fhwedel
UNIVERSITY OF APPLIED SCIENCES

Endliche Körper

Seminar: Diskrete Mathematik
Leitung: Prof. Dr. Rainer Lang
Von: Steffen Lohrke (ii5105)
SS2005

Inhaltsverzeichnis

Abelsche Gruppe

Eine Abelsche Gruppe ist eine algebraische Struktur, die aus einer Menge K und einer Verknüpfung * besteht. Die Verknüpfung entspricht einer Abbildung der folgenden Form:

$$V: K \times K \rightarrow K$$

Außerdem müssen die folgenden Eigenschaften gelten:

Abgeschlossenheit:	$\forall\, a, b \in K: \; a * b \in K$
Assoziativgesetz:	$\forall\, a, b, c \in K: a * (b * c) = (a * b) * c$
Existenz eines neutralen Elements e:	$\forall\, a \in K: \exists\, e \in K: a * e = a$
Existenz eines inversen Elements b:	$\forall\, a \in K: \exists\, b \in K: a * b = e$
Kommuntativgesetz:	$\forall\, a, b \in K: a * b = b * a$

Anmerkung: Die Verknüpfung * kann für eine additive oder eine multiplikative Verknüpfung stehen. Im folgenden wird das Symbol * als Multiplikationszeichen verwendet.

Gilt das nur Kommuntativgesetz nicht, dann ist diese Struktur nur eine Gruppe und keine abelsche Gruppe.

Schreibweise: (*Menge*, *Verknüpfung*)

Einige einfache Beispiele:

($\mathbb{Z}$, +) Menge aller ganzen Zahlen. Es kann addiert und mit Hilfe der inversen Elemente subtrahiert werden.
Neutrales Element: 0
Inverses Element z.B. von 2: -2

($\mathbb{R}$, +) Menge aller reelen Zahlen. Es kann addiert und mit Hilfe der inversen Elemente subtrahiert werden.
Neutrales Element: 0
Inverses Element z.B. von 1,5: -1,5

$(\mathbb{Q}\backslash\{0\}, *)$ Menge aller rationalen Zahlen ohne Null. Es kann multipliziert und mit Hilfe der inversen Elemente dividiert werden. Die Null darf aus dem selben Grund wie im 3. Beispiel nicht in der Menge enthalten sein.
Neutrales Element: 1
Inverses Element z.B. von 3/4: 4/3

$(\mathbb{Q}^-, *)$ Menge aller positiven rationalen Zahlen. Es kann multipliziert und mit Hilfe der inversen Elemente dividiert werden.
Neutrales Element: 1
Inverses Element z.B. von -2/5: -5/2

Keine (abelsche) Gruppen sind:

$(\mathbb{N}, +)$, $(\mathbb{R}^+, +)$, $(\mathbb{Q}^-, +)$, $(\mathbb{Z}\backslash\{0\}, *)$

In jeder dieser Mengen gibt es Elemente, deren inverses Element bezüglich der jeweiligen Verknüpfung nicht in der Menge enthalten ist.

$(\mathbb{Z}\backslash\{1\}, +)$

Die Menge $\mathbb{Z}\backslash\{1\}$ bildet bezüglich der Addition keine Gruppe, da diese nicht Abgeschlossen wäre: $3 + (-2) = 1$

Kommutativer Ring

Ein kommutativer Ring ist eine algebraische Struktur, die aus einer Menge K und einer additiven und einer multiplikativen Verknüpfung ($\oplus$, $\otimes$) besteht. Die Verknüpfungen entsprechen einer Abbildung der folgenden Form:

$$V: K \times K \rightarrow K$$

Des weiteren müssen folgende eigenschaften gelten:

(K, $\oplus$) ist eine Abelsche Gruppe, das neutrale Element wird als Null bezeichnet.

Abgeschlossenheit:	$\forall$ a, b $\in$ K: a $\otimes$ b $\in$ K
Assoziativgesetz:	$\forall$ a, b, c $\in$ K: a $\otimes$ (b $\otimes$ c) = (a $\otimes$ b) $\otimes$ c
Existenz eines neutralen Elements e:	$\forall$ a, b $\in$ K: $\exists$ e $\in$ K: a $\otimes$ e = a
Kommuntativgesetz:	$\forall$ a, b $\in$ K: a $\otimes$ b = b $\otimes$ a
Distributivgesetz: $\forall$ a, b, c $\in$ K:	a $\otimes$ (b $\oplus$ c) = (a $\otimes$ b) $\oplus$ (a $\otimes$ c)
	(b $\oplus$ c) $\otimes$ a = (b $\otimes$ a) $\oplus$ (c $\otimes$ a)

Schreibweise: (*Menge*, *Verknüpfung1*, *Verknüpfung2*)

In einem Ring kann also addiert, multipliziert und subtrahiert werden. Nur die Division ist nicht möglich, da keine inversen Elemente bzgl. der Multiplikation in der Menge K enthalten sein müssen.
Gilt das Kommutativgesetz nicht, so handelt es sich nur um einen Ring.

Beispiele für einen Ring:

($\mathbb{R}$, +, *), ($\mathbb{Q}$, +, *), ($\mathbb{Z}$, +, *)

Gegenbeispiele:

($\mathbb{N}$, +, *), ($\mathbb{R}^+$, +, *)

In diesen beiden Beispielen existieren keine inversen Elemente bzgl. der Addition.

Körper

Ein Körper ist eine algebraische Struktur, die aus einer Menge K und einer additiven und einer multiplikativen Verknüpfung ($\oplus$, $\otimes$) besteht. Die Verknüpfungen entsprechen einer Abbildung der folgenden Form:

$$V: K \times K \rightarrow K$$

Des weiteren müssen folgende eigenschaften gelten:

(K, $\oplus$) ist eine Abelsche Gruppe, das neutrale Element wird als Null bezeichnet.

(K\{0},$\otimes$) ist eine Abelsche Gruppe, das neutrale Element wird als Eins bezeichnet.

Distributivgesetz: $\forall$ a, b, c $\in$ K: $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$

$(b \oplus c) \otimes a = b \otimes a \oplus c \otimes a$

Ein Körper ist also ein kommutativer Ring in dem es auch zu jedem Element aus K ein inverses Element bzgl. der Multiplikation gibt.

