

Übungsblatt 13

Aufgabe 1: (Irreduzible Polynome in endlichen Körpern)

1. Wie viele (paarweise nicht isomorphe) endliche Körper mit weniger als 50 Elementen gibt es? Listen Sie die Anzahlen der Elemente dieser Körper auf.
2. Schreiben Sie eine Prozedur, die zu einer Primzahlpotenz q alle normierten, über $GF(q)$ irreduziblen Polynome vom Grad 2 bestimmt.
3. Bestimmen Sie für alle $GF(q)$, $q < 50$ die Anzahl $\alpha(q)$ der über $GF(q)$ irreduziblen, normierten Polynome vom Grad 2.
4. Beschreiben Sie das Wachstum von $\alpha(q)$ in q und in der Anzahl der Primfaktoren von q anhand der berechneten Daten.

(8 Punkte)

Aufgabe 2: (Methoden zur Berechnung der Resultanten) In der Vorlesung wurde die Resultante auf zwei Weisen berechnet. Setzen Sie beide Methoden in Mathematica-Prozeduren um:

1. Implementieren Sie die Berechnung als Determinante der Sylvester-Matrix.
2. Implementieren Sie eine zweite Version mit den Rekursionsformeln aus Satz 7.38 der Vorlesung. Arbeiten Sie dabei iterativ, nicht wie in der Vorlesung rekursiv.
3. Führen Sie einen Laufzeitvergleich mit einigen geeigneten Beispielpolynomen durch. Begründen Sie, warum ihre Polynome geeignet sind.

(8 Punkte)

Aufgabe 3: (Minimalpolynome und Resultanten)

Beweisen Sie: Sind α und β zwei algebraische Zahlen mit den Minimalpolynomen $p(x)$ und $q(x)$, so gilt folgende Tabelle:

Zahl	Nullstellenpolynom
$\alpha + \beta$	$\text{res}(p(x - y), q(y), y)$
$\alpha - \beta$	$\text{res}(p(x + y), q(y), y)$
α/β	$\text{res}(p(x \cdot y), q(y), y)$
$\sqrt[n]{\alpha}$	$\text{res}(p(y), x^n - y, y)$

Finden Sie ähnlich ein Nullstellenpolynom für $\alpha \cdot \beta$.

Achtung: $p(x/y)$ ist kein Polynom, daher ist $\text{res}(p(x/y), q(y), y)$ nicht definiert! Man braucht also noch einen Trick.

(6 Punkte)