Algebra und Diskrete Mathematik, PS3

Sommersemester 2018

24. und 26. April 2018

1) Was ist eine *Basis* eines Moduls? Es sei $a \in \mathbb{Z}$. Begründen Sie, warum $((x-a)^i)_{i\in\mathbb{N}}$ eine $\mathbb{Z}$-Basis des Polynomringes $\mathbb{Z}[x]$ ist. Wie kann man die Koordinaten eines Polynoms bezüglich dieser Basis berechnen?
Berechnen Sie eine natürliche Zahl n und Elemente $c_0, \ldots, c_n \in \mathbb{Z}$ so, dass

$$\text{a) } y^3 - 5y + 3 = \sum_{i=0}^{n} c_i (y-4)^i \in \mathbb{Z}[y]$$

$$\text{b) } 3t^4 - t^2 + 2 = \sum_{i=0}^{n} c_i (t-5)^i \in \mathbb{Z}[t]$$

ist.
Welche Analogie besteht zwischen dieser Aufgabe und der Aufgabe „Berechnen Sie die Ziffern zur Basis b einer natürlichen Zahl $a > 1$?“.

2) Es seien a und b zwei verschiedene rationale Zahlen und $f \neq 0$ ein Polynom in $\mathbb{Q}[x]$.
Zeigen Sie, dass das Koeffizientenpaar (c, d) des Restes $cx + d$ von f nach Division mit Rest durch $(x-a)(x-b)$ die eindeutig bestimmte Lösung des Systems linearer Gleichungen
$ay + z = f(a),\ by + z = f(b)$ ist.
Verwenden Sie das, um den Rest von x^{100} nach Division mit Rest durch $x^2 - 3x + 2$ zu berechnen.

3) Was ist eine *Nullstelle* eines Polynoms? Schreiben Sie drei Polynome mit rationalen Koeffizienten an, die Grad 8 und genau 6 verschiedene Nullstellen haben.
Zeigen Sie:
a) Wenn ein Polynom u vom Grad 2 mit rationalen Koeffizienten eine rationale Nullstelle hat, gibt es rationale Zahlen a, b, c so, dass $u = a(x-b)(x-c)$ ist.
b) Ist p eine Primzahl, dann ist $x^p - x = \prod_{z\in\mathbb{Z}_p}(x-z) \in \mathbb{Z}_p[x]$.

4) Was ist eine *Interpolationsaufgabe*? Erläutern Sie die Methoden von Lagrange und von Newton zur Lösung solcher Aufgaben. Berechnen Sie mit beiden Methoden ein Polynom f vom Grad 2 mit rationalen Koeffizienten so, dass $f(-3) = 3$, $f(2) = -3$ und $f(5) = 1$ ist.

5) Was ist der *größte gemeinsame Teiler* zweier oder mehrerer Polynome? Erläutern Sie den Euklidischen Algorithmus zu seiner Berechnung. Berechnen Sie den größten gemeinsamen Teiler der Polynome

$$x^3 + 1 \quad \text{und} \quad x^3 + 2x^2 + 2x + 1$$

in $\mathbb{Q}[x]$ und

$$x^4 + x^2 + x + \bar{1} \quad \text{und} \quad x^4 + x^3 + x^2 + x$$

in $\mathbb{Z}_2[x]$.

Was ist das *kleinste gemeinsame Vielfache* zweier oder mehrerer Polynome?
Berechnen Sie das kleinste gemeinsame Vielfache der Polynome

$$5x^3 + 5 \quad \text{und} \quad x^3 + 2x^2 + 2x + 1$$

in $\mathbb{Q}[x]$.

6) Erklären Sie den *erweiterten Euklidischen Algorithmus* für ganze Zahlen und für Polynome.
Es seien $a := x^4 + x^2 + 1$ und $b := x^3 + x + 1$ Polynome in $\mathbb{Z}_2[x]$. Berechnen Sie (falls möglich) $u, v \in \mathbb{Z}_2[x]$ so, dass

$$x + 1 = ua + vb$$

ist.
Berechnen Sie (falls möglich) Polynome $u, v \in \mathbb{Q}[x]$ so, dass

$$(x^4 + x^2 - x + 2)u + (-x^2 + 3x + 1)v = x$$

ist. Verwenden Sie dazu ein Computeralgebra-System.