

Algebra für Informationssystemtechniker – Sommersemester 2018

14. Übungsblatt

Rechnen in Polynomringen

Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.

- Berechnen Sie 9^{-1} in $(\mathbb{Z}_{23}, +, \cdot)$ mit dem erweiterten euklidischen Algorithmus.
 - Wie viele Polynome vom Grad höchstens 3 gibt es in $\mathbb{Z}_2[x]$?
Welche Einheiten gibt es im Polynomring $(\mathbb{Z}_2[x], \oplus, \otimes)$?
-

Ü79 Berechnen Sie die Summe und das Produkt folgender Polynome im Ring $(\mathbb{Z}_3[x], \oplus, \otimes)$:

$$p(x) = x^2 + 2x + 2 \quad \text{und} \quad q(x) = 2x + 1.$$

Berechnen Sie weiterhin $p(x) \bmod q(x)$ und $q(x) \bmod p(x)$.

Ü80 (a) Verwenden Sie den euklidischen Algorithmus, um einerseits im Ring $(\mathbb{Q}[x], \oplus, \otimes)$ andererseits im Ring $(\mathbb{Z}_2[x], \oplus, \otimes)$ einen größten gemeinsamen Teiler der Polynome

(i) $p_1(x) = x^4 + x^3 + x^2 + 1$ und $p_2(x) = x^3 + x^2 + x + 1$,

(ii) $p_1(x) = x^5 + x^4 + x$ und $p_2(x) = x^2 + x + 1$.

zu berechnen.

(b) Verwenden Sie den euklidischen Algorithmus um im Ring $(\mathbb{Z}_5[x], \oplus, \otimes)$ einen größten gemeinsamen Teiler der Polynome

$$p(x) = 3x^4 + 2x^3 + 2 \quad \text{und} \quad q(x) = 2x^2 + 3$$

zu berechnen.

Ü81 (a) Geben Sie alle Elemente des Ringes $(\mathbb{Z}_3[x]/x^2 + 2x + 1, \oplus, \otimes)$ an.

Finden Sie einen Nullteiler in diesem Ring.

Berechnen Sie das Element $x \otimes (2x)$ in $\mathbb{Z}_3[x]/x^2 + 2x + 1$ und untersuchen Sie, ob dieses Element eine Einheit von $\mathbb{Z}_3[x]/x^2 + 2x + 1$ ist.

(b) Berechnen Sie mit dem erweiterten euklidischen Algorithmus

- $(x^2)^{-1}$ in $\mathbb{Z}_3[x]/x^3 + 2x + 2$,

- $(x^2 + x + 1)^{-1}$ in $\mathbb{Z}_2[x]/x^3 + x + 1$.

H82 Berechnen Sie in $\mathbb{Z}_5[x]$ einen größten gemeinsamen Teiler $g(x)$ für die Polynome

$$p_1(x) = 3x^6 + x^5 + 3x^4 + 4x^3 + 4 \quad \text{und} \quad p_2(x) = x^4 + 4x^3 + 2x^2 + x + 2.$$

H83 In $\mathbb{Z}_2[x]$ ist das Polynom $f(x) = x^3 + x^2 + 1$ gegeben.

(a) Wie viele Elemente enthält der Ring $(\mathbb{Z}_2[x]/f(x), \oplus, \otimes)$?

(b) Berechnen Sie mit dem erweiterten euklidischen Algorithmus für $p(x) = x^2 + x + 1$ sein multiplikativ Inverses $p(x)^{-1}$ in $\mathbb{Z}_2[x]/f(x)$.

H84 Stellen Sie für den Ring $(\mathbb{Z}_2[x]/x^2 + x + 1, \oplus, \otimes)$ die Verknüpfungstabellen der Addition und Multiplikation auf.

Zu welcher bekannten Gruppe ist $(\mathbb{Z}_2[x]/x^2 + x + 1, \oplus)$ isomorph?

Begründen Sie anhand der Verknüpfungstabellen, dass $(\mathbb{Z}_2[x]/x^2 + x + 1, \oplus, \otimes)$ sogar ein Körper ist.