3. Zur Algebra der Restklassen

3.1 Restklassen bei ganzen Zahlen und Polynomen

A Ideale, Restklassen und Restklassenringe bei ganzen Zahlen

Def. 3.1: (zweiseitiges) Ideal I in einem Ring R

:= eine additive Untergruppe I eines Ringes R = (R;+;$*$) der Art, dass gilt: $\forall r \in R$ und $\forall i \in I$: $r * i \in I$ und $i * r \in I$.

Bemerkungen:

a) Besteht ein Ideal I = I(x) aus allen Vielfachen eines Elementes $x \in R$, so wird es als **Hauptideal** bezeichnet.

b) Die additiven Nebenklassen eines Ringes bzgl. eines Ideales I heißen **Restklassen**.

c) Die Eigenschaften von Nebenklassen (siehe Kapitel 1.3) treffen voll auf Restklassen zu. Insbesondere ist jedes Ideal auch ein Normalteiler, da die Addition als Gruppenverknüpfung kommutativ ist.

d) Liegen zwei Elemente x und y in der selben Restklasse zu einem Ideal I, so erfüllen sie eine **Kongruenzrelation** "$\equiv$ mod I", welche auch die Eigenschaften einer Äquivalenzrelation besitzt, d. h. es ist $x \equiv y \bmod I$ ("x kongruent y modulo I").

Satz 3.1: (Restklassenringe)

Die Restklassen der Faktorgruppe R/I eines Ringes R bezüglich eines Ideals I bilden ebenfalls einen Ring, den **Restklassenring** R/I.

Beispiel 3.1 (Einfache Restklassenringe):

a) Im Ring der ganzen Zahlen einschließlich der 0 bildet jede Menge aller Vielfachen einer ganzen Zahl z ein Ideal. So ist beispielsweise ($\{R_0, R_1, R_2, R_3, R_4\}$; +; $*$) mit Restklassen R_0 = {0,5,-5,10,-10,...}, ... , R_4 = {4,9,-1,14,-6,...} ein Restklassenring bzgl. des Ideales R_0.

b) Seien I = R_0 = {0,2,-2,4,-4,...} bzw. R_1 = {1,3,-1,5,-3,...} die Mengen der geraden bzw. ungeraden ganzen Zahlen. Dann ist die Arithmetik des Restklassenringes ({R_0, R_1}; +; $*$) identisch mit der **Arithmetik modulo 2**.

Def. 3.2: Hauptidealring R

:= ein Ring R, in dem jedes Ideal I ein Hauptideal ist, d. h.aus allen Vielfachen r$*$a mit r$\in$R eines Elementes a$\in$R besteht.

Def. 3.3: Euklidischer Ring R

:= ein Hauptidealring R, in dem eine Division mit Quotienten und Rest sowie eine eindeutige Primzahlzerlegung definiert sind und in dem zu je zwei Zahlen ein größter gemeinsamer Teiler (ggT) existiert.

Bemerkung:

Die Menge der ganzen Zahlen bildet einen Euklidischen Ring.

Def. 3.4: Restklasse a modulo m (a mod m)

:= zu festem m und a die Menge [a] = {x | x = a + i$*$m mit i$\in\mathbb{Z}$}.

Def. 3.5: Restklassenring der ganzen Zahlen modulo m

:= der Restklassenring $\mathbb{Z}$ modulo m, der durch homomorphe Abbildung aus der Menge $\mathbb{Z}$ der ganzen Zahlen entsteht und zum Faktorring Z/I(m) isomorph ist, wobei I(m) ein Hauptideal darstellt.

Satz 3.2: (Restklassenring der ganzen Zahlen) - ohne Beweis -

Jede Restklasse im Restklassenring $\mathbb{Z}$ modulo m enthält die 0 oder eine positive ganze Zahl kleiner als m. Die 0 liegt im Ideal I(m) und jede positive Zahl kleiner als m liegt in einer anderen Restklasse.

Bemerkungen:

a) Der Restklassenring $\mathbb{Z}$ modulo m ist von der endlichen Ordnung m. Seine Elemente sind [0], [1], ... , [m-1].

b) Bei der Schreibweise [a] wird die Kenntnis der Zahl m, welche das Ideal I(m) und damit den Restklassenring $\mathbb{Z}$ modulo m erzeugt, vorausgesetzt.

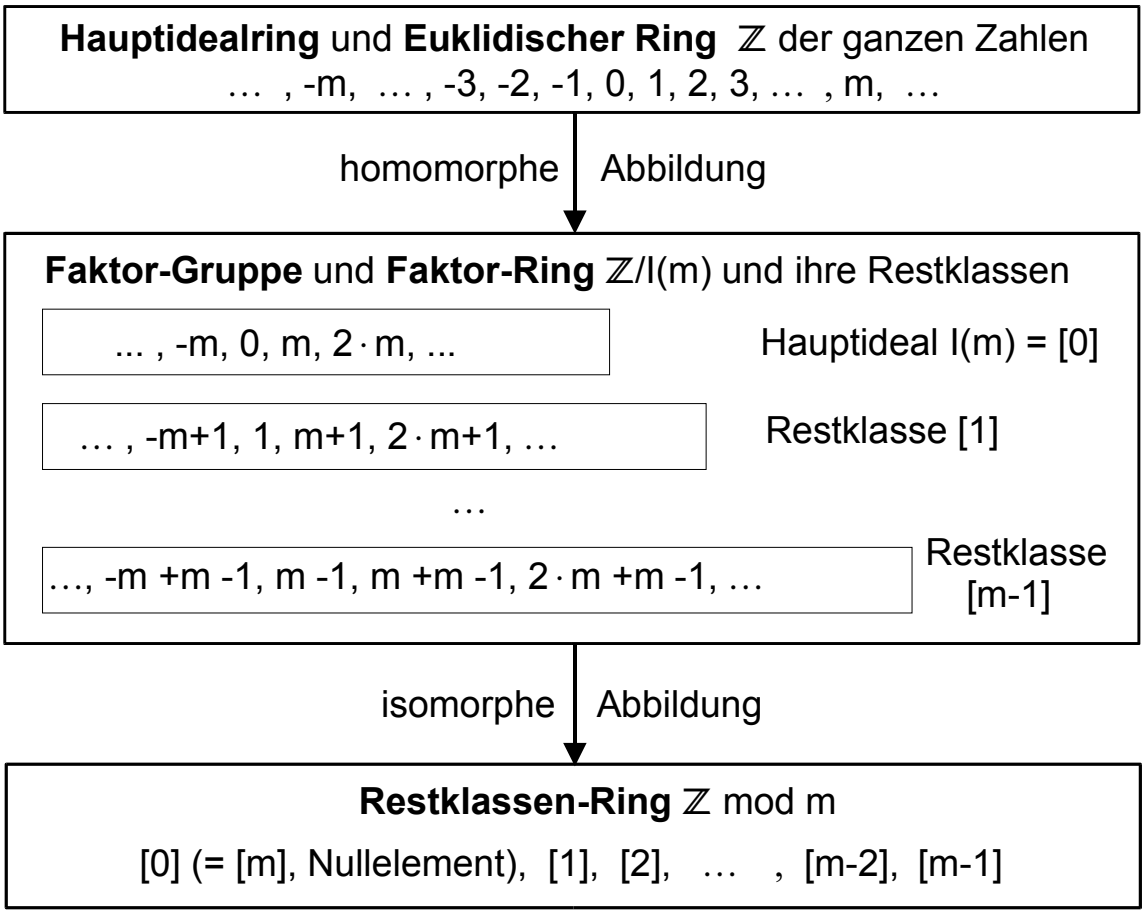


Bild 3.1 Ring der ganzen Zahlen und Restklassenring $\mathbb{Z}$ mod m

Bemerkungen:

a) Das **inverse** Element zu [a] bzgl. der Addition ist jenes Element [b] = -[a], für das gilt [b] + [a] = [b + a] = [m] mit sign(b) = sign(a).
So ergibt sich z. B. für m = 6 das Inverse zu [4] als -[4] = [2], denn [2] + [4] = [6].

b) Das inverse Element zu [a] bzgl. der Multiplikation existiert nur dann in eindeutiger Weise für alle Restklassen, wenn m eine Primzahl ist. Andernfalls gilt nämlich das Axiom K3 nicht.
So folgt z. B. für m = 6 das Inverse zu [3] aus $[3] * [3]^{-1} = [1] = [7]$. Dafür existiert aber im Restklassenring $\mathbb{Z}$ mod 6 keine Lösung.

