

25. Oktober 2025

8. Übungsblatt Computeralgebra

Aufgabe 1:

Das Polynom $f = X^7 + 11X^5 - 8X^4 - 21X^3 + X^2 + 72X - 35$ erfüllt die Kongruenz

$$f \equiv (X^4 + 21X^2 + 22X + 5)(X^3 + 13X + 16) \pmod{23}.$$

- a) Setzen sie diese Faktorisierung nach dem HENSELSchen Lemma fort zu einer Faktorisierung modulo 23^2 . Für den erweiterten EUKLIDischen Algorithmus können Sie ein Computeralgebrasystem benutzen. In Maxima liefert `gcdex(f, g)` die Liste $[a, b, \text{ggT}]$.
- b) Versuchen Sie, daraus eine Faktorisierung von $f \in \mathbb{Z}[X]$ zu erraten, und überprüfen Sie, ob diese korrekt ist!

Aufgabe 2:

- a) Berechnen Sie den ggT der beiden Polynome

$$f = X^5 - 2X^4 - X^3 + 2X^2 + X - 2 \quad \text{und} \quad g = X^4 - 2X^3 - X^2 + X + 2$$

nach dem EZ GCD Algorithmus mit der Primzahl $p = 11$!

- b) Für welche Primzahlen p hat dieses ggT-Problem schlechte Reduktion?

Aufgabe 3:

- a) Bestimmen Sie die quadratfreie Zerlegung des Polynoms

$$f = X^8 - 4X^6 - 3X^5 + 3X^4 + 6X^3 + 2X^2 - 3X - 2!$$

- b) Zerlegen Sie f in ein Produkt irreduzibler Faktoren!

Abgabe bis zum Mittwoch, dem 29. Oktober 2025, um 15.30 Uhr