

WS 2005/06

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2005WS/ds/index.html.de>

9. Dezember 2005

Satz 155

Sei $g \in K[x]$, $\text{grad}(g) \geq 1$. Dann gilt:

$K[x]/(g)$ ist ein Körper $\Leftrightarrow g$ ist irreduzibel.

Beweis:

“ \Rightarrow ” Sei $K[x]/(g)$ ein Körper. Angenommen, g ist **nicht** irreduzibel.

Dann gibt es $g_1, g_2 \in K[x]$ mit $g = g_1 \cdot g_2$ und $\text{grad}(g_1), \text{grad}(g_2) \geq 1$.

Da $d := \text{grad}(g) = \text{grad}(g_1) + \text{grad}(g_2)$, folgt $\text{grad}(g_1) < d$ und $\text{grad}(g_2) < d$. Also gilt $[g_1]_g \neq [0]_g$ und $[g_2]_g \neq [0]_g$.

Jedoch ist

$$[g_1]_g \cdot [g_2]_g = [g_1 g_2]_g = [g]_g = [0]_g,$$

d.h. $[g_1]_g$ und $[g_2]_g$ sind **Nullteiler**. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 120).

“ \Leftarrow ” Sei g irreduzibel, und sei $[f]_g \neq [0]_g$ gegeben.
 $[f]_g \neq [0]_g$ bedeutet, dass f nicht durch g teilbar ist. Da g irreduzibel ist, sind f und g daher teilerfremd.
Somit existieren Polynome $p, q \in K[x]$ mit $pf + qg = 1$, und es folgt

$$\begin{aligned} [p]_g \cdot [f]_g &= [pf]_g = [1 - qg]_g = [1]_g - \underbrace{[qg]_g}_{=[0]_g} \\ &= [1]_g . \end{aligned}$$

Also ist $[p]_g = ([f]_g)^{-1}$.



3.7 Konstruktion endlicher Körper

Satz 156

Zu jeder Primzahl p und zu jeder natürlichen Zahl $n \geq 1$ gibt es einen endlichen Körper mit p^n Elementen; dieser wird mit $GF(p^n)$ bezeichnet ($GF = \text{Galois Field}$, nach *Evariste Galois* (1811–1832)).

Beweis:

- $n = 1$: $\mathbb{Z}_p = GF(p)$ ist ein Körper mit p Elementen.
- $n > 1$: Sei $K = \mathbb{Z}_p$. Sei $g \in K[x]$ ein *irreduzibles* Polynom vom Grad n (zur Existenz eines solchen Polynoms: siehe Bemerkung unten).
Nach Satz 155 ist $K[x]/(g)$ ein Körper, und nach Satz 153 hat $K[x]/(g)$ genau p^n Elemente.



Satz 157

Je zwei endliche Körper mit p^n Elementen sind *isomorph*.

Beweis:

siehe geeignetes Textbuch zur Algebra oder Zahlentheorie,
ebenfalls bzgl. der Existenz irreduzibler Polynome! □

Beispiel 158

Wir betrachten den Fall $K = \mathbb{Z}_3 = GF(3)$ und $p(x) = x^2 + 1$.

Der Ring $\mathbb{Z}_3[x]/(p)$ besteht also aus allen Polynomen in $\mathbb{Z}_3[x]$ vom Grad ≤ 1 :

$$\mathbb{Z}_3[x]/(p) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\} .$$

Bemerkung zur Notation: Wir schreiben hier (und auch sonst) das Polynom f statt der Restklasse $[f]_g$.

Das Polynom p ist irreduzibel. **Wieso?**

Beispiel 159

Für $K = \mathbb{Z}_2 = GF(2)$ und $p(x) = x^2 + x + 1$ gilt in ähnlicher Weise

$$\mathbb{Z}_2[x]/(p) = \{0, 1, x, x + 1\} .$$

Für die Addition und Multiplikation modulo p ergibt sich

$+_p$	0	1	x	$x + 1$	\cdot_p	0	1	x	$x + 1$
0	0	1	x	$x + 1$	0	0	0	0	0
1	1	0	$x + 1$	x	1	0	1	x	$x + 1$
x	x	$x + 1$	0	1	x	0	x	$x + 1$	1
$x + 1$	$x + 1$	x	1	0	$x + 1$	0	$x + 1$	1	x

Aus diesen beiden Tabellen folgt, dass $\mathbb{Z}_2[x]/(p)$ mit den angegebenen Verknüpfungen $+_p$ und \cdot_p einen Körper mit **4 Elementen** bildet (den wir schon früher gesehen haben).

