3. „Kongruenz modulo g“ definiert auf $K[x]$ eine Äquivalenzrelation $\sim_g$: $h \sim_g f \iff h - f$ ist durch g teilbar, und $[f]_g$ ist die Äquivalenzklasse von f.
4. Auf der Menge aller Restklassen $[f]_g$ kann man Addition und Multiplikation wie folgt definieren

$$[f]_g + [h]_g := [f + h]_g, \qquad [f]_g \cdot [h]_g := [f \cdot h]_g,$$

und erhält einen kommutativen Ring; er heißt der Restklassenring $K[x]$ modulo g und wird mit $K[x]/(g)$ bezeichnet.

3.6.2 Eigenschaften von Restklassenringen

Teilt man Polynome durch ein fest gewähltes Polynom g, $\mathrm{grad}(g) \geq 1$, so treten als Reste sämtliche Polynome vom Grad $< d = \mathrm{grad}(g)$ auf. Deshalb setzen wir

$$K[x]_d := \{h \in K[x] : \mathrm{grad}(h) < d\},$$

und definieren auf $K[x]_d$ Addition $+_g$ und Multiplikation $\cdot_g$ wie folgt:

Mit $Rem(f)$ bezeichnen wir den Rest der Polynomdivision von f durch g.

$$f +_g h := f + h, \qquad f \cdot_g h := Rem(f \cdot h).$$

Man prüft leicht nach, dass $(K[x]_d, +_g, \cdot_g)$ ein kommutativer Ring ist.

Satz 155

Sei $g \in K[x]$ ein Polynom, $d = \mathrm{grad}(g) \geq 1$. Dann ist die Abbildung

$$(K[x]/(g), +, \cdot) \to (K[x]_d, +_g, \cdot_g), \quad [f]_g \mapsto Rem(f)$$

ein Ringisomorphismus, die Umkehrabbildung ist gegeben durch $r \mapsto [r]_g$.

Beweis:

Es gilt

1. $$[f]_g = [0]_g \iff g|f \iff Rem(f) = 0$$

2. $$[f]_g + [h]_g = [f+h]_g \mapsto Rem(f+h) = Rem(f) + Rem(h) = Rem(f) +_g Rem(h)$$

3. $$[f]_g \cdot [h]_g = [f \cdot h]_g \mapsto Rem(f \cdot h) = Rem(Rem(f) \cdot Rem(h)) = Rem(f) \cdot_g Rem(h).$$

Aus (1) - (3) folgt, dass obige Abbildung wohldefiniert, injektiv und ein Ringhomomorphismus ist; sie ist auch surjektiv, denn für $f \in K[x]_d$ ist $Rem(f) = f$. □

Satz 156

Sei K ein Körper mit n Elementen, und sei $g \in K[x]$, $d = \mathrm{grad}(g) \geq 1$. Dann besitzt $K[x]/(g)$ genau n^d Elemente.

Beweis:

Nach Satz 155 ist $|K[x]/(g)| = |K[x]_d|$, und offensichtlich gilt $|K[x]_d| = n^d$. □

Definition 157

Ein Polynom $g \in K[x]$ heißt irreduzibel, falls $\mathrm{grad}(g) \geq 1$ gilt und aus $g = g_1 \cdot g_2$ mit $g_1, g_2 \in K[x]$ stets $\mathrm{grad}(g_1) = 0$ oder $\mathrm{grad}(g_2) = 0$ folgt; ansonsten heißt g reduzibel.

Satz 158

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

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

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 $\mathrm{grad}(g_1), \mathrm{grad}(g_2) \geq 1$.
Da $d := \mathrm{grad}(g) = \mathrm{grad}(g_1) + \mathrm{grad}(g_2)$, folgt $\mathrm{grad}(g_1) < d$ und $\mathrm{grad}(g_2) < d$.
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 123).

Beweis (Forts.):

"$\Leftarrow$" 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 159

*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 = **G**alois **F**ield, 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 158 ist $K[x]/(g)$ ein Körper, und nach Satz 156 hat $K[x]/(g)$ genau p^n Elemente.

□

Satz 160

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 161

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 162

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	$x+1$
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

$\cdot_p$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	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 163

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 $c_0, \ldots, c_{k-1} \in K$. 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 127) und seien

$$
\begin{aligned}
g(x) &:= \prod_{i=1}^{2t}(x-\alpha^i)\ , \\
c(x) &:= \sum_{i=0}^{k-1} c_i x^i\ , \text{ und} \\
d(x) = \sum_{i=0}^{k+2t-1} d_i x^i &:= g(x)\cdot c(x)\ .
\end{aligned}
$$

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

Satz 164

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

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

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

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

Beweis (Forts.):

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

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

Beweis (Forts.):

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 $i = 1, \ldots, 2t$, 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.

□

4. Die elementaren Zählfunktionen

4.1 Untermengen

Definition 165 (Binomialkoeffizienten)

$$\binom{n}{0} := 1 \qquad \forall n \in \mathbb{N}_0$$

$$\binom{n}{k} := 0 \qquad n < k, n \in \mathbb{N}_0, k \in \mathbb{N}$$

$$\binom{n}{k} := \binom{n-1}{k} + \binom{n-1}{k-1} \qquad \text{sonst} \quad (n, k \in \mathbb{N})$$

Satz 166

Sei N eine Menge mit $|N| = n$ Elementen. Die Menge aller k-elementigen Untermengen von N wird bezeichnet mit

$$\binom{N}{k}.$$

Es gilt:

$$\left|\binom{N}{k}\right| = \binom{|N|}{k} = \binom{n}{k}.$$

Beweis:

Seien $n, k \geq 0$, $a \in N$.

1. $\binom{n}{0}$ und $k > n$ sind klar.
2. Definiere

$$S_a := \left\{ A \in \binom{N}{k};\ a \in A \right\},$$
$$\tilde{S}_a := \left\{ A \in \binom{N}{k};\ a \notin A \right\}.$$

Beweis (Forts.):

3. Damit gilt

$$S_a \cup \tilde{S}_a = \binom{N}{k}, \quad S_a \cap \tilde{S}_a = \emptyset.$$

$$|S_a| = \left|\binom{N \setminus \{a\}}{k-1}\right| = \binom{n-1}{k-1} \quad \text{(per Induktion)}$$

$$|\tilde{S}_a| = \left|\binom{N \setminus \{a\}}{k}\right| = \binom{n-1}{k} \quad \text{(per Induktion)}$$

Daraus folgt

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

□