Schreibweise: (*Menge*, *Verknüpfung1*, *Verknüpfung2*)

In einem Körper kann addiert, subtrahiert, multipliziert und dividiert werden.

Beispiele:

($\mathbb{R}$, +, *), ($\mathbb{Q}$, +, *)

Gegenbeispiele:

($\mathbb{N}$, +, *) In diesem Beispiel fehlen die inversen Elemente bzgl. der Multiplikation und der Addition.

($\mathbb{R}^+$, +, *) ($\mathbb{R}^+$, +) ist keine Gruppe.

($\mathbb{Z}$, +, *) ($\mathbb{Z}\backslash\{0\}$, *) ist keine Gruppe.

Endliche Körper

Ein endlicher Körper ist ein Körper, wobei die Anzahl der Elemente der Menge K endlich ist. Endliche Körper werden auch nach dem französischem Mathematiker Everiste Galois „Galoiskörper“ (engl. Galois field) genannt.

Everiste Galois wurde im Jahr 1811 geboren und starb 1832 im alter von 20 Jahren in einem Duell. Er legte die Grundlagen für die Theorie der endlichen Körper.

Beispiel des endlichen Körpers ($\mathbb{Z}_2, +_2, *_2$):

Die Menge der Restklassen $\mathbb{Z}_2$ bilden mit der Addition und der Multiplikation einen endlichen Körper. Die Menge $\mathbb{Z}_2$ enthält die folgenden Restklassen als Elemente:

$[0]_2$, $[1]_2$ mit $[0]_2$ = { ..., -4, -2, 0, 2, 4, ...} und $[1]_2$ = { ..., -3, -1, 1, 3, 5, ...}

Die Addition und die Multiplikation werden mit Hilfe von Tabellen dargestellt.
Es ist üblich in diesen Tabellen nur den Restklassenanführer der Restklasse als Element des Körpers zu schreiben:

$+_2$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	0	0
1	0	1

Die Zahlen stehen insofern nur als Symbole in den Tabellen. Ersetzt man jedoch die Addition und Multiplikation durch eine Addition bzw. Multiplikation modulu 2 (2 da $\mathbb{Z}_2$), so können diese Symbole auch als Zahlen aufgefasst werden und dem entsprechend mit ihnen gerechnet werden.

Dieser endliche Körper wird auch mit GF(2) bezeichnet (von Galois field).

Der endlichen Körper GF(3) bzw. ($\mathbb{Z}_3$, $+_3$, $*_3$):

Elemente des Körpers: $\mathbb{Z}_3 = \{[0]_3 , [1]_3 , [2]_3\}$

Additions und Multiplikationstabellen:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Aus diesen Tabellen können unmittelbar die inversen Elemente entnommen werden. So ist z.B. das inverse Element von 1 bzgl. der Addition die 2, da 1 + 2 mod 3 = 0 ist.
Es ist ebenfalls ersichtlich, dass die Verknüpfungen kommutativ sind, da die Tabellen bzgl. der Hauptdiagonalen symmetrisch sind.

Man könnte nun annehmen, dass jede Struktur ($\mathbb{Z}_n$, $+_n$, $*_n$) mit $n \in \mathbb{N}$ und $n > 1$ einen endlichen Körper bildet. Dass dies nicht stimmt, erkennt man an dem nachfolgendem Beispiel.

($\mathbb{Z}_4$, $+_4$, $*_4$):

Additions und Multiplikationstabellen:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

An der hervorgehobenen Spalte bzw. Zeile ist erkennbar, dass es kein inverses Element bzgl. der Multiplikation für die 2 gibt. Daher ist ($\mathbb{Z}_4$, $+_4$, $*_4$) kein Körper.
Außerdem sind endliche Körper Nullteilerfrei. D.h. wenn zwei von Null verschiedene Elemente des Körpers miteinander multipliziert werden darf das Ergebnis nicht Null sein. Dies wird im folgenden bewiesen.

Für den Beweis der Nullteilerfreiheit von Körpern muß zuvor bewiesen werden, dass das Ergebnis einer Multiplikation eines beliebigen Elementes des Körpers mit der Null Null ergibt:

Lemma:

In jedem Körper K gilt: $\forall a \in K: \quad a * 0 = 0 * a = 0$

Beweis:

$0 + (a * 0)$

$= a * 0$ Null ist das neutrale Element bzgl. der Addition

$= a * (0 + 0)$ Null ist das neutrale Element bzgl. der Addition

$= (a * 0) + (a * 0)$ Distributivgesetz

$\Rightarrow \quad 0 = a * 0$

Lemma (Beweis der Nullteilerfreiheit):

In jedem Körper K gilt: $\forall a, b \in K: \; a * b = 0 \quad \Rightarrow \quad a = 0 \vee b = 0$

Beweis: Wenn $a \neq 0$, dann existiert auch das inverse Element a^{-1}.

b

$= 1 * b$ Eins ist das neutrale Element bzgl. der Multiplikation

$= a^{-1} * a * b$ $a^{-1} * a = 1$ (Definition)

$= a^{-1} * 0$ $a * b = 0$ (laut der Annahme)

$= 0$ nach obigem Lemma

$\Rightarrow \quad b = 0$

Es stellt sich nun die Frage für welche n $(\mathbb{Z}_n, +_n, *_n)$ ein Körper ist:

Satz:

Bezeichnet man mit $+_n$ und $*_n$ die Addition bzw. die Multiplikation modulo n, so gilt:

$(\mathbb{Z}_n, +_n, *_n)$ ist ein Körper $\quad \Leftrightarrow \quad$ n ist Primzahl

Begründung:

Wenn $(\mathbb{Z}_n, +_n, *_n)$ ein Körper ist, ergibt sich, dass n eine Primzahl sein muß, da es ansonsten Nullteiler gibt.