Beispiel 160

Für $K = \mathbb{Z}_2$ und $q(x) = x^2 + 1$ gilt wiederum

$$\mathbb{Z}_2[x]/(q) = \{0, 1, x, x + 1\} .$$

Für die Addition und Multiplikation modulo q ergibt sich nunmehr jedoch

$+_q$	0	1	x	$x + 1$
0	0	1	x	$x + 1$
1	1	0	$x + 1$	x
x	x	$x + 1$	0	1
$x + 1$	$x + 1$	x	1	0

\cdot_q	0	1	x	$x + 1$
0	0	0	0	0
1	0	1	x	$x + 1$
x	0	x	1	$x + 1$
$x + 1$	0	$x + 1$	$x + 1$	0

Aus der zweiten Tabelle folgt, dass $\mathbb{Z}_2[x]/(q) \setminus \{0\}$ bzgl. \cdot_q **keine Gruppe** bildet. Der Grund ist, dass q nicht irreduzibel ist.

3.8 Redundante Datenspeicherung und Fehlerkorrektur

Seien natürliche Zahlen k, t und s so gewählt, dass

$$k + 2t \leq 2^s - 1.$$

Sei weiter $K = GF(2^s)$, und seien $c_0, \dots, c_{k-1} \in K$. Wir fassen die c_i sowohl als Elemente von K als auch (in frei festzulegender, eindeutiger Weise) als *Binärwörter der Länge s* auf.

Sei weiter α ein primitives Element in $K = GF(2^s)$ (existiert nach Satz 124) und seien

$$g(x) := \prod_{i=1}^{2t} (x - \alpha^i),$$

$$c(x) := \sum_{i=0}^{k-1} c_i x^i, \text{ und}$$

$$d(x) = \sum_{i=0}^{k+2t-1} d_i x^i := g(x) \cdot c(x).$$

Wir sagen, dass der Vektor der Koeffizienten von $d(x)$ den Vektor (c_0, \dots, c_{k-1}) **kodiert** (**Reed-Solomon-Code** $RS(s, k, t)$).

Satz 161

Für jedes $s \in \mathbb{N}$ und $k, t \in \mathbb{N}$ mit $k + 2t \leq 2^s - 1$ ist der Reed-Solomon-Code $RS(s, k, t)$ *t-fehlerkorrigierend* und *2t-fehlererkennend*.

Das bedeutet, dass, falls bei der Übertragung des Vektors der d_i nicht mehr als $2t$ der d_i 's verändert werden, dies **erkannt** werden kann. Werden höchstens t der d_i 's verändert, so können die ursprünglichen d_i 's sogar **rekonstruiert** werden.

Beweis:

Sei (f_0, \dots, f_{k+2t-1}) der sich nach der Übertragung ergebende Code-Vektor, sei $e_i := f_i - d_i$ für $i = 0, \dots, k + 2t - 1$, und seien

$$e(x) := \sum_{i=0}^{k+2t-1} e_i x^i \quad \text{und} \quad f(x) := \sum_{i=0}^{k+2t-1} f_i x^i .$$

Dann gilt $f(x) = d(x) + e(x)$, und es folgt

$$f(\alpha^i) = e(\alpha^i) \quad \text{für alle } 1 \leq i \leq 2t .$$

In Matrixschreibweise sieht dies wie folgt aus:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(k+2t-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(k+2t-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \alpha^{6t} & \dots & \alpha^{2t(k+2t-1)} \end{pmatrix} \cdot \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{k+2t-2} \\ e_{k+2t-1} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$

Falls nur e_{i_1}, \dots, e_{i_r} ungleich 0 sind, fallen Spalten weg und es ergibt sich

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \dots & \alpha^{3i_r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2ti_1} & \alpha^{2ti_2} & \dots & \alpha^{2ti_r} \end{pmatrix} \cdot \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$

Immer wenn die Anzahl r der Spalten \leq der Anzahl $2t$ der Zeilen ist, hat diese Matrix vollen Spaltenrang (Vandermonde-Matrix).

- Wenn $(e(\alpha^i) =) f(\alpha^i) = 0$ für $i = 1, \dots, 2t$, dann ist $e_i = 0$ für alle i eine Lösung, und zwar dann die einzige (Spaltenrang).
- Falls $\leq t$ Fehler aufgetreten sind, können wir entsprechende e_{i_j} eindeutig bestimmen (z.B. durch Probieren) und damit die d_i rekonstruieren.

