Damit haben wir die geforderte Polynomgleichung gefunden.

Aufgabe 3. Irreduzible Polynome

- Zeige, dass normierte Polynome vom Grad 2 oder 3 über den rationalen Zahlen genau dann reduzibel sind, wenn sie mindestens eine rationale Nullstelle besitzen.
- Finde ein Polynom mit rationalen Koeffizienten, das keine rationale Nullstelle besitzt und trotzdem über den rationalen Zahlen reduzibel 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

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

- a) Zeige, dass jedes prime Polynom irreduzibel ist.
b) Zeige umgekehrt, dass irreduzible Polynome prim sind.

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 $f|gh$, also nach Voraussetzung $f|g$ oder $f|h$.

Aufgabe 5. Euklidischer Algorithmus für ganze Zahlen

Beweise folgenden Satz, etwa durch Imitation des Vorlesungsbeweises für Polynome: Seien a und b ganze Zahlen. Dann existiert eine ganze Zahl $d \geq 0$, 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.