Modul Algebra 2 6. Juni 2006
SoSe 2006
Schmale

Aufgabenblatt 7

(19) $\boldsymbol{g = x^2 + x + 1}$ **über** $\boldsymbol{\mathbb{Z}_p}$**.**

(a) Für welche $p \in \{5, 7, 11\}$ ist ${}^{\mathbb{Z}_p[x]}\!/_{g\mathbb{Z}_p[x]}$ oder $\mathbb{Z}_p[x]_{2,g}$ ein Körper und wie viele Elemente enthält er ?

(b) Berechnen Sie $\big((x^2+1) + g\mathbb{Z}_p[x]\big)^{-1}$ in ${}^{\mathbb{Z}_p[x]}\!/_{g\mathbb{Z}_p[x]}$ oder $(x^2+1)^{\textcircled{-1}}$ in $\mathbb{Z}_p[x]_{2,g}$ für $p \in \{5, 7, 11\}$.

(20) Vereinfachung eines Ausdrucks.

(a) Seien K ein Unterkörper eines Körpers L, g ein unzerlegbares Polynom in $K[x]$, $\alpha \in L$ und $g(\alpha) = 0$. Zeigen Sie:

Der Kern des Einsetzungsmorphismus π_α ist $g\,K[x]$.

(b) Sei α eine komplexe Zahl mit der Eigenschaft $\alpha^3 = \alpha + 1$. Gegeben sei außerdem der Ausdruck

$$\frac{\alpha^5 + 2\alpha^2 - \alpha + 1}{\alpha^5 - \alpha^2 + \alpha + 1}$$

Zeigen Sie: Der Ausdruck ist wohldefiniert, stellt also eine komplexe Zahl dar, und lässt sich vereinfachen zu

$$a\alpha^2 + b\alpha + c$$

mit geeigneten $a, b, c \in \mathbb{Q}$. Bestimmen Sie a, b, c.
Benutzen Sie ggf. ohne Beweis, die Unzerlegbarkeit des Polynoms $x^3 - x - 1$ in $\mathbb{Q}[x]$. Systematische Kriterien behandeln wir demnächst.

(21) Eine Abbildung aus der Kodierungstheorie.[1]

Sei K ein Körper mit mindestens n Elementen und seien $\alpha_1, \ldots, \alpha_n$ paarweise verschiedene Elemente aus K. Seien weiter $k \leq n$, $\phi : K^k \longrightarrow K[x]_k$ mit $\phi(b_0, \ldots, b_{k-1}) = \sum_{\mu=0}^{k-1} b_\mu x^\mu$, $\pi : K[x]_k \longrightarrow K^n$ mit $\pi(f) = \big(f(\alpha_1), \ldots, f(\alpha_n)\big)$ und $\varepsilon = \pi \circ \phi$.
Zeigen Sie:

(a) ε ist eine injektive K-lineare Abbildung.

(b) Für alle $u, v \in K^k$ mit $u \neq v$ hat der Vektor $\varepsilon(u) - \varepsilon(v)$ höchstens $k-1$ Nulleinträge.

.....

[1] In der Kodierungstheorie ist meist K ein Körper dessen Elementeanzahl eine 2-er-Potenz ist. K^k enthält dann die in gleich lange "Pakete" unterteilten digitalisierten Nachrichtenvektoren. ε ist die Kodierungsabbildung, die die Nachrichtenvektoren in einem höherdimensionalen Raum so verteilt, dass die Bildvektoren sich paarweise an möglichst vielen Komponenten unterscheiden, m.a.W. so, dass der so genannte Hammingabstand möglichst groß ist. Dies erlaubt es eine gewisse Anzahl Sende- oder Lesefehler (z.B. Handy oder CD-Player) auf rein algebraischem Wege zu korrigieren ohne den Sende- oder Lesevorgang zu wiederholen. Der Bildraum von ε heißt *linearer Code*. Die Kodierungsabbildung der Aufgabe führt durch spezielle Wahl der α_i direkt zu den täglich mindestens milliardenfach benutzten Reed-Solomon-Codes. Letztere sind sogenannte *lineare, zyklische, fehlerkorrigierende Codes*. Ein weit verbreiteter Text dazu: http://www.siam.org/siamnews/mtc/mtc193.htm