Dass es zu jeder Primzahl n einen Körper $(\mathbb{Z}_n, +_n, *_n)$ gibt, wird hier auf die Frage reduziert, ob es zu jedem Element des Körpers ein inverses Element bzgl. der Multiplikation gibt. Hierzu wird der folgende satz von Euklid verwendet:

Für alle $a, n \in \mathbb{N}, a \leq n$ gibt es $x, y \in \mathbb{Z}$ mit $ggT(a,n) = a * x + n * y$

Da in diesem Fall n eine Primzahl ist und a als beliebiges Element des Körpers echt kleiner als n ist, ist der größte gemeinsame Teiler von a und n die 1. Es ergibt sich also folgende Gleichung.

$$a*x + n*y = 1$$

Nun addiert man auf die linke Seite $+k*n*a \; -k*n*a$ mit $k \in \mathbb{Z}$:

$$a*x + n*y + k*n*a - k*n*a = 1$$
$$\Leftrightarrow \quad a*(x + k*n) + n*(y - k*a) = 1$$

Es kann nun k so gewählt werden, dass $x + k*n$ ein Element des Körpers ist.
Die Addittion von $n\,(y - k*a)$ entspricht einer modulo Operation.
Also ist $(x + k*n)$ das inverse Element zu a.

Beispiel:

$n=7, a=3 \quad \Rightarrow \quad 3*x + 7*y = 1$
Mögliche Lösung für x und y: $x = 12$ und $y = -5$
$\Rightarrow \quad 3*12 + 7*(-5) = 1$
$\Leftrightarrow \quad 3*(12 + k*7) + 7*(-5 - k*3) = 1$

k so wählen, so dass gilt: $0 \leq (12 + k*7) \leq 6 \quad \Rightarrow k = -1$

$\Rightarrow \quad 3*5 + 7*(-2) = 1$

Also ist das Element 5 das inverse Element bzgl. der Multiplikation zu dem Element 3 im GF(7).

Endliche Körper mit p^k Elementen

Neben den schon vorgestellten endlichen Körpern mit einer primen Anzahl an Elementen können auch Körper mit p^k Elementen konstruiert werden, wobei p prim und k ein Element der natürlichen Zahlen sein muss. Zwar ist ($\mathbb{Z}_4$, $+_4$, $*_4$) kein Körper, so gibt es trotzdem einen Körper mit vier Elementen (2^2):

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

*	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Überprüft man diesen Körper mit den Elementen 0, 1, a, b und den angegebenen Verknüpfungstabellen, so wird man feststellen, dass alle Eigenschaften eines Körpers eingehalten worden sind.

Konstruktion

Körper mit einer nicht primen Anzahl an Elementen können mit Hilfe von Polynomen konstruiert werden. Zunächst definiert man folgende Menge aller Polynome mit Koeffizienten in K:

$$K[x] := \{ \sum_{i=0}^{n} a_i x^i , n \in \mathbb{N}_0 , a_i \in K \text{ und } a_n \neq 0 \text{ oder } n = 0 \}$$

Beispiele:

$\mathbb{Z}_2[x] = \{0, 1, x, x + 1, x^2, x^2 + 1, x^3, x^3 + 1, x^4, \dots \}$

$\mathbb{Z}_3[x] = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x+2, x^2, x^2 + 1, \dots \}$

K[x] bildet einen Ring. Damit man jedoch ein endlichen Körper erhält, wird zusätzlich ein irreduzibles Polynom über K benötigt.

Definition:

Ein Polynom $p(x) \in K[x]$ mit $p(x) \neq 0$ heißt irreduzibel über K, falls gilt:

$p(x) = f(x) * g(x)$ mit $f(x), g(x) \in K[x] \Rightarrow \text{grad}(f)=0$ oder $\text{grad}(g)=0$.

Beispiel:

Das Polynom $x^2 + 1$ ist irreduzibel über $\mathbb{Z}_3$. Es ist jedoch nicht irreduzibel über $\mathbb{Z}_2$, da $(x + 1) * (x + 1) = x^2 + 2x + 1 = x^2 + 1$ ist. In diesem Fall wird aus 2x Null, da der Koeffizient 2 nicht in $\mathbb{Z}_2$ enthalten ist, also eine modulo 2 Operation durchgeführt wird. (bzw. die 2 ist in der Restklasse $[0]_2$ enthalten).

Eine einfache Möglichkeit zu überprüfen, ob ein Polynom p(x) über $\mathbb{Z}_n$ irreduzibel ist, besteht darin, dass man folgende Eigenschaft prüft:

$\forall a \in \mathbb{Z}_n$: p(a) modulo $n \neq 0$

Beispiel:

$p(x) = x^2 + 1$ mit Koeffizienten in $\mathbb{Z}_2$:
$p(0) = (0^2 + 1) \bmod 2 = 1 \bmod 2 = 1$
$p(1) = (1^2 + 1) \bmod 2 = 2 \bmod 2 = 0$ $\Rightarrow$ p(x) ist nicht irreduzibel

$p(x) = x^2 + 1$ mit Koeffizienten in $\mathbb{Z}_3$:
$p(0) = (0^2 + 1) \bmod 3 = 1 \bmod 3 = 1$
$p(1) = (1^2 + 1) \bmod 3 = 2 \bmod 3 = 2$
$p(2) = (2^2 + 1) \bmod 3 = 5 \bmod 3 = 2$ $\Rightarrow$ p(x) ist irreduzibel

Mit Hilfe eines irreduziblen Polynoms kann nun ein Körper konstruiert werden:

Beispiel:

$(\mathbb{Z}_2[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ mit $p(x) = x^3 + x^2 + 1$

Die Elemente des Körpers sind alle Polynome in $\mathbb{Z}_2$, deren Grad echt kleiner sind, als der Grad von p(x). In diesem Beispiel gibt es also 2^3 Elemente:

$\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$

Adition

Das Ergebnis der Addition zweier Polynome $p_1(x)$ und $p_2(x)$ wird wir folgt berechnet:

$$p_1(x) = \sum_{i=0}^{k-1} a_i x^i \; mit \; a_i \in \mathbb{Z}_n \quad , p_2(x) = \sum_{i=0}^{k-1} b_i x^i \; mit \; b_i \in \mathbb{Z}_n$$

$$P_{sum}(x) = p_1(x) + p_2(x) = \sum_{i=0}^{k-1} \left((a_i + b_i) \bmod n \right) * x^i \; mit \; a_i, b_i \in \mathbb{Z}_n$$

Anm.: k ist der Grad des irreduziblen Polynoms p(x).

