Übungen zur Vorlesung Algebra

Institut für Reine Mathematik WS 07/08 – Blatt 07

Abgabetermin: Dienstag 04.12.2007 um 12:15 Uhr vor Beginn der Vorlesung

---

1. Sei K ein Körper und $R := \left\{ \sum_{i=0}^{<\infty} c_i Y^i \in K[Y] \; ; \; c_1 = 0 \right\}$. Zeigen Sie:

   (a) R ist ein Integritätsring.

   (b) Es gibt einen kanonischen Morphismus der Quotientenkörper

   $$\mathrm{Quot}(R) \longrightarrow \mathrm{Quot}(K[Y]) \ .$$

   Dieser ist ein Isomorphismus.

   (c) Y ist Nullstelle eines normierten Polynoms $P \in R[T]$.

2. Man führe die in Satz 2.5.5 beschriebene Division mit Rest in folgenden Fällen explizit durch:

   (a) $f = 3X^5 + 2X^4 - X^3 + 3X^2 - 4X + 7, \quad g = X^2 - 2X + 1$

   (b) $f = X^5 + X^4 - 5X^3 + 2X^2 + 2X - 1, \quad g = X^2 - 1$

3. Bestimmen Sie ein Polynom $f \in \mathbb{F}_{17}[T]$ mit

   $$f(13) = 1 \; ; \; f(15) = 4 \; ; \; f(10) = 2 \; ; \; f(5) = 16 \; ; \; f(8) = 3 \ .$$

4. Es sei R ein Integritätsring. Es seien $a_1, a_2 \in R$ und $d \in \mathrm{ggT}(a_1, a_2)$. Also gilt $a_i = d \cdot a_i'$ für $i = 1, 2$. Zeigen Sie, dass a_1', a_2' teilerfremd sind.

5. Die folgende Aufgabe demonstriert eine Anwendung der elementaren Algebra in der Informationstheorie.

   Es sei $\mathbb{F}_2$ der Körper mit 2 Elementen. Es seien $0 \leq r \leq m$ ganze Zahlen. Zeigen Sie:

   (a) Die Abbildung

   $$\Phi : \mathbb{F}_2[T_1, \ldots, T_m] \longrightarrow \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) \; ; \; f \mapsto (x \to f(x))$$

   ist surjektiv aber nicht injektiv. Es ist $\dim \mathrm{Abb}(\mathbb{F}_2^m, \mathbb{F}_2) = 2^m$.

   (b) Es sei

   $$\mathcal{P}(r,m) := \{ f \in \mathbb{F}_2[T_1, \ldots, T_m] \; ; \; f = \sum_{\rho=0}^{r} \sum_{1 \leq i_1 < \ldots < i_\varrho \leq m} a_{i_1,\ldots,i_\rho} T_{i_1} \cdot \ldots \cdot T_{i_\rho} \}$$

   Dann ist die Abbildung $\Phi \,\big|\, \mathcal{P}(r,m)$ injektiv.

   (c) Das Bild

   $$\mathcal{R}(r,m) := \Phi(\mathcal{P}(r,m))$$

   ist ein Untervektorraum mit

   - Dimension $k = \binom{m}{0} + \ldots + \binom{m}{r}$.
   - Minimalabstand $d = 2^{m-r}$; d.h. für je zwei Polynome $f, g \in \mathcal{P}(r,m)$ mit $f \neq g$ unterscheiden sich $\Phi(f)$ und $\Phi(g)$ an mindestens d Positionen.

   Hinweis: Für den Minimalabstand zeigen Sie:

   $$d\,(\mathcal{R}(r,m)) \geq \min \{ 2 \cdot d\,(\mathcal{R}(r,m-1)) \; , \; d\,(\mathcal{R}(r-1,m-1)) \}$$

   indem Sie ein $f \in \mathcal{P}(r,m)$ in $f = g + T_m \cdot h$ zerlegen, wobei g und h unabhängig von T_m sind.

   (d) Indem man z.B. 64 Farbstufen als die Elemente des $\mathbb{F}_2^6$ interpretiert, kann man eine Farbstufe c auch als ein Element f_c von $\mathcal{P}(1,5)$ auffassen. Für die Übertragung von c benutzt man nun $\Phi(f_c)$; man baut also Redundanz ein und stabilisiert dadurch die Übertragung gegen Rauschen.

   Wie viele Fehler kann man so in einem übertragenen Wort reparieren, wenn es durch Rauschen gestört wurde?

   Was leistet der Code bei Übertragung von Bildern in 64 Farbstufen, falls durch Rauschen bei der Übertragung höchstens 10% der Zeichen in einem Wort falsch übertragen werden?