Satz 3.3: (Restklassen-Körper $\mathbb{Z}$ modulo m) - ohne Beweis -

Der Restklassenring der ganzen Zahlen $\mathbb{Z}$ modulo m ist genau dann ein Körper, wenn m eine **Primzahl** p ist (Schreibweise: $\mathbb{Z}$ **mod p** statt mod m).

Beispiel 3.2 (einfaches Rechnen mit Restklassen):

a) **Multiplikation** mit **Skalaren**:

$$2 * \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \bmod 5 = \begin{bmatrix} 2*1 \\ 2*3 \\ 2*4 \end{bmatrix} \bmod 5 = \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix} .$$

b) **Vektoraddition**:

(2, 3, 4, 0, 3, 1) + (1, 1, 0, 2, 3, 4) mod 5 = (3, 4, 4, 2, 1, 0).

c) Multiplikation **modulo 2**:

```
101100111*10011
101100111
    101100111
     101100111
1010111011001
```

Multipliktion **im Ring** $\mathbb{Z}$ zur Basis 2 und mit Übertrag:

```
101100111*10011
101100111
    101100111
     101100111
1101010100101
```

d) Division **modulo 2**:

```
101111001:10011 = 10100
10011
0010010
   10011
   000101
```

positiver oder negativer Rest

Probe:
10100 * 10011+101 mod 2
= 101111100+101 mod 2
= 101111001 mod 2

Division **im Ring** $\mathbb{Z}$:

```
101111001:10011 = 10011
10011
00100100
   10011
   0100011
    10011
    010000
```

positiver Rest

Probe:
10011 * 10011+10000
= 101101001+10000
= 101111001.

Def. 3.6: Galoisfeld GF(p)

:= ein endlicher Körper, der zum Restklassenkörper $\mathbb{Z}$ mod p, mit Primzahl p, isomorph ist und dessen p Elemente mit 0, 1, ... , p-1 bezeichnet werden.

Bemerkungen:

a) Jedes Element k eines Galoisfeldes GF(p) repräsentiert eigentlich die unendlich vielen Elemente k, k-p, k+p, k-2 · p, k+2 · p, ... mit $0 \leq k < p$, die z. B. bei Rechenoperationen auftreten können aber bzgl. der Rechnung **mod p** identisch sind.

b) Bei Berechnungen in einem GF(p) ist i. Allg. die **Reduktion mod p** fest vorgeschrieben, d. h. alle Ergebniswerte werden nach dem Ende der Rechenoperationen mod p in das Intervall [0, p-1] abgebildet.

c) Die additive Gruppe eines GF(p) besteht aus allen p Elementen des GF(p) und besitzt demgemäß die **Ordnung** p.

d) Die multiplikative Gruppe enthält die 0 nicht, d. h. ihre Ordnung ist p - 1. Alle Elemente in ihr besitzen multiplikative Inverse und heißen **Einheiten**.

e) Jeder endliche Körper ist isomorph zu einem Galois-Feld.

Satz 3.4: (zyklische Gruppen in Galois-Feldern)

a) Die **additive** Gruppe eines GF(p) ist zyklisch, und für das Inverse jedes Elementes a ergibt sich $-a = p - a \mod p$.

b) Die **multiplikative** Gruppe GF(p)\{0} eines GF(p) ist zyklisch, und für das Inverse jedes Elementes a ergibt sich $a^{-1} = a^{p-2} \mod p$. Weiter gilt für jedes Element $b \in GF(p)\backslash\{0\}$: $b^{p-1} = 1 \mod p$.

Beweis:

Zu a): Für jedes $a \in GF(p)$ ist $a = \underbrace{1 + ... + 1}_{\text{a-mal}} = a \cdot 1 \mod p$, d. h. das Einselement **erzeugt** alle Elemente des GF(p), und damit ist die additive Gruppe zyklisch.
Dabei ist u. a. $p \cdot 1 = p = 0 \mod p$. Unter Verwendung der Subtraktion folgt daraus $a + (-a) = 0 = p \mod p$, d. h. $(-a) = p - a \mod p$.

Zu b): Jedes GF(p) besitzt ein **primitives Element** a, das die p - 1 von 0 verschiedenen Elemente $a^0 = 1, a^1, ..., a^{p-2}$, der multiplikativen Gruppe **erzeugt** (Beweis z. B. in /11/), d. h. GF(p)\{0} ist zyklisch.

Damit existiert zu jedem Element b der multiplikativen Gruppe ein $i \in \{0, \ldots, p-2\}$ mit $b = a^i$ und $b^{p-1} = (a^i)^{p-1} = (a^{p-1})^i = 1^i = 1 \bmod p$.
Weiter gilt für das Inverse jedes Elementes a:
$1 = a^{p-1} = a^1 \cdot a^{p-2} \cdot \bmod p$ bzw. $a^{-1} = a^{p-2} \bmod p$.

Satz 3.5: (Einfache Rechenregel in Galois-Feldern)
In jedem Galois-Feld mit $p \geq 2$ gilt für alle von 0 verschiedenen Elemente a,b: $(a \pm b)^p = a^p \pm b^p = a \pm b \bmod p$.

Beweis:
In jedem GF(p) gilt zunächst: $(a \pm b)^p = \sum_{i=0}^{p} \binom{p}{i} \cdot a^{p-i} \cdot b^i \cdot (\pm 1)^i \bmod p$.

Dabei ist $\binom{p}{i} \bmod p = 0$, wenn p (= 0 mod p) darin als unkürzbarer Faktor vorkommt, d. h. also für i = 1,...,p - 1 aber nicht für 0 und p.
Weiter ist p für p > 2 ungerade, d. h. $(\pm 1)^p = \pm 1$, und für p = 2 ist (a - b) = (a + b) (selbstinvers!).
Zusammen mit Satz 3.4b) folgt daraus Satz 3.5.

B Polynom-Ideale und Polynom-Restklassen

Def. 3.7: Polynom f über einem Ring R
:= eine ganze rationale Funktion f(x) über einer **Unbestimmten** x von der Form
$f(x) = a_n \cdot x^n + \ldots + a_1 \cdot x^1 + a_0$
mit **Koeffizienten** $a_0, a_1, \ldots, a_n \in R$.

Bemerkungen:
a) Die Menge P(R) der Polynome über einem Ring R entsteht durch **Ringadjunktion** der Unbestimmten x zum Ring R.
b) Die Größe x wird im Hinblick darauf, dass je endlich viele Potenzen $x^0=1, x^1, \ldots, x^n$ linear unabhängig sind, als Unbestimmte bezeichnet.

c) Der **Grad** eines Polynomes ist gleich der höchsten Potenz von x, die einen nicht verschwindenden (d. h. von 0 verschiedenen) Koeffizienten besitzt.

d) Ein Polynom heißt **normiert**, wenn der Koeffizient seiner höchsten nicht verschwindenden Potenz von x gleich 1 ist.

e) In abgekürzter Koeffizientenschreibweise ist $f(x) \equiv a_n...a_1a_0$.

Beispiel 3.3: (Einfache Rechnungen mit Polynomen)

a) **Addition** von Polynomen über einem Ring R:
$(x^5 + 3 \cdot x^2 + 1) + (4 \cdot x^3 + x + 17) = x^5 + 4 \cdot x^3 + 3 \cdot x^2 + x + 18.$

b) **Multiplikation** von Polynomen:
$(x^3 + 2x^2 + 1) \cdot (x + 2) = x^4 + 4 \cdot x^3 + 4 \cdot x^2 + x + 2.$

c) **Division** von Polynomen:
$(3 \cdot x^4 + x^3 + 1):(x^2 - 1) = 3 \cdot x^2 + x + 3$ mit dem Rest $(x + 4)$.
Kontrollrechnung:
$(3 \cdot x^2 + x + 3) \cdot (x^2 - 1) + (x + 4)$
$= 3 \cdot x^4 + x^3 + 3 \cdot x^2 - 3 \cdot x^2 - x - 3 + x + 4$
$= 3 \cdot x^4 + x^3 + 1.$

Satz 3.6: (Ring von Polynomen) - ohne Beweis -

Die Menge P(R) aller Polynome über einem Ring R bildet einen Polynomring.