Für das obige Beispiel ergibt sich daraus folgende Additionstabelle:

$+_{x^3+x^2+1}$	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	x+1	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	x+1	0	1	x^2+x	x^2+x+1	x^2	x^2+1
x+1	x+1	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	x+1
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	x+1	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	x+1	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	x+1	x	1	0

Multiplikation

Da das Produkt zweier Polynome ggf. ein Polynom ergibt, welches nicht Element des Körpers ist, muß dieses Produkt auf ein Polynom kleineren Grades zurückgeführt werden, dass Element des Körpers ist. Dies erreicht man indem das Produkt mit dem irreduziblen Polynom p(x) dividiert. der Rest der Division ist das gesuchte Element.

$p_{prod}(x) = (p_1(x) * p_2(x)) \bmod p(x)$

Beispiele für den den obigen Körper:

$(x^2+1) * (x^2+x+1) = x^4+x^3+x^2+x^2+x+1 = x^4+x^3+x+1$

$(x^4+x^3+x+1) : (x^3+x^2+1) = x$

$-\underline{(x^4+x+x)}$

$\underline{\mathbf{1}}$

$(x^2+x) * (x^2+x+1) = x^4+x^3+x^2+x^3+x^2+x = x^4+x$

$(x^4+x) : (x^3+x^2+1) = x+1$

$-\underline{(x^4+x^3+x)}$

x^3

$-\underline{(x^3+x^2+1)}$

$\underline{\mathbf{x^2+1}}$

Anm.: Die Subtraktion müsste eigentlich durch die Addition ersetzt werden, indem jeder Koeffizient durch das inverse Element bzgl. der Addition ersetzt wird. Da in diesem Fall die Koeffizienten aus $\mathbb{Z}_2$ stammen, ist dies nicht nötig, weil im $\mathbb{Z}_2$ das Inverse eines Elementes gleich dem Element selber ist. D.h. statt zu subtrahieren wird addiert und modulo 2 gerechnet.

Die vollständige Multiplikationstabelle:

$*_{x^3+x^2+1}$	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	x^2+1	x^2+x+1	1	x+1
x+1	0	x+1	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	0	x^2	x^2+1	1	x^2+x+1	x+1	x	x^2+x
x^2+1	0	x^2+1	x^2+x+1	x	x+1	x^2+x	x^2	1
x^2+x	0	x^2+x	1	x^2+x+1	x	x^2	x+1	x^2+1
x^2+x+1	0	x^2+x+1	x+1	x^2	x^2+x	1	x^2+1	x

Subtraktion

Die Subtraktion wird durch die Addition erstetzt, wobei der Subtrahend durch das inverse Element bzgl. der Addition ersetzt wird. Das inverse Element kann aus der Additionstabelle entnommen werden.

Division

Die Division wird analog zur Subtraktion durch die Multiplikation ersetzt.

Das primitive Element

Satz:

> In jedem endlichen Körper K gibt es mindestens ein
> Element $\alpha \in K\backslash\{0\}$ mit $K\backslash\{0\} = \{\alpha^0, \alpha^1, \ldots, \alpha^{|K|-2}\}$.
> α ist das primitive Element.

Durch Potenzieren des primitiven Elementes eines endlichen Körpers kann jedes Element außer die Null berechnet werden. In der Polynomdarstellung ist z.B. x ein primitives Element:

Beispiel: $(\mathbb{Z}_2[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ mit $p(x) = x^3 + x^2 + 1$

ord	Polynomdarstellung	Tupeldarstellung
0	0	000
α^0	1	100
α^1	x	010
α^2	x^2	001
α^3	$1 + x^2$	101
α^4	$1 + x + x^2$	111
α^5	$1 + x$	110
α^6	$x + x^2$	011

Um z.B. das Element α^5 zu berechenen, teilt man x^5 durch p(x). Der Rest ergibt das Ergebnis (x+1). Anstatt der Polynomschreibweise können die Elemente auch als Tupel dargestellt werden, indem nur die Koeffizienten des Polynoms gechrieben werden.

Die Darstellung der Elemente als eine Potenz des primitiven Elements vereinfacht die Multiplikation. Für Körper $(\mathbb{Z}_n[x]_{p(x)}, +_{p(x)}, *_{p(x)})$, p(x) irreduzibel über $\mathbb{Z}_n$ und Grad(p(x)) = k gilt:

$$\alpha^r * \alpha^s = \alpha^{(r+s) \bmod (n^k-1)}$$

Beispiel:

In einem vorhergehenden Beispiel wurde gezeigt, dass $(x^2+1) * (x^2+x+1) = 1$ ist. Ersetzt man die Polynome durch die entsprechende Potenz des primitiven Elements, so erhält man:

$(x^2+1) = \alpha^3$ und $(x^2+x+1) = \alpha^4$

$\alpha^3 * \alpha^4 = \alpha^{(3+4) \bmod (2^3-1)} = \alpha^{7 \bmod 7} = \alpha^0$

$\alpha^0 = 1$

Satz:

Sei K ein endlicher Körper und p(x) ein Polynom in K[x]. Dann gilt:

$(K[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ ist ein Körper $\Leftrightarrow$ p(x) ist irreduzibel über K[x].

Begründung:

Wenn $(K[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ ein Körper ist, muß p(x) zwangsläufig irreduzibel sein, da es ansonsten Nullteiler geben würde und ein Körper Nullteilerfrei sein muß.

