
Übungen zur Vorlesung Computeralgebra
Blatt 9

Prof. Dr. Klaus Madlener

Abgabe bis 25.06.2010

Aufgabe 1:

Zeigen oder widerlegen Sie:

- a) Das Polynom $x^{1000} + 2 \in \mathbb{Z}_5[x]$ ist quadratfrei.
- b) Sei F ein Körper und seien $f, g \in F[x]$. Dann ist der quadratfreie Anteil von fg das Produkt der quadratfreien Anteile von f und g .

Der quadratfreie Anteil eines Polynoms $h = \prod_{1 \leq i \leq r} h_i^{e_i}$ ist dabei $\prod_{1 \leq i \leq r} h_i$ (mit paarweise verschiedenen irreduziblen h_i).

Aufgabe 2:

Faktorisieren Sie das Polynom $x^8 + x^7 + 2x^6 + 3x^5 + 3x^4 + 3x^3 + 2x^2 + 2x + 1$ mit der Distinct-Degree-Methode jeweils über $\mathbb{Z}_7[x]$, $\mathbb{Z}_{19}[x]$ und $\mathbb{Z}_{23}[x]$.

Aufgabe 3:

Wie viele Faktoren hat $a(x) = x^4 + 1 \in \mathbb{Z}_p[x]$ (p prim), wenn (i) $p = 2$, (ii) $p \equiv 1 \pmod{8}$, (iii) $p \equiv 3 \pmod{8}$ bzw. (iv) $p \equiv 5 \pmod{8}$?

Aufgabe 4:

Machen Sie sich mit den Begriffen Sylvestermatrix und Resultante vertraut, z.B. Modern Computer Algebra, von zur Gathen, Kap. 6.3 S. 142-147, oder Algorithms for Computer Algebra, Geddes, Kap. 7.3, S. 285-288.

Zeigen Sie: Seien $f, g \in \mathbb{Z}[x]$, $r = \text{res}(f, g) \in \mathbb{Z}$, und $u \in \mathbb{Z}$. Dann gilt $\text{gcd}(f(u), g(u)) | r$.

Aufgabe 5:

Sei $p \in \mathbb{Z}$ prim und $n > 1$. Zeigen Sie die folgenden „pathologischen“ Eigenschaften von $R = \mathbb{Z}_{p^n}[x]$ ($f, g \in R$):

- a) Es gilt nicht notwendigerweise $\deg fg = \deg f + \deg g$.
- b) R ist kein ZPE-Ring.
- c) Es ist $\text{ggT}(f, g)$ nicht notwendigerweise als Linearkombination von f und g darstellbar.