Bemerkungen:

a) Im Hinblick auf die algebraische Codierungstheorie interessieren vor allem Polynomringe P(K) über endlichen Körpern K.

b) Eine Menge I(f(x)) bildet im Ring P(K) ein Ideal, wenn sie aus allen Vielfachen eines Polynomes f(x) besteht, und P(K) ist ein Hauptidealring.

c) Je zwei Polynome f(x) und g(x) besitzen im Ring P(K) in eindeutiger Weise einen größten gemeinsamen Teiler, das ist jenes normierte Polynom maximalen Grades, welches gleichzeitig Teiler beider Polynome ist.

d) P(K) ist sogar ein Euklidischer Ring, da zu je zwei Polynomen f(x) und g(x) mit $g(x) \neq 0$ zwei, bis auf die Einheiten von K eindeutige, Polynome existieren, der **Quotient** q(x) sowie der **Rest** r(x) bei Division von f(x) durch g(x), der Art, dass gilt $f(x) = q(x) \cdot g(x) + r(x)$ mit Grad(r(x)) < Grad(g(x)).

Satz 3.7: (Darstellbarkeit von einzelnen Polynomwerten)

Zu jedem Paar von Polynomen f(x) und g(x) = (x - a) mit $a \in K \backslash \{0\}$ gibt es weitere Polynome q(x) und r(x), so dass gilt $f(x) = q(x) \cdot (x - a) + r(x)$ mit r(x) = r(a) = f(a)

Beweis:

Für x = a ist $f(a) = q(a) \cdot 0 + r(a)$, und gemäß Bemerkung d) zu Satz 3.6 ist hier Grad(r(x)) = 0 < Grad((x - a)) = 1. Also ist r(a) = f(a) konstant.

Satz 3.8: (Zerlegung von Polynomen in Linearfaktoren)

Zu jedem Paar von Polynomen f(x) sowie g(x) = (x - a) mit $a \in K \backslash \{0\}$ und f(a) = 0 gibt es die Zerlegung $f(x) = q(x) \cdot (x - a)$ mit dem Linearfaktor (x - a).

Beweis:

Für x = a ist $f(a) = q(a) \cdot 0 + r(a) = 0$. Daraus ergibt sich r(a) = 0 und $f(x) = q(x) \cdot (x - a)$.

Bemerkung:

In Definition 3.18 wird weiter unten für Elemente a mit f(a) = 0 die Bezeichnung "Wurzel von f(x)" eingeführt.

Def. 3.8: Über einem Körper K reduzibles Polynom f

:= ein Polynom $f(x) = q(x) \cdot g(x)$ mit Teilerpolynomen g(x) und q(x), die beide vom Grad größer als Null sind, über dem Körper K.

Def. 3.9: Über einem Körper K irreduzibles Polynom f

:= ein Polynom f(x) über dem Körper K, das nicht reduzibel ist, d. h. zu dem es keine zwei Teiler-Polynome vom Grad größer als 0 gibt.

Satz 3.9: (eindeutige Zerlegung in irreduzible Teilerpolynome)

Ist ein Polynom f(x) über dem Koeffizientenkörper K reduzibel, so gibt es eine Zerlegung $f(x) = f_1(x) \cdot f_2(x) \cdot ... \cdot f_s(x)$ von f(x) in irreduzible, **bis auf** die **Einheiten** von K **eindeutige,** Teilerpolynome $f_1(x), f_2(x), ..., f_s(x)$ vom Grad größer 0 über K.

Beweis (hier für den Fall des GF(2) mit **mod 2**-Rechnung):

Konstruktiv mit folgendem **Verfahren 3.1** zur Berechnung der irreduziblen Teiler-Polynome vom Grad größer als Null:

Sei i = 1 und $q_1(x) = f(x) = c_n \cdot x^n + ... + c_1 \cdot x^1 + c_0$ mit $c_n \neq 0$.

a) Das Polynom $q_i(x)$ wird in der Reihenfolge wachsenden Grades n = 1, 2, ... , $\max(1, \lfloor n/2 \rfloor)$ und, bzgl. der Koeffizientenschreibweise $c_n ... c_1 c_0$, in alphabetischer Reihenfolge durch alle irreduziblen Polynome zu dividieren versucht.

   Dabei sind allePolynome vom Grad 1 irreduzibel, und irreduzible Polynome höheren Grades werden mit dem beschriebenen Verfahren selbst iterativ bestimmt.

   Das erste gefundene irreduzible Teiler-Polynom von $q_i(x)$ wird $f_i(x)$ genannt. Ist $q_i(x)$ selbst irreduzibel, so ergibt sich $f_i(x) := q_i(x)$.

b) Es wird gesetzt $i := i+1$, $q_i(x) := q_{i-1}(x)/f_{i-1}(x)$, und n, c_n, ... , c_1, c_0 werden entspechend umbenannt.

   Ist $q_i(x) = q$ eine Einheit (d. h. $q_i \in K \setminus \{0\}$), so endet das Verfahren. Andernfalls wird mit a) fortgefahren.

Bemerkungen:

a) Für p > 2 müssen **normierte** Teilerpolynome bestimmt werden, da mit 1,...,(p - 1) mehrere Einheiten existieren. So ist z. B. im GF(5)

$$\begin{aligned}(x^2 + 1) \cdot (x + 1) &= x^3 + x^2 + x + 1 \\ &= 6 \cdot x^3 + 6 \cdot x^2 + 6 \cdot x + 6 = (2 \cdot x^2 + 2) \cdot (3 \cdot x + 3) \\ &= 16 \cdot x^3 + 16 \cdot x^2 + 16 \cdot x + 16 \\ &= (4 \cdot x^2 + 4) \cdot (4 \cdot x + 4) \mod 5.\end{aligned}$$

b) Die irreduziblen Polynome über einem Körper K sind nur durch sich selbst teilbar und durch die Einheiten von K, da diese ein Inverses besitzen.

c) Wird ein Polynom f(x) mit einer Einheit des Körpers K multipliziert, so heißt das entstehende Polynom **assoziiert zu f(x)**. 4) mod 5.

Beispiel 3.4: (Berechnung der irreduziblen Teiler-Polynome im GF(2) mit dem Verfahren 3.1)

Sei i = 1 und $q_1(x) = f(x) = x^5 + x^4 + x^2 + x$.

1) **a):** x ist offensichtlich ein irreduzibles Teiler-Polynom von $q_1(x)$.
Deshalb wird gesetzt: $f_1(x) := x$ sowie
b): $i := 2$ und $q_2(x) := x^4 + x^3 + x + 1$.

2) **a):** x ist kein Teiler von $q_2(x)$. Deshalb wird durch das in alphabetischer Reihenfolge nächste Polynom vom Grad 1 dividiert:
$(x^4 + x^3 + x + 1):(x + 1) = x^3 + 1$, d. h. $(x + 1)$ ist ein irreduzibler Teiler von $(x^4 + x^3 + x + 1)$.
Also wird gesetzt: $f_2(x) := (x + 1)$ sowie
b): $i := 3$ und $q_3(x) := x^3 + 1$.

NR.: 11011:11 = 1001 $\equiv x^3 + 1$

```
11
 0011
  11
```

3) **a):** x ist kein Teiler von $q_3(x)$. Deshalb wird wie folgt mod2 dividiert:
$(x^3 + 1):(x + 1) = x^2 + x + 1$, d. h. $(x + 1)$ ist ein irreduzibler Teiler von $(x^3 + 1)$.
Also wird gesetzt: $f_3(x) := (x + 1)$,
b): $i =: 4$ und $q_4(x) := x^2 + x + 1$.

NR.: 1001:11 = 111 $\equiv x^2 + x + 1$

```
11
 10
 11
  11
```

4) **a):** x ist kein Teiler von $q_4(x)$. Deshalb wird wie folgt mod2 dividiert:
$(x^2 + x + 1):(x + 1) = x$ mit einem Rest $\neq 0$, d. h. $(x + 1)$ ist kein Teiler von $x^2 + x + 1$.
Weitere Teiler gibt es nicht, da alle Polynome bis zum maximalen Grad 1 bereits eingesetzt wurden. Also ist $q_4(x)$ irreduzibel und es wird gesetzt: $f_4(x) := q_4(x) = x^2 + x + 1$ sowie

NR.: 111:11 = 10

```
11
 01   mit Rest ≠ 0
```

b): $i := 5$, $q_5(x) = 1$, womit das Verfahren endet.

Ergebnis:

$f(x) = f_1(x) \cdot f_2(x) \cdot f_3(x) \cdot f_4(x) = x \cdot (x + 1) \cdot (x + 1) \cdot (x^2 + x + 1)$.

Def. 3.10: Polynom-Restklasse modulo f(x) über einem Körper K

:= über einem Körper K zu einem **Hauptpolynom** (auch Modularpolynom) $f(x) = c_n \cdot x^n + ... + c_1 \cdot x^1 + c_0$ vom Grad(f(x)) = n zu jedem Polynom r(x) mit Grad(r(x)) < n die Menge von **Restpolynomen [r(x)]** = $\{g(x) \mid g(x) = r(x) + q(x) \cdot f(x)$ mit $r(x),q(x) \in P(K)\}$.