Der umgekehrte Fall, dass aus "p(x) ist irreduzibel über K[x]" folgt $(K[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ ist ein Körper, soll hier nur in sofern gezeigt werden, dass die Existenzs der inversen Elemente bzgl. der Multiplikation nachgewiesen wird:

$p_1(x), p_2(x), f(x) \in K[x]_{p(x)} \backslash \{0\}$

1. $p_1(x) * p_2(x) = 0 \quad \Rightarrow \quad p_1(x) = 0 \vee p_2(x) = 0$ (wg. Nullteilerfreiheit)

2. Für $p_1(x) \neq p_2(x)$ gilt: $f(x) * p_1(x) \neq f(x) * p_2(x)$
   Ansonsten würde gelten:
   $$f(x) * p_1(x) = f(x) * p_2(x) \quad | - f(x) * p_2(x)$$
   $$\Leftrightarrow f(x) * (p_1(x) - p_2(x)) = 0$$
   Damit dieses Produkt zu Null wird, muß - bedingt durch die Nullteilerfreiheit - einer der Multiplikanten Null sein. Da f(x) nach der Voraussetzung ungleich Null ist, kann nur noch $p_1(x) - p_2(x) = 0$ sein. Also müsste $p_1(x) = p_2(x)$ sein, dies jedoch verstößt gegen die Voraussetzung.

3. Da die Multiplikation mit einem beliebigen Polynom f(x) einer Abbildung der Form V: $K[x]_{p(x)} \backslash \{0\} \rightarrow K[x]_{p(x)} \backslash \{0\}$ entspricht, diese Abbildung injektiv ist (siehe 2.), sowie die Definitionsmenge und die Zielmenge gleich viele Elemente enthalten, ist die Abbildung auch bijektiv.
   Daher gibt es auch ein Polynom $p_1(x)$ für das gilt:
   $$p_1(x) * f(x) = 1$$
   $p_1(x)$ ist dann das inverse Element zu f(x) bzgl. der Multiplikation.

Satz:

> Für ein $n \in \mathbb{N}$ gibt es genau einen Körper mit n Elementen, wenn $n = p^k$ für eine Primzahl p und ein $k \in \mathbb{N}$. Sind K1 und K2 zwei endliche Körper mit $|K1| = |K2|$, so gilt $K1 \cong K2$.

Dieser Satz sagt aus, dass es zum einen nur endliche Körper mit einer Primzahlpotenz an Elementen gibt. D.h. es gibt keine Körper mit z.B. 10 oder 14 Elementen. Außerdem existiert zwischen Körpern mit einer gleichen Anzahl an Elementen eine bijektive Abbildung. Diese Körper sind also isomorph.

Anwendungsbeispiel

Endliche Körper werden in der Kryptographie und für Kodierungsverfahren verwendet. Es wird im folgenden ein Beispiel aus der Kodierungstheorie vorgestellt.

Reed-Solomon-Code

Das Reed-Solomon-Code Verfahren ist ein Kodierungsverfahren, dass beispielsweise zum Speicher von Daten auf CD's oder DVD's verwendet wird. Es ermöglicht durch hinzufügen von Zusatzinformationen Fehler zu erkennen und zu reparieren.

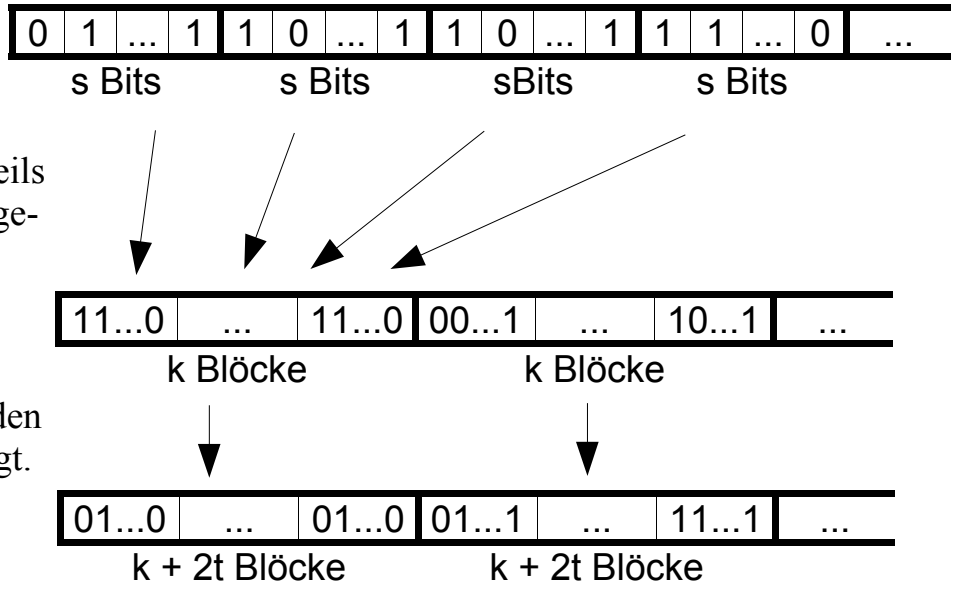
Anm.: Das Verfahren wird mit Hilfe eines Beispiels erläutert. Die vollständigen Rechnungen zu diesem Beispiel befinden sich am Ende dieser Ausarbeitung. Es wird an den entsprechenden Stellen darauf verwiesen.

Für dieses Verfahren müssen die drei Parameter s, k und t festgelegt. Die Wahl ist relativ frei, es müssen jedoch natürlich Zahlen sein und es muß folgende Beziehung gelten:

$$k + 2t \leq 2^s$$

Übersicht – Ablauf Kodierung

Ausgehend von einer Sequenz von Datenbits werden diese in Blöcken zu je s Bits zusammen gefasst.



k dieser bilden eine Einheit, auf die jeweils der Algorithmus angewendet wird.

Aus k Blöcken werden k + 2t Blöcke erzeugt.

Diese Bitsequenz kann nun auf einen Datenträger geschrieben werden.

