

16. Oktober 2025

7. Übungsblatt Computeralgebra

Aufgabe 1:

- a) R sei ein faktorieller Ring. Zeigen Sie: Für zwei Polynome $f, g \in R[X]$ ist $I(fg) = I(f) \cdot I(g)$!
- b) Bestimmen Sie die Inhalte der beiden Polynome $f = 12X^5 + 90X^4 + 78X^2 + 18X + 36$ und $g = (15X - 5)(12X - 24)$ aus $\mathbb{Z}[X]$!
- c) Was sind die primitiven Anteile f^* und g^* von f und g ?
- d) Bestimmen Sie $\text{ggT}(f^*, g^*)$ und $\text{ggT}(f, g)$!

Aufgabe 2:

- a) Betrachten Sie $f = X^3Y^2 - X^3 + X^2Y + XY^2 - X^2 + Y^2 - XY - 3Y + 2$ als Polynom in Y über $\mathbb{Z}[X]$ und berechnen Sie den Inhalt und den primitiven Anteil von f !
- b) Betrachten Sie f nun als Polynom in X über $\mathbb{Z}[Y]$, und berechnen Sie wieder Inhalt und primitiven Anteil!

Aufgabe 3:

Wir betrachten die Polynome $f = 2X^4 - X^3 + 24X^2 - 46X + 17$ und $g = 4X^3 - 46X^2 + 74X - 26$ aus $\mathbb{Z}[X]$.

- a) Finden Sie nach CAUCHY eine obere Schranke für die Nullstellen von f !
- b) Modulo welcher Schranke müssen Sie $\text{ggT}(f, g) \in \mathbb{Z}[X]$ kennen um ihn eindeutig bestimmen zu können?
- c) Für welche Primzahlen p könnte $\text{ggT}(f^{(p)}, g^{(p)})$ einen kleineren Grad als $\text{ggT}(f, g)$ haben?
- d) Berechnen Sie die modularen ggTs für diese Primzahlen!
- e) Wenden Sie den modularen Algorithmus an, zunächst nur mit $p = 17$ und $p = 19$. Bestimmen Sie jeweils den ggT mit führendem Koeffizienten eins!
- f) Finden Sie ein Polynom aus $\mathbb{Z}[X]$, das modulo 17 und 19 gleich diesen Polynomen ist!
- g) Warum ist auch ohne Probedivisionen klar, daß dieses Polynom nicht $\text{ggT}(f, g)$ sein kann?
- h) Finden Sie ein anderes Polynom aus $\mathbb{Z}[X]$, das zu den modularen Ergebnissen paßt, und zeigen Sie, daß es der ggT von f und g ist!
- i) Für welche Primzahlen p hat $\text{ggT}(f^{(p)}, g^{(p)})$ einen größeren Grad als $\text{ggT}(f, g)$?
- j) Berechnen Sie (mit CAS) die modularen ggTs für diese Primzahlen!

Aufgabe 4:

Wir betrachten die Polynome $f = X^3 - XY^2 + X - Y$ und $g = Y^3 - X^2Y + Y - X$ aus $\mathbb{Z}[X, Y]$.

- a) Finden Sie eine obere Schranke für den X -Grad und für den Y -Grad von $\text{ggT}(f, g)$!
- b) Modulo wie vieler Spezialisierungen für X müssen Sie $\text{ggT}(f, g)$ kennen, um ihn zu rekonstruieren?
- c) Für welche $x \in \mathbb{C}$ könnte $\deg \text{ggT}(f(x, Y), g(x, Y)) < \deg_Y \text{ggT}(f, g)$ sein?
- d) Berechnen Sie $\text{ggT}(f(x, Y), g(x, Y))$ für $x = 1, 0, -1$!
- e) Was ist $\text{ggT}(f, g)$?
- f) Für welche Spezialisierungen $x \in \mathbb{C}$ hat $\text{ggT}(f(x, Y), g(x, Y))$ einen größeren Grad als $\deg_Y \text{ggT}(f, g)$?

Abgabe bis zum Mittwoch, dem 22. Oktober 2025, um 15.30 Uhr