Beispiel 3.5: (Polynom-Restklassen)

Seien die Polynome $h(x) = x^3 + 1$ und $f(x) = x^2 + 1$ gegeben.

Dann gilt im GF(2), d. h. unter modulo 2-Rechnung:

$h(x)/f(x) = (x^3 + 1 + x - x)/(x^2 + 1) = ((x^2 + 1) \cdot x + 1 - x)/(x^2 + 1)$

$= x + (x + 1)/(x^2 + 1)$ (mit $x = -x \mod 2$),

d. h. h(x) liegt in der Polynom-Restklasse [x + 1] und es ist

$[x + 1] = \{x + 1, x + 1 + 1 \cdot f(x), x + 1 + x \cdot f(x), x + 1 + (x + 1) \cdot f(x), ... \}$

$= \{x + 1, x^2 + x, h(x), x^3 + x^2, ... \}$

Bemerkungen:

a) Die obige Restklassenbildung setzt voraus, dass P(K) ein Euklidischer Ring ist, in dem r(x) und q(x) in eindeutiger Weise existieren.

b) Jede Restklasse modulo eines Polynomes f(x) vom Grad n enthält entweder das "Polynom" 0 oder ein Polynom vom Grad kleiner n.

c) Alle Polynome vom Grad kleiner n liegen in verschiedenen Restklassen, und die Anzahl der Restklassen ist gleich der Anzahl aller Polynome vom Grad kleiner n (über einem GF(p) also p^n Stück).

d) Gemäß Definition 3.10 ist r(x) das Polynom kleinsten Grades in der jeweiligen Restklasse [r(x)] und charakterisiert diese Restklasse.

e) Bei Rechnungen ist die **Reduktion modulo f(x)** i. Allg. fest vorgeschrieben, d. h. die Ersetzung von Ergebnis-Polynomen g(x) beliebigen Grades durch das Polynom r(x) kleinsten Grades aus der Restklasse [g(x)].

Def. 3.11: Restpolynomring P(K) modulo f(x)

:= der Ring der Restklassen, der erzeugt wird durch das Hauptideal I(f(x)) = [f(x)] = [0] und isormorph ist zur Faktorgruppe P(K)/I(f(x)) bzw. P(K)/[f(x)]

(andere Bezeichnung: Restpolynomring P(K) modulo f(x)).

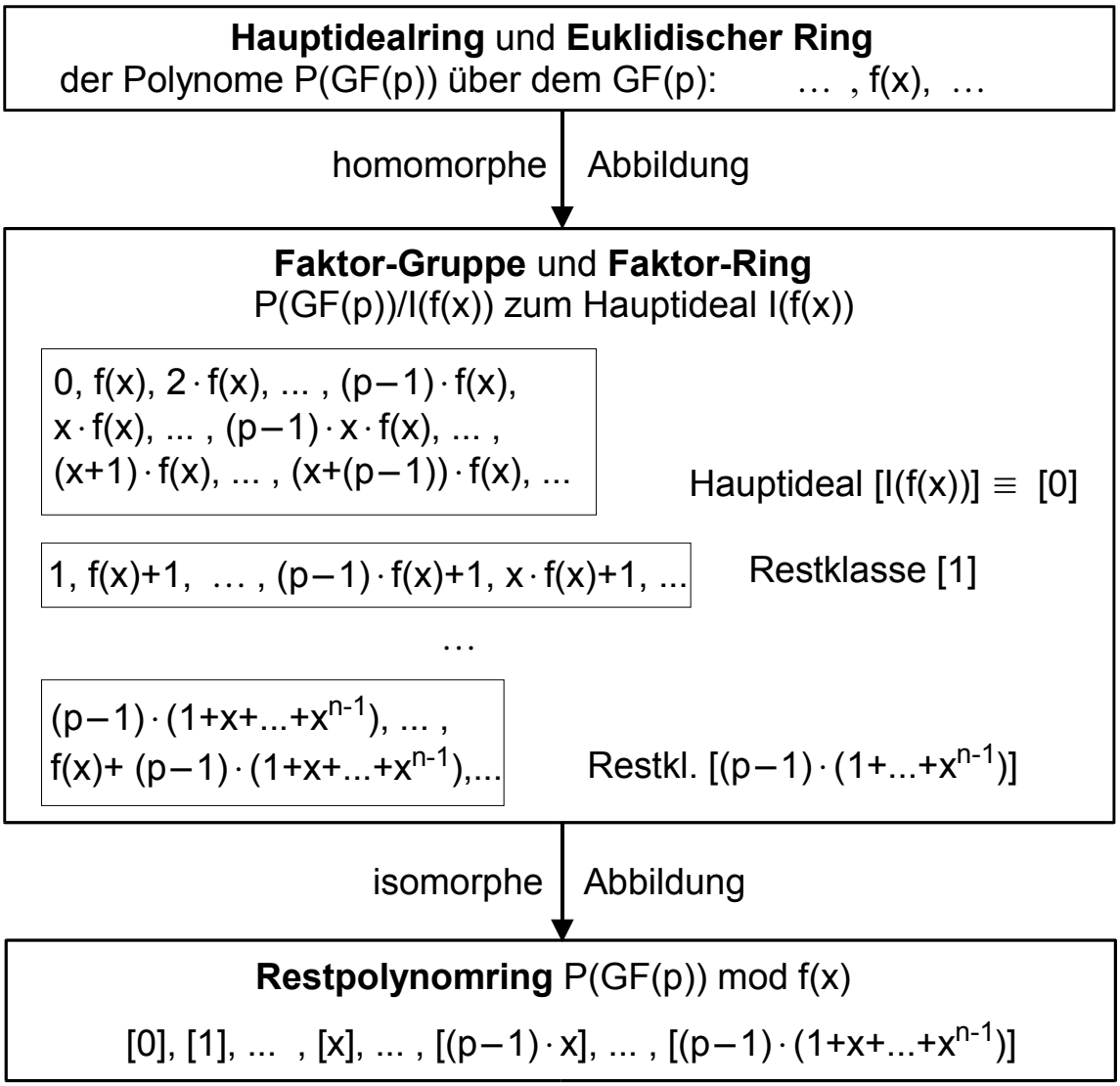


Bild 3.2 Ring der Polynome über einem Körper GF(p) und **Restpolynomring P(K) modulo f(x)** mit Grad(f(x) = n

Bemerkungen:

a) Von den unendlich vielen im Restpolynomring P(K) mod f(x) enthaltenen Polynomen sind (analog Galoisfeldern) nur die p^n Polynome vom Grad kleiner n = Grad(f(x)) voneinander verschieden.

b) Der Restpolynomring P(K) mod f(x) ist isomorph zum endlichen Euklidischen Ring, der entsteht, wenn die Restklasse [x] isomorph auf ein festes Element $u \equiv [x]$ (abgekürzt: u = [x]) abgebildet wird und jede Restklasse [r(x)] mit Grad(r(x)) < n auf das feste Polynom r(u) mit konstantem u abgebildet wird.

c) Wegen der linearen Unabhängigkeit unterschiedlicher Potenzen von x ist $[x^i] = [x]^i = u^i$ für i = 0,1,... , und das Ergebnis einer Rechnung hängt nicht davon ab, an welcher Stelle die Reduktionen modulo f(x) und mod p durchgeführt werden.

d) Aus b) und c) folgt für jedes Polynom $g(x) = c_r \cdot x^r + ... + c_1 \cdot x^1 + c_0$ vom Grad r < n des Restpolynomringes P(K) mod f(x)

$$\mathbf{[g(x)]} = [c_r \cdot x^r + ... + c_1 \cdot x^1 + c_0] = c_r \cdot [x^r] + ... + c_1 \cdot [x^1] + c_0$$
$$= c_r \cdot [x]^r + ... + c_1 \cdot [x]^1 + c_0 = c_r \cdot u^r + ... + c_1 \cdot u^1 + c_0 = \mathbf{g(u)} .$$

3.2 Zur Algebra im Restpolynomring P(K) modulo f(x)

A Ideale im Restpolynomring P(K) mod f(x)

Satz 3.10: (spezielle Restklassen im Restpolynomring P(K) modulo f(x))

Im Restpolynomring P(K) modulo f(x) ist f(u) = 0, und es ist $g(u) \neq 0$ für jedes Polynom g(x) vom Grad(g(x)) < n = Grad(f(x)), das von 0 verschieden ist.