Kodierung einer aus k Blöcken bestehenden Einheit

Für die Codierung wird jede mögliche Bitsequenz auf ein Element aus einem endlichen Körper mit 2^s Zeichen bijektiv abgebildet. Außerdem werden die k Blöcke einer Einheit durchnummeriert. So können die k Blöcke auch als eine Folge von Elementen des Körpers $(\mathbb{Z}_2[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ Grad(p(x)) = s dargestellt werden:

$c_1, ..., c_i, ... c_k$ mit $c_i \in \mathbb{Z}_2[x]_{p(x)}$

Beispiel:

Parameter s = 4, k = 4, t = 2	
Zu kodierende Bitsequenz:	0101110110100011
Unterteilen in 4 Blöcke zu je 4 Bits:	0101 1101 1010 0011
Abbilden der Bitsequenzen auf ein Element aus $\mathbb{Z}_2[x]_{p(x)}$: (siehe Anlagen A, B)	α^{10} α^5 α^9 α^{14}

Nun wird aus der Folge der Elemente ein Polynom in x vom Grad k-1 erzeugt:

$$c(x) := \sum_{i=0}^{k-1} c_{i+1} x^i$$

Beispiel:

α^{10} α^5 α^9 α^{14} $\Rightarrow$ $c(x) = x^3 \alpha^{14} + x^2 \alpha^9 + x^1 \alpha^5 + x^0 \alpha^{10}$

Außerdem wird das folgende Polynom 2t-ten Grades benötigt:

$$g(x) := (x - \alpha^1) * (x - \alpha)^2 * ... * (x - \alpha)^{2t}$$

Beispiel (t = 2):

$g(x) = (x - \alpha^1) * (x - \alpha^2) * (x - \alpha^3) * (x - \alpha^4)$

Anschließend werden die beiden Polynome miteinander Multipliziert. Es entsteht dabei das polynom d(x) mit dem Grad 2t+k–1. Die Koeffizienten sind ebenfalls Elemente des Körpers. Durch die Abbildung der Koeffizienten von d(x) auf die entsprechenden Bitfolgen erhält man den kodierten Datensatz der beispielsweise auf einer CD gespeichert werden kann.

$$d(x) := c(x) * g(x)$$

$$d(x) = \sum_{i=0}^{2t+k-1} d_{i+1} x^i$$

Beispiel:

$d(x) = c(x) * g(x) = x^7 \alpha^{14} + x^6 \alpha^{10} + x^5 \alpha^0 + x^4 \alpha^1 + x^3 \alpha^5 + x^2 \alpha^0 + x^1 \alpha^{13} + x^0 \alpha^5$
(siehe Anlage C)

Resultierende Bitsequenz:

1101	0110	1000	1101	0100	1000	0101	0011
(α^5	α^{13}	α^0	α^5	α^1	α^0	α^{10}	α^5)

Dekodierung des Datensatzes

Aus den wieder eingelesen Koeffizienten wird das Polynom f(x) gebildet. Sofern kein Fehler aufgetreten ist, ist f(x) = d(x).

$$f(x) = \sum_{i=0}^{2t+k-1} f_{i+1} x^i$$

Definition Fehler:

Ein Fehler liegt vor, wenn ein Koeffizient fehlerhaft ist. Es ist dabei egal, ob ein oder mehrere Bits, die den Koeffizienten repräsentieren, fehlerhaft sind.

Fehlererkennung:

Da das Polynom d(x) durch die Multiplikation von g(x) und c(x) entstanden ist und g(x) die Nullstellen α^1, α^2, ..., α^{2t} besitzt, besitzt auch d(x) diese Nullstelle. Wenn f(x) = d(x) ist müsste also gelten:

$$\forall i \in 1...2t : f(\alpha^i) = 0$$

Stellt sich heraus, das eine oder mehrere der Gleichungen ungleich Null sind, ist f(x) fehlerhaft. Es können so bis zu 2t Fehler erkannt werden. Sind mehr als 2t Koeffizienten falsch, so kann es sein, dass die Fehler nicht erkannt wird.

Beispiel:

$f(x) = x^7 \alpha^{14} + \underline{x^6 \alpha^8} + x^5 \alpha^0 + \underline{x^4 \alpha^0} + x^3 \alpha^5 + x^2 \alpha^0 + x^1 \alpha^{13} + x^0 \alpha^5$

Anm.: Die unterstrichenen Koeffizienten sind falsch!

$f(\alpha) = \alpha^{14} \neq 0 \quad \Rightarrow \quad$ f(x) ist fehlerhaft

Fehlerkorrektur:

Sind maximal t Koeffizient von f(x) falsch, so können diese behoben werden. Hierzu nimmt man an, dass f(x) die Summe von d(x) und einem Fehler e(x) ist. Wenn man e(x) bestimmen könnte, kann man aus f(x) d(x) rekonstruieren.

$$f(x)=d(x)+e(x)\ ,\quad e(x)=\sum_{i=0}^{2t+k-1} e_{i+1}x^{i}$$

Sofern ein Koeffizient f_i von f(x) falsch ist, ist der entsprechende Koeffizient e_i ungleich Null. Ist bekannt welche e_i's ungleich Null sind, können diese mit der folgenden Matrix berechnet werden. Sind die fehlerhaften Koeffizienten nicht bekannt, so müssen alle korrigierbaren Möglichkeiten ausprobiert werden.

$$\begin{pmatrix} \alpha^{i_1-1} & \alpha^{i_2-1} & \dots & \alpha^{i_r-1} \\ \alpha^{2(i_1-1)} & \alpha^{2(i_2-1)} & \dots & \alpha^{2(i_r-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2t(i_1-1)} & \alpha^{2t(i_2-1)} & \dots & \alpha^{2t(i_r-1)} \end{pmatrix} * \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}$$

Die e_i's ungleich Null erhalten einen weiteren Index von 1 bis r.

Wurden die e_i's errechnet, kann e(x) gebildet und von f(x) subtrahiert werden. So ergibt sich d(x). Durch teilen von d(x) mit g(x) erhält man c(x), woraus sich die gesuchte ursprüngliche Bitsequence erzeugen lässt.

