Wolfgang K. Seiler
Tel. 2515

B6, B4.08

30. Oktober 2025

9. Übungsblatt Computeralgebra

Aufgabe 1:

a) Zeigen Sie, daß das Polynom $f = X^3 + 1$ modulo einer Primzahl p genau dann in Linearfaktoren zerfällt, wenn es eine ganze Zahl x gibt mit $x^2 \equiv -3 \bmod p$!

b) Stellen Sie $f^{(5)}$ und $f^{(7)}$ als Produkte irreduzibler Faktoren dar!

Aufgabe 2:

Wir betrachten das Polynom $f = X^4 + 1 \in \mathbb{Z}[X]$.

a) Finden Sie über die dritte binomische Formel die vollständige Zerlegung von $f^{(5)}$ in irreduzible Faktoren!

b) Zeigen Sie, daß $f^{(17)}$ in Linearfaktoren zerfällt!

c) Zerlegen Sie $f^{(3)}$ in ein Produkt irreduzibler Faktoren!

Aufgabe 3:

In $\mathbb{F}_2[X]$ ist $X^5+X^3+X+1 = (X+1)(X^4+X^3+1)$, und X^4+X^3+1 ist irreduzibel. Folgern Sie (ohne Computerhilfe), daß das Polynom $X^5 + X^3 + X + 1 \in \mathbb{Z}[X]$ irreduzibel ist!

Aufgabe 4:

Sei $f = X^5 + X^4 + 1 \in \mathbb{Z}[X]$.

a) Zeigen Sie, daß das Polynom $f^{(2)} \in \mathbb{F}_2[X]$ quadratfrei ist!

b) Finden Sie die irreduziblen Faktoren von $f^{(2)}$!

c) Überprüfen Sie, ob f in $\mathbb{Z}[X]$ irreduzible Faktoren der Höhe eins hat, die modulo zwei zu den in *b)* berechneten werden!

Aufgabe 5:

a) Zeigen Sie, daß die Swinnerton-Dyer-Polynome nur X-Potenzen mit geraden Exponenten enthalten!

b) q und r seien zwei verschiedene Primzahlen. Bestimmen Sie das Swinnerton-Dyer-Polynom f mit den Nullstellen $\pm\sqrt{q} \pm \sqrt{r}$ mit möglichst geringem Aufwand explizit!

c) p sei eine weitere, von q und r verschiedene Primzahl, die auch kein Teiler der Differenz von p und q ist. Zeigen Sie: Wenn $f^{(p)}$ in $\mathbb{F}_p$ eine Nullstelle hat, zerfällt es in $\mathbb{F}_p[X]$ in ein Produkt von Linearfaktoren. (*Hinweis:* Verwenden Sie die dritte binomische Formel!)

d) Dies ist genau dann der Fall, wenn sowohl q als auch r modulo p Quadrate sind.

e) Falls weder q noch r modulo p Quadrate sind, läßt sich $f^{(p)}$ als ein Produkt der Form $(X^2 + a)(X^2 + b)$ schreiben.

f) Falls genau eine der beiden Primzahlen q und r modulo p ein Quadrat ist, läßt sich $f^{(p)}$ als ein Produkt der Form $(X^2 + aX + b)(X^2 - aX + b)$ schreiben.

Abgabe bis zum Mittwoch, dem 5. November 2025, um 15.30 Uhr