Beweis:

Gemäß Bemerkung d) zu Bild 3.2 ist f(u) = [f(x)] = [0], und unter den Bedingungen von Satz 3.10 ist $g(u) = [g(x)] \neq [f(x)] = [0]$.

Bemerkungen:

a) Da jedes Polynom g(x) durch f(x) mit einem Rest h(x) teilbar ist vom Grad(h(x)) < n, liegt auch jedes in einer Restklasse, die ein Polynom vom Grad < n enthält.

b) Aus Satz 3.10 folgt, dass unterschiedliche Polynome g(x), h(x) mit Graden kleiner n in unterschiedlichen Restklassen liegen. Andernfalls gäbe es ein Polynom $g(x) - h(x) \neq 0$ vom Grad kleiner n, das in der Restklasse $[g(x) - h(x)] = [g(x)] - [h(x)] = [0]$ läge.

c) Gemäß a) und b) liegt in jeder Polynom-Restklasse [g(x)] genau ein Polynom vom Grad < n. Dieses dient im Folgenden als Anführer der Restklasse [g(x)].

Satz 3.11: (Ideale im Restpolynomring P(K) modulo f(x))

Jedes Ideal $I_g = I(g(x))$ im Restpolynomring P(K) modulo f(x) besteht genau aus den Vielfachen eines normierten Polynomes g(x) kleinsten Grades in der Restklasse [g(x)], der Art dass Grad(g(x)) < Grad(f(x)) ist und g(x) ein Teiler von f(x) ist.

Beweis:

a) Jedes Ideal I_g enthält ein Polynom h(x) kleinsten Grades m < n mit $h(x) = c_m \cdot x^m + ... + c_1 \cdot x^1 + c_0$ mit $c_m,...,c_1,c_0 \in K$ und $c_m \neq 0$. Gemäß Axiom K3 (Existenz des Inversen) liegen damit auch das normierte Polynom kleinsten Grades $g(x) = c_m^{-1} \cdot h(x)$ und alle seine Vielfachen $s(x) = q(x) \cdot g(x)$ modulo f(x) im Ideal I_g.

b) Nach Definition 3.1 enthält I_g als additive Untergruppe des Restpolynomringes P(K) modulo f(x) die Restklasse [0] = [f(x)] modulo f(x). Also muss f(x) ein Vielfaches von g(x) sein, d. h. g(x)|f(x).

Satz 3.12: (Dimension von Idealen im Restpolynomring P(K) modulo f(x))

Sei $f(x) = g(x) \cdot h(x)$ mit Grad(f(x)) = n > k = Grad(h(x)) ein Hauptpolynom. Dann erzeugt das Teilerpolynom g(x) von f(x) im Restpolynomring P(K) modulo f(x) ein Ideal I(g(x)) der Dimension k.

Beweis:

Die Polynome $g(x), x \cdot g(x), ... , x^{k-1} \cdot g(x)$ sind in dem von g(x) erzeugten Ideal vom Grad < n und damit linear unabhängig, d. h. I(g(x)) enthält (auf Grund der Reduktion modulo f(x)) genau alle Polynome i(x) der Form

$$i(x) = (c_{k-1} \cdot x^{k-1} + ... + c_1 \cdot x^1 + c_0) \cdot g(x) \text{ mit } c_{k-1},...,c_0 \in K,$$

d. h. genau alle **Linearkombinationen** von $g(x)$, $x \cdot g(x)$, ... , $x^{k-1} \cdot g(x)$.

Also besitzt das Ideal I_g bzgl. des Galois-Feldes GF(p) die Mächtigkeit $|K|^k = p^k$.

Damit erzeugt I_g als Hauptideal und Normalteiler gemäß Kapitel 2 einen Vektor-Unterraum U der Dimension k, der von den Vektoren $g(u)$, $u \cdot g(u)$, ... , $u^{k-1} \cdot g(u)$ aufgespannt wird.

Def. 3.12: Generatorpolynom g(x) (eines Ideals I(g(x)))

:= das normierte Polynom g(x) kleinsten Grades m (i. Allg. mit m > 0), dessen Restklasse [g(x)] im Ideal I(g(x)) enthalten ist (andere Bezeichnung: **Basispolynom**).

Bemerkungen:

a) Jede Polynom-Restklasse i(u) des von g(x) erzeugten Ideales I(g(x)) enthält genau ein Polynom vom Grad kleiner n, das durch g(x) teilbar ist.

b) Jedes normierte Polynom g(x) vom Grad m < n, das ein Teiler des Hauptpolynomes f(x) ist, erzeugt (als Generatorpolynom) ein (anderes) Ideal I(g(x)).

c) In Koeffizientenschreibweise bilden die Polynome jedes Ideales I(g(x)) die Wörter eines **Linearcodes** gemäß Definition 2.1.

Satz 3.13: (Polynome und orthogonale Unterräume) - ohne Beweis -

Seien f(x), g(x) und h(x) normierte Polynome vom Grad > 0 und sei $f(x) = g(x) \cdot h(x)$. Dann erzeugen g(x) bzw. h(x) zueinander orthogonale Unterräume U bzw. V.

Bemerkungen:

a) Die Gleichung $g(x) \cdot h(x) = f(x) = 0 \bmod f(x)$ entspricht der Orthogonalitätsbedingung für Vektor-Unterräume in Kapitel 2, wobei die volle Äquivalenz der Polynome g(x) bzw. h(x) mit der Generatormatrix bzw. mit der Kontrollmatrix nur für Hauptpolynome der Form $f(x) = x^n - 1$ gegeben ist (siehe Kapitel 4).

b) Aus a) lässt sich damit die modifizierte **Codewortbedingung**
$$i(x) \cdot h(x) = (c_{k-1} \cdot x^{k-1} + ... + c_1 \cdot x^1 + c_0) \cdot g(x) \cdot h(x) = 0 \bmod f(x)$$
bzw. (nach Division durch h(x)) **$i(x) = 0 \bmod g(x)$** ableiten.

c) Zu den k = Grad(h(x)) Nachrichtenstellen liefert diese Codewortbedingung die m = Grad(g(x)) eindeutigen Kontrollstellen des Codewortes eines systematischen Linearcodes, d. h. mit Satz 3.13 lassen sich die Ergebnisse des Kapitels 3 auf die in Kapitel 2 definierten Codes anwenden.

B Grundkörper und Erweiterungskörper

Satz 3.14: (Restpolynomring P(K) mod f(x) als Galois-Feld GF(p^m)) - ohne Beweis -

Ist das **Hauptpolynom** f(x) mit Grad(f(x)) = m irreduzibel über dem Koeffizientenkörper K, so bildet der Restpolynomring P(K) mod f(x) ein Galois-Feld GF(p^m), d. h. einen Körper, der (incl. der 0) genau p^m Elemente enthält.

Satz 3.15: (Existenz irreduzibler Polynome über Galois-Feldern GF(p)) - ohne Beweis -

Zu jeder natürlichen Zahl m > 0 gibt es über jedem Galoisfeld GF(p) mindestens ein irreduzibles Polynom f(x) vom Grad m.

Def. 3.13: Erweiterungskörper vom Grad m über einem GF(p)

:= das Galois-Feld GF(p^m), das von einem irreduziblen Hauptpolynom f(x) vom Grad m über dem GF(p) erzeugt wird.

Bemerkung:

Jedes irreduzible Hauptpolynom f(x) erzeugt einen Erweiterungskörper, wohingegen ein Generatorpolynom g(x) als Teiler eines Hauptpolynomes ein Ideal in einem Restpolynomring erzeugt.

Def. 3.14: Grundkörper GF(p)

≔ ein Körper GF(p) zu einer Primzahl p, der gemäß Def. 3.13 einem Erweiterungskörper GF(p^m) als (Koeffizienten-)Basis zugrunde liegt.

Def. 3.15: Charakteristik p eines Körpers K

≔ eine Primzahl p der Art, dass K entweder ein Grundkörper GF(p) oder ein Erweiterungskörper GF(p^m) des GF(p) ist.