Beispiel:

In dem Beispiel sind $e_{i_1} = e_5$ und $e_{i_2} = e_7$ ungleich Null.
Es muß also folgende Matrix gelöst werden:

$$\begin{pmatrix} \alpha^{5-1} & \alpha^{7-1} \\ \alpha^{2(5-1)} & \alpha^{2(7-1)} \\ \alpha^{3(5-1)} & \alpha^{3(7-1)} \\ \alpha^{4(5-1)} & \alpha^{4(7-1)} \end{pmatrix} * \begin{pmatrix} e^5 \\ e^7 \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ f(\alpha^4) \end{pmatrix}$$

$$\Leftrightarrow \quad \begin{pmatrix} \alpha^4 & \alpha^6 \\ \alpha^8 & \alpha^{12} \\ \alpha^{12} & \alpha^{18} \\ \alpha^{16} & \alpha^{24} \end{pmatrix} * \begin{pmatrix} e^5 \\ e^7 \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ f(\alpha^4) \end{pmatrix} \quad \Leftrightarrow \quad \begin{pmatrix} \alpha^4 & \alpha^6 \\ \alpha^8 & \alpha^{12} \\ \alpha^{12} & \alpha^3 \\ \alpha^1 & \alpha^9 \end{pmatrix} * \begin{pmatrix} e^5 \\ e^7 \end{pmatrix} = \begin{pmatrix} \alpha^{14} \\ \alpha^7 \\ \alpha^8 \\ \alpha^2 \end{pmatrix}$$

Durch lösen des entsprechenden Gleichungssystems erhält man die Werte $e_5 = \alpha^{12}$ und $e_7 = \alpha^2$. Subtrahiert man e_5 von f_5 und e_7 von f_7 ergibt sich aus f(x) d(x) (siehe Anlage D)

Um das gesuchte Polynom c(x) zu erhalten, muß d(x) nur noch durch g(x) geteilt werden.

Quellenangaben

Diskrete Strukturen Band 1
Angelika Steger
Springer-Verlag

Vorlesungsskript „Diskrete Mathematik“
von Prof. Dr. Rainer Lang (Handout)

Vorlesungsfolien „Diskrete Mathematik“
von Prof. Dr. Sebastian Iwanowski
http://www.fh-wedel.de/~iw

Vorlesungsskript „Einführung in Kanalcodierungsverfahren“
von Dr. Peter Stammnitz
http://iphome.hhi.de/stammnitz/ (nicht mehr online)

http://www.galois-group.net/

Anhang A

$(\mathbb{Z}_2[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ $\quad p(x) = x^4 + x^3 + 1$

ord	Polynomdarstellung	Tupel (Bitsequenz)
0	0	0000
α^0	1	1000
α^1	x	0100
α^2	x^2	0010
α^3	x^3	0001
α^4	$1 + x^3$	1001
α^5	$1 + x + x^3$	1101
α^6	$1 + x + x^2 + x^3$	1111
α^7	$1 + x + x^2$	1110
α^8	$x + x^2 + x^3$	0111
α^9	$1 + x^2$	1010
α^{10}	$x + x^3$	0101
α^{11}	$1 + x^2 + x^3$	1011
α^{12}	$1 + x$	1100
α^{13}	$x + x^2$	0110
α^{14}	$x^2 + x^3$	0011

Anhang B

$(\mathbb{Z}_2[x]_{p(x)}, +_{p(x)}, *_{p(x)})$ $\quad p(x) = x^4 + x^3 + 1$

Additionstabelle

+	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
α^0	α^0	0	α^{12}	α^9	α^4	α^3	α^{10}	α^8	α^{13}	α^6	α^2	α^5	α^{14}	α^1	α^7	α^{11}
α^1	α^1	α^{12}	0	α^{13}	α^{10}	α^5	α^4	α^{11}	α^9	α^{14}	α^7	α^3	α^6	α^0	α^2	α^8
α^2	α^2	α^9	α^{13}	0	α^{14}	α^{11}	α^6	α^5	α^{12}	α^{10}	α^0	α^8	α^4	α^7	α^1	α^3
α^3	α^3	α^4	α^{10}	α^{14}	0	α^0	α^{12}	α^7	α^6	α^{13}	α^{11}	α^1	α^9	α^5	α^8	α^2
α^4	α^4	α^3	α^5	α^{11}	α^0	0	α^1	α^{13}	α^8	α^7	α^{14}	α^{12}	α^2	α^{10}	α^6	α^9
α^5	α^5	α^{10}	α^4	α^6	α^{12}	α^1	0	α^2	α^{14}	α^9	α^8	α^0	α^{13}	α^3	α^{11}	α^7
α^6	α^6	α^8	α^{11}	α^5	α^7	α^{13}	α^2	0	α^3	α^0	α^{10}	α^9	α^1	α^{14}	α^4	α^{12}
α^7	α^7	α^{13}	α^9	α^{12}	α^6	α^8	α^{14}	α^3	0	α^4	α^1	α^{11}	α^{10}	α^2	α^0	α^5
α^8	α^8	α^6	α^{14}	α^{10}	α^{13}	α^7	α^9	α^0	α^4	0	α^5	α^2	α^{12}	α^{11}	α^3	α^1
α^9	α^9	α^2	α^7	α^0	α^{11}	α^{14}	α^8	α^{10}	α^1	α^5	0	α^6	α^3	α^{13}	α^{12}	α^4
α^{10}	α^{10}	α^5	α^3	α^8	α^1	α^{12}	α^0	α^9	α^{11}	α^2	α^6	0	α^7	α^4	α^{14}	α^{13}
α^{11}	α^{11}	α^{14}	α^6	α^4	α^9	α^2	α^{13}	α^1	α^{10}	α^{12}	α^3	α^7	0	α^8	α^5	α^0
α^{12}	α^{12}	α^1	α^0	α^7	α^5	α^{10}	α^3	α^{14}	α^2	α^{11}	α^{13}	α^4	α^8	0	α^9	α^6
α^{13}	α^{13}	α^7	α^2	α^1	α^8	α^6	α^{11}	α^4	α^0	α^3	α^{12}	α^{14}	α^5	α^9	0	α^{10}
α^{14}	α^{14}	α^{11}	α^8	α^3	α^2	α^9	α^7	α^{12}	α^5	α^1	α^4	α^{13}	α^0	α^6	α^{10}	0