Bemerkungen:

a) Zu jeder Primzahlpotenz p^m existiert ein GF(p^m) (vgl. Satz 3.15).

b) Erweiterungskörper enthalten alle Elemente des Grundkörpers.

c) Jeder endliche Körper besitzt eine Primzahl-Charakteristik p, d. h. er ist zu einem Galois-Feld isomorph (vgl. Satz 3.15).

d) Jeder Erweiterungskörper GF(p^m) entsteht durch die **einfache Adjunktion** (= Hinzunahme) einer beliebigen Wurzel jenes irreduziblen Polynomes m(x) vom Grad m, welches den Erweiterungskörper erzeugt (s. u.), so wie z. B. analog die Menge der imaginären Zahlen durch die Adjunktion von $\sqrt{-1}$ erzeugt wird.

e) In allen Körpern der Charakteristik p ist p = 0 mod p.

f) Die Elemente eines Erweiterungskörpers GF(p^m) können (in Koeffizientenschreibweise) aufgefasst werden als Wörter der Länge m über dem GF(p).

Satz 3.16: (Rechnen im Erweiterungskörper)

In jedem Erweiterungskörper GF(p^m) ist gemäß der Sätze 3.4, 3.5 $(a \cdot r(u) \pm b \cdot s(u))^{p^m} = a \cdot r(u) \pm b \cdot s(u)$ (modulo f(x) und modulo p gerechnet) für alle $a,b \in GF(p)\backslash\{0\}$ und für alle $r(u),s(u) \in GF(p^m)\backslash\{0\}$.

Beweis:

Jedes Element $a \cdot r(u) \pm b \cdot s(u)$ liegt im GF(p^m). Wird Satz 3.4 sinngemäß angewandt (die Ordnung der multiplikativen Gruppe ist $p^m - 1$), so ergibt sich Satz 3.16.

C Zyklische Eigenschaften von Restpolynomen

Satz 3.17: (Zyklische multiplikative Gruppen in Erweiterungskörpern)

Jede Polynom-Restklasse $[r(x)] = r(u) \neq 0$ eines Erweiterungskörpers $GF(p^m)$ erzeugt eine zyklische multiplikative (Unter-)Gruppe der Form $\{r(u)^0, r(u)^1, \ldots\}$.

Beweis:

Das $GF(p^m)\backslash\{0\}$ enthält $p^m - 1$ Restpolynome r(u), d. h. endlich viele. Also gibt es zu jeder Folge $r(u)^0, r(u)^1, \ldots$ einen Index s mit $s \leq p$, für den erstmals gilt $r(u)^s = r(u)^0$ und ab dem sich die Folge periodisch wiederholt. Damit bildet $\{r(u)^0, \ldots, r(u)^{s-1}\}$ eine zyklische multiplikative Gruppe bzw. Untergruppe der Ordnung s.

Dabei liegt allen Rechnungen jenes irreduzible Hauptpolynom f(x) vom Grad m zu Grunde, welches das $GF(p^m)$ erzeugt. Die Form der (Unter-)Gruppen hängt demgemäß von f(x) ab.

Satz 3.18: (Ordnung zyklischer Untergruppen in Erweiterungskörpern)

Die Ordnung jeder zyklischen Untergruppe von Restpolynomen in einem Erweiterungskörper $GF(p^m)$ ist ein Teiler der Ordnung $p^m - 1$ der zyklischen multiplikativen Gruppe des Galois-Feldes $GF(p^m)$.

Beweis:

Jede zyklische Untergruppe und alle von ihr (incl. der Untergruppe) erzeugten n_s Restklassen besitzen die selbe Ordnung bzw. Mächtigkeit s. Für alle $p^m - 1$ Elemente der multiplikativen Gruppe zusammen ist also $n_s \cdot s = p^m - 1$, d. h. $s|(p^m - 1)$.

Bemerkungen:

a) Die Sätze 3.17, 3.18 gelten nur beim Rechnen mit **irreduziblen** Hauptpolynomen vom Grad m, da nur diese ein $GF(p^m)$ erzeugen.

b) Im Hinblick auf technische Schaltungen (siehe Kapitel 5.3) und auf die Wortstrukturen zyklischer Codes (siehe Kapitel 4) interessieren insbesondere zyklische Untergruppen der Form $\{u^0,u^1,...,u^{s-1}\}$ und die dazu **isomorphen** Mengen $\{r(u)\cdot u^0,r(u)\cdot u^1,...,r(u)\cdot u^{s-1}\}$.

c) Die graphischen Darstellungen der unter b) aufgeführten Restklassen (s. u.) werden als **Zyklen** bezeichnet, wobei $\{u^0,u^1,...,u^{s-1}\}$ den **Hauptzyklus** bildet.

d) Jedes Restpolynom r(x) bzw. jede Restklasse $r(u)\in GF(p^m)\setminus\{0\}$ liegt in eindeutiger Weise in genau einem dieser Zyklen.

e) Ist f(x) reduzibel, so zerfallen einige Zyklen in Teil-Zyklen, und es können **Anlaufstücke** auftreten (s. u.).

Def. 3.16: Periode s eines Polynomes f(x)

:= der Wert s = <Ordnung des Restklassenelementes u = [x]>
= $\min(i \mid i\in\mathbb{N}^+ \text{ und } u^i = 1 \bmod f(x))$
= Länge des Hauptzykluses.

Def. 3.17: Primitives Polynom f(x)

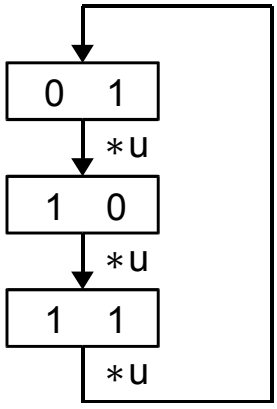
:= ein Polynom f(x) mit der maximal möglichen Periode $s_{max} = p^m - 1$.

Beispiel 3.6: (Zyklen zu irreduziblen und reduziblen Hauptpolynomen)

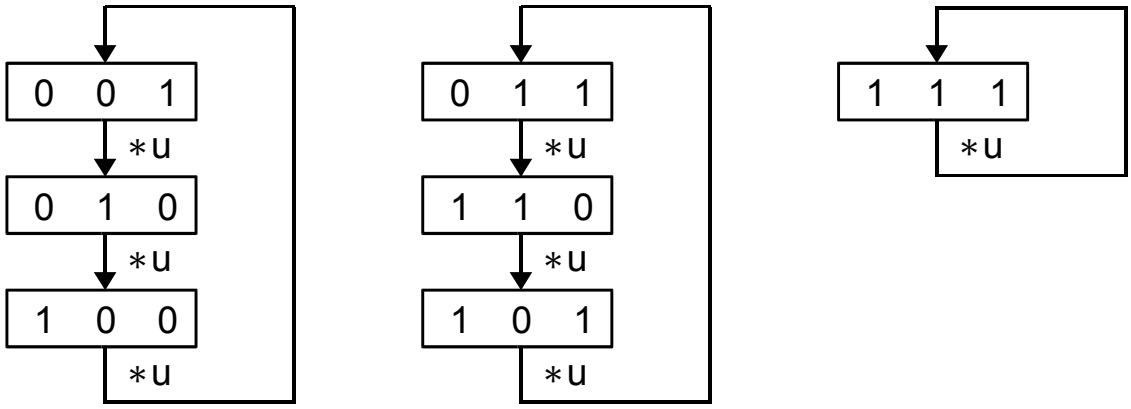
a) Das irreduzible Hauptpolynom $f(x) = x^2 + x + 1$ erzeugt die ganze multiplikative zyklische Gruppe des Galois-Feldes $GF(2^2)$ wie folgt:

1. Periode:
$u^0 \bmod f(x) = 1$
$u^1 \bmod f(x) = u$
$u^2 \bmod f(x) = u + 1$
2. Periode:
$u^3 \bmod f(x) = 1$
$u^4 \bmod f(x) = u$
$u^5 \bmod f(x) = u + 1$
....

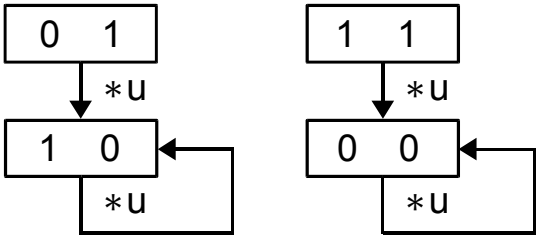
Zugehöriger **Haupt-Zyklus:**



b) Das Polynom $g(x) = x^3 + 1$ ist nicht irreduzibel, und es erzeugt deshalb kein Galois-Feld. Jede der Restklassen 1, u+1, u^2+u+1 liegt, bei der Rechnung mod f(x), wie folgt in einem anderen Zyklus:



c) Das Polynom $h(x) = x \cdot (x^2 + 1)$ ist reduzibel. Wegen des Faktors x ergeben sich folgende Teilzyklen, in denen sogar das Nullelement 00 auftritt, das zu keiner multiplikativen zyklischen Gruppe gehört:



Satz 3.19: (Grad reduzibler Polynome und ihrer Teiler)

Ist ein Polynom $f(x) = g_1(x) \cdot ... \cdot g_t(x)$ das Produkt von $t > 1$ irreduziblen Teiler-Polynomen $g_1(x)$, ... , $g_t(x)$ vom Grad größer als 0, und sind s, s_1, ... ,s_t die Perioden von f(x), $g_1(x)$, ... , $g_t(x)$ sowie m der Grad von f(x), so gilt:

a) s_1, ... ,s_t sind Teiler von s.

b) $\max(m, kgV(s_1, ... ,s_t)) \leq s < s_{max} = p^m - 1$.

Beweis:

a) Gemäß Definition 3.16 gilt für die Perioden
$u^s = 1 \bmod f(x)$ bzw. $u^s = 1 \bmod g_1(x) \cdot ... \cdot g_t(x)$ sowie
$u^s = u^{s_i} = 1 \bmod g_i(x)$ für i = 1,...,t.
Da alle s_i minimal sind, sind sie auch alle Teiler von s.

b) Aus a) folgt, dass auch $kgV(s_1, ... ,s_t)$ ein Teiler von s sein muss. Außerdem ist $s \geq m$, denn die m linear unabhängigen Restklassen $[x^0], ... ,[x^{m-1}]$ liegen (modulo f(x) gerechnet) alle im selben Zyklus (nämlich im Hauptzyklus).
Für $f_1(x) = g_2(x) \cdot ... \cdot g_t(x) = f(x)/g_1(x)$ bilden $g_1(u) \cdot u^0$, $g_1(u) \cdot u^1$, ... bzgl. der Rechnung mod f(x) einen Zyklus von Restklassen einer Länge größer 0, der **isomorph** ist zum Zyklus der Restklassen $u^0, u^1, ...$ mod $f_1(x)$. Dieser Zyklus enthält wegen des Grades von $f_1(x) < m$ nicht alle Restklassen des Hauptzyklus. Also ist $s < s_{max}$.

Bemerkung:
In Satz 3.19 b) wäre die Abschätzung $kgV(s_1, ... ,s_t) \leq s$, die m nicht enthält, unzureichend, denn z. B. gilt für das reduzible Polynom $f(x) = (x + 1) \cdot (x^2 + x + 1) \cdot (x + 1) = (x^4 + x^3 + x + 1)$ die Abschätzung $kgV(s_1, s_2, s_3) = 3 < m = Grad(f(x)) = 4 < s = 6 < s_{max} = 2^4-1 = 15$ mit $s_1|s$, $s_2|s$, $s_3|s$.

N.R.:

$111 \cdot 11$	$1001 \cdot 11$	und	$1000000...:11011 = 111$
111	1001		11011
111	1001		10110
1001	11011		11011
			11010
			11011
			0001

Satz 3.20: (Primitive und irreduzible Polynome)
a) Ist ein Polynom f(x) primitiv, so ist f(x) auch irreduzibel.
b) Die Umkehrung gilt nicht.

Beweis:
a) Wäre f(x) reduzibel, so ergäbe sich ein Widerspruch zu Satz 3.19.
b) **Gegenbeispiel:** $f(x) = x^4 + x^3 + x^2 + x + 1$ ist irreduzibel über dem GF(2) aber nicht primitiv, denn es ist $x^5 = 1$ mod f(x) und damit $s = 5 < s_{max} = 2^4 - 1 = 15$.

3.3 Wurzeln und Minimal-Polynome

A Wurzeln und Erweiterungskörper über Wurzeln

Def. 3.18: Wurzel r(u) eines Polynomes g(x) über einem GF(p)

:= eine Restklasse r(u) aus einem Grundkörper GF(p) oder aus einem Erweiterungskörper $GF(p^m)$, so dass für ein gegebenes Polynom g(x) über dem GF(p) g(r(u)) = 0 ist.

Bemerkungen:

a) Die Berechnung von g(r(u)) erfolgt durch Einsetzen von r(u) für x in g(x) verbunden (gemäß Satz 3.5) mit der **Reduktion** $a^p = a$ **mod p** für alle $a \in GF(p)$ und verbunden (gemäß Satz 3.16) mit der Reduktion $r(u)^{p^m} = r(u)$ **mod f(x)** für alle $r(u) \in GF(p^m)$, wobei allerdings f(x) u. U. unbekannt ist.

b) Ist r(u) eine Wurzel von g(x), so führen die Reduktionen u. U. auch bei unbekanntem f(x) direkt zu g(r(u)) = 0 (vgl. Beispiel 3.7a).
Allerdings sind die Reduktionen nicht immer leicht durchführbar bzw. ist ihre Durchführbarkeit nicht leicht zu erkennen.

c) Ist r(u) keine Wurzel von g(x) oder gelingen die Reduktionen nicht vollständig, so liefert g(r(u)) ein Restpolynom aus $GF(p^m)\backslash\{0\}$.

d) Bei der Berechnung der Wurzeln von g(x) kann jedes Polynom f(x), welches das $GF(p^m)$ erzeugt,als Hauptpolynom verwendet werden. Insbesondere kann gemäß Satz 3.14 auch das Polynom g(x) selbst dazu dienen, sofern es irreduzibel und vom Grad m ist.

f) Alle Wurzeln eines irreduziblen Polynomes f(x) liegen außerhalb des Koeffizientenkörpers K von f(x), d. h. hier außerhalb von GF(p).

Satz 3.21: (Abspaltung von Wurzel-Faktoren eines Polynomes)

$r(u) \in GF(p^m)$ ist **Wurzel** eines Polynomes g(x) über dem GF(p)	gdw	Es gibt ein Polynom q(x) über dem $GF(p^m)$, so dass gilt $g(x) = \mathbf{(x - r(u))} \cdot q(x)$.

Beweis:

⇒: Gemäß Definition 3.18 ist f(r(u)) = 0 und es gilt Satz 3.8.

⇐: Folgt aus Definition 3.18 beim Einsetzen von r(u) in g(x).

Bemerkungen:

a) Die Anzahl der Wurzeln ist gleich dem Grad eines Polynomes, wobei Mehrfachwurzeln entsprechend ihrer Häufigkeit zählen.

b) Die Wurzeln eines Polynomes stammen aus dem Grundkörper GF(p) oder aus (evtl. mehreren) Erweiterungskörpern.

c) Sind $r_1(u), r_2(u), \ldots, r_m(u)$ sämtliche Wurzeln eines Polynomes g(x),

so ist $g(x) = a \cdot \prod_{i=1}^{m} (x - r_i(u))$ mit $a \in GF(p) \backslash \{0\}$.

Beispiel 3.7: (Wurzeln über Körpern und Erweiterungskörpern)

a) Sei $g(x) = x^3 + 2 \cdot x$ ein Polynom über dem GF(3). Dann ergibt sich $g(0) = 0$, $g(1) = 3 = 0$, $g(2) = 12 = 0 \mod 3$. Also besitzt g(x) genau die drei Elemente des GF(3) als Wurzeln, d. h.

$g(x) = (x - 0) \cdot (x - 1) \cdot (x - 2) = x \cdot (x^2 - 3 \cdot x + 2)$

$= x^3 - 3 \cdot x^2 + 2 \cdot x = x^3 + 2 \cdot x \mod 3$.

b) Sei $g(x) = x^4 + x^2 + 1$ ein Polynom über dem GF(2).

Dann ist $(x^4 + x^2 + 1) = (x^2 + x + 1)^2$, d. h. in g(x) besitzt jede Wurzel des Polynomes $h(x) = (x^2 + x + 1)$ zweifach als Wurzel.

Im GF(2) gilt: $h(0) = h(1) = 1$, d. h. die Wurzeln liegen in ein oder zwei Erweiterungskörpern $GF(2^m)$ mit unbekanntem m.

Da (x + 1) als einziges irreduzibles Hauptpolynom vom Grad 1 bereits den Grundkörper $GF(2^1)$ erzeugt, muss $m \geq 2$ sein.

Versuch mit m = 2:

Da 0 und 1 keine Wurzeln von h(x) sind (s. o.), verbleiben aus dem $GF(2^2)$ nur noch u und u+1. Für sie ergibt sich (mod 2 gerechnet)

$h(u) = u^2 + u + 1$ bzw.

$h(u+1) = (u + 1)^2 + (u + 1) + 1$

$= u^2 + 2 \cdot u + 1 + u + 1 + 1 = u^2 + u + 1 = h(u) \mod 2$.

Nach dem Beweis zu Satz 3.4, b) ist die Ordnung jedes Elementes der multiplikativen Gruppe $GF(2^2)\backslash\{0\} = \{1,u,u+1\}$ ein Teiler von $2^2-1 = 3$. Da die Ordnungen von u und u+1 größer als 1 sind, besitzen also beide die Ordnung 3 und sind sogar primitiv, d. h. also $u^0 = 1$, $u^1 = u$, $u^2 = u + 1$, $u^3 = 1$, ...

Mit $u^2 = u + 1$ ist $h(u) = (u+1) + u + 1 = 0 = h(u+1)$, d. h. u und u+1 sind Wurzeln von h(x), und aus Bemerkung c) zu Satz 3.21 folgt

$$\begin{aligned} g(x) &= (x - u)\cdot(x - u)\cdot(x - (u + 1))\cdot(x - (u + 1)) \\ &= (x^2 + u^2)\cdot(x^2 + (u + 1)^2) \\ &= x^4 + (u^2 + (u + 1)^2)\cdot x^2 + u^2\cdot(u + 1)^2 \\ &= x^4 + x^2 + u^6 = x^4 + x^2 + 1 \ . \end{aligned}$$

c) **Alternative Lösung** zu b):

Nach Satz 3.14 erzeugt das über dem GF(2) irreduzible Teilerpolynom h(x) von g(x) vom Grad 2 das Galois-Feld $GF(2^2)$, d. h. es kann für die Rechnung als Hauptpolynom verwendet werden.

Dann besitzen nach Satz 3.10 h(x) und damit auch g(x) u als Wurzel und mit

$$\begin{aligned} g(u+1) &= (u + 1)^4 + (u + 1)^2 + 1 = (u^4 + 1) + (u^2 + 1) + 1 \\ &= u^4 + u^2 + 1 = g(u) \end{aligned}$$

ergibt sich u + 1 als weitere Wurzel.

Wegen $g(x) = h(x)\cdot h(x)$ zählen beide Wurzeln bei g(x) zweifach.

Satz 3.22: (Wurzeln beliebiger Polynome über einem GF(p))

a) Ist g(x) ein irreduzibles Polynom vom Grad m über dem GF(p) und ist r(u) eine Wurzel von g(x) in einem Erweiterungskörper $GF(p^m)$, so besitzt g(x) genau die Wurzeln $r(u)^{p^0}$, $r(u)^{p^1}$, ... , $r(u)^{p^{m-1}}$, die alle im $GF(p^m)$ liegen.

b) Ist g(x) ein reduzibles Polynom, so besitzt g(x) als Wurzeln alle Wurzeln der irreduziblen Teiler-Polynome von g(x) mit den Eigenschaften aus Teil a).

Beweis:

a) Sei $g(x) = a_m\cdot x^m + ... + a_1\cdot x^1 + a_0\cdot x^0$ mit $a_m,...,a_0 \in GF(p)$.

Dann fallen nach Satz 3.5 und Satz 3.16 bei der Multiplikation alle gemischten Produkte weg, und es ergibt sich

$$(g(x))^p = (a_m \cdot x^m + ... + a_1 \cdot x^1 + a_0 \cdot x^0)^p$$
$$= (a_m \cdot x^m)^p + ... + (a_1 \cdot x^1)^p + (a_0 \cdot x^0)^p$$
$$= a_m \cdot (x^m)^p + ... + a_1 \cdot (x^1)^p + a_0 \cdot (x^0)^p = g(x^p) .$$

Damit gilt auch für jede Wurzel r(u) von g(x):

$g(r(u)) = 0 = g(r(u)^p) =$ $g((r(u)^p)^p) =$ **$g(r(u)^{p^2}) =$** ... = **$g(r(u)^{p^3}) =$**... .

Der Beweis für die Vollständigkeit der Menge der Wurzeln findet sich z. B. in /2/, Seite 212 ff., oder in /10/, Seite 142 ff. (siehe auch die unten folgenden Bemerkungen a) und b)).

b) Folgt aus den Bemerkungen zu Satz 3.21 und aus Satz 3.22a).

Bemerkungen:

a) Alle Wurzeln eines irreduziblen Polynomes g(x) vom Grad m liegen im (z. B. von g(x) selbst erzeugten) Erweiterungskörper $GF(p^m)$.

b) Alle Wurzeln eines irreduziblen Polynomes g(x) sind von derselben Ordnung und erzeugen denselben Zyklus von Wurzeln.

c) Die Wurzeln reduzibler Polynome über dem GF(p) liegen u. U. in mehreren, unterschiedlichen Erweiterungskörpern des GF(p).

d) Jedes irreduzible Polynom g(x) besitzt nach Satz 3.10 über dem Erweiterungskörper $GF(p^m)$, sofern es ihn selbst erzeugt, die Wurzel r(u) = u. Das $GF(p^m)$ wird dann durch **Adjunktion** (s. o.) der Wurzel u = [x] zum Grundkörper GF(p) gewonnen.

e) Ist g(x) primitiv, so ist in dem von g(x) erzeugten Erweiterungskörper $GF(p^m)$ auch die Wurzel u primitiv und erzeugt alle Elemente der multiplikativen Gruppe des $GF(p^m)$.

Beispiel 3.8: (Erweiterungskörper mit vollständigem Hauptzyklus)

Wird der Erweiterungskörper $GF(2^4)$ über dem GF(2) als Körper der Restpolynome modulo $(x^4 + x + 1)$ gebildet, so ist gemäß Satz 3.10 u eine der Wurzeln des Polynomes $g(x) = x^4 + x + 1$.

Wie weiter unten mit einer Rechnung gezeigt werden kann, ist g(x) primitiv und somit u ein primitives Körperelement.

Alle $2^4 - 1 = 15$ von 0000 verschiedenen Körperelemente liegen damit wie folgt im Hauptzyklus:

$$
\begin{array}{lcll}
r_1(u) & = & u^0 \bmod (x^4+x+1) & = 1 \equiv 0001 \\
r_2(u) & = & u^1 \bmod (x^4+x+1) & = u \equiv 0010 \\
r_3(u) & = & u^2 \bmod (x^4+x+1) & = u^2 \equiv 0100 \\
r_4(u) & = & u^3 \bmod (x^4+x+1) & = u^3 \equiv 1000 \\
r_5(u) & = & u^4 \bmod (x^4+x+1) & = u+1 \equiv 0011 \\
r_6(u) & = & u^5 \bmod (x^4+x+1) & = u^2+u \equiv 0110 \\
r_7(u) & = & u^6 \bmod (x^4+x+1) & = u^3+u^2 \equiv 1100 \\
r_8(u) & = & u^7 \bmod (x^4+x+1) & = u^3+u+1 \equiv 1011 \\
r_9(u) & = & u^8 \bmod (x^4+x+1) & = u^2+1 \equiv 0101 \\
r_{10}(u) & = & u^9 \bmod (x^4+x+1) & = u^3+u \equiv 1010 \\
r_{11}(u) & = & u^{10} \bmod (x^4+x+1) & = u^2+u+1 \equiv 0111 \\
r_{12}(u) & = & u^{11} \bmod (x^4+x+1) & = u^3+u^2+u \equiv 1110 \\
r_{13}(u) & = & u^{12} \bmod (x^4+x+1) & = u^3+u^2+u+1 \equiv 1111 \\
r_{14}(u) & = & u^{13} \bmod (x^4+x+1) & = u^3+u^2+1 \equiv 1101 \\
r_{15}(u) & = & u^{14} \bmod (x^4+x+1) & = u^3+1 \equiv 1001 \\
r_1(u) & = & u^{15} = u^0 \bmod (x^4+x+1) & = 1 \equiv 0001 \\
\ldots & = & \ldots & = \ldots \equiv \ldots
\end{array}
$$

Nach Satz 3.22 und den Bemerkungen zu Satz 3.22 sind sämtliche Wurzeln von g(x), nämlich die Restpolynome **u**, $\mathbf{u^2}$, $u^4 = \mathbf{u+1}$ und $u^8 = (u+1)^2 = \mathbf{u^2+1} \mod g(x)$, von derselben Ordnung wie u, d. h. sie sind ebenfalls primitiv. So lautet z. B. der Zyklus für das primitive Element u^8: $(u^8)^0 = 1$, $(u^8)^1 = u^2+1$, $(u^8)^2 = u$, $(u^8)^3 = u^3+u$, $(u^8)^4 = u^2$, $(u^8)^5 = u^2+u+1$, ... Der Zyklus der Wurzeln, für