Anhang C

$$c(x) = \underline{x^3\alpha^{14} + x^2\alpha^9 + x^1\alpha^5 + x^0\alpha^{10}}$$

$$\begin{aligned}
g(x) &= (x-\alpha^1)\,(x-\alpha^2)\,(x-\alpha^3)\,(x-\alpha^4) \\
&= (x+\alpha^1)\,(x+\alpha^2)\,(x+\alpha^3)\,(x+\alpha^4) \\
&= x^4 + x^3\alpha^4 + x^3\alpha^3 + x^2\alpha^7 + x^3\alpha^2 + x^2\alpha^6 + x^2\alpha^5 + x^1\alpha^9 + \\
&\quad x^3\alpha^1 + x^2\alpha^5 + x^2\alpha^4 + x^1\alpha^8 + x^2\alpha^3 + x^1\alpha^7 + x^1\alpha^6 + \alpha^{10} \\
&= x^4 + x^3(\alpha^4 + \alpha^3 + \alpha^2 + \alpha^1) + x^2(\alpha^7 + \alpha^6 + \alpha^5 + \alpha^5 + \alpha^4 + \alpha^3) + \\
&\quad x^1(\alpha^9 + \alpha^8 + \alpha^7 + \alpha^6) + \alpha^{10} \\
&= \underline{x^4 + x^3\alpha^7 + x^2\alpha^4 + x^1\alpha^{12} + \alpha^{10}}
\end{aligned}$$

$$\begin{aligned}
c(x) * g(x) &= x^7\alpha^{14} + x^6\alpha^6 + x^5\alpha^3 + x^4\alpha^{11} + x^3\alpha^9 + \\
&\quad x^6\alpha^9 + x^5\alpha^1 + x^4\alpha^{13} + x^3\alpha^6 + x^2\alpha^4 + \\
&\quad x^5\alpha^5 + x^4\alpha^{12} + x^3\alpha^9 + x^2\alpha^2 + x^1\alpha^0 + \\
&\quad x^4\alpha^{10} + x^3\alpha^2 + x^2\alpha^{14} + x^1\alpha^7 + \alpha^5 \\
&= x^7\alpha^{14} + x^6(\alpha^6 + \alpha^9) + x^5(\alpha^3 + \alpha^1 + \alpha^5) + \\
&\quad x^4(\alpha^{11} + \alpha^{13} + \alpha^{12} + \alpha^{10}) + x^3(\alpha^6 + \alpha^9 + \alpha^9 + \alpha^2) + \\
&\quad x^2(\alpha^4 + \alpha^2 + \alpha^{14}) + x^1(\alpha^0 + \alpha^7) + \alpha^5 \\
&= \underline{x^7\alpha^{14} + x^6\alpha^{10} + x^5\alpha^0 + x^4\alpha^1 + x^3\alpha^5 + x^2\alpha^0 + x^1\alpha^{13} + \alpha^5} \\
&= d(x)
\end{aligned}$$

Anhang D

$\alpha^4 e_5 + \alpha^6 e_7 = \alpha^6 + \alpha^{14} + \alpha^5 + \alpha^4 + \alpha^8 + \alpha^2 + \alpha^{14} + \alpha^5$

$\alpha^8 e_5 + \alpha^{12} e_7 = \alpha^{13} + \alpha^5 + \alpha^{10} + \alpha^8 + \alpha^{11} + \alpha^4 + \alpha^0 + \alpha^5$

$\alpha^{12} e_5 + \alpha^3 e_7 = \alpha^5 + \alpha^{11} + \alpha^0 + \alpha^{12} + \alpha^{14} + \alpha^6 + \alpha^1 + \alpha^5$

$\alpha^1 e_5 + \alpha^9 e_7 = \alpha^{12} + \alpha^2 + \alpha^5 + \alpha^1 + \alpha^2 + \alpha^8 + \alpha^5 + \alpha^5$

$\alpha^4 e_5 + \alpha^6 e_7 = \alpha^{14}$

$\alpha^8 e_5 + \alpha^{12} e_7 = \alpha^7$

$\alpha^{12} e_5 + \alpha^3 e_7 = \alpha^8$

$\alpha^1 e_5 + \alpha^9 e_7 = \alpha^2$

$e_7 = (\alpha^{14} - \alpha^4 e_5) : \alpha^6 = (\alpha^{14} + \alpha^4 e_5) * \alpha^9 = \underline{\alpha^8 + \alpha^{13} e_5}$

$\alpha^8 e_5 + \alpha^{12} (\alpha^8 + \alpha^{13} e_5) = \alpha^7$

$\Leftrightarrow \quad \alpha^8 e_5 + \alpha^5 + \alpha^{10} e_5 = \alpha^7$

$\Leftrightarrow \quad \alpha^2 e_5 = \alpha^{14}$

$\Leftrightarrow \quad e_5 = \alpha^{14} : \alpha^2$

$\Leftrightarrow \quad e_5 = \alpha^{14} * \alpha^{13}$

$\Leftrightarrow \quad \underline{e_5 = \alpha^{12}}$

$e_7 = \alpha^8 + \alpha^{13} e_5$

$\Rightarrow \quad e_7 = \alpha^8 + \alpha^{13} \alpha^{12}$

$\Leftrightarrow \quad e_7 = \alpha^8 + \alpha^{10}$

$\Leftrightarrow \quad \underline{e_7 = \alpha^2}$

$d(x) = f(x) - e(x)$

$= \quad x^7 \alpha^{14} + x^6 \alpha^8 + x^5 \alpha^0 + x^4 \alpha^0 + x^3 \alpha^5 + x^2 \alpha^0 + x^1 \alpha^{13} + x^0 \alpha^5 - x^6 \alpha^2 - x^4 \alpha^{12}$

$= \quad x^7 \alpha^{14} + x^6 (\alpha^8 - \alpha^2) + x^5 (\alpha^0 - \alpha^{12}) + x^4 \alpha^0 + x^3 \alpha^5 + x^2 \alpha^0 + x^1 \alpha^{13} + x^0 \alpha^5$

$= \quad x^7 \alpha^{14} + x^6 (\alpha^8 + \alpha^2) + x^5 (\alpha^0 + \alpha^{12}) + x^4 \alpha^0 + x^3 \alpha^5 + x^2 \alpha^0 + x^1 \alpha^{13} + x^0 \alpha^5$

$= \quad \underline{x^7 \alpha^{14} + x^6 \alpha^{10} + x^5 \alpha^1 + x^4 \alpha^0 + x^3 \alpha^5 + x^2 \alpha^0 + x^1 \alpha^{13} + x^0 \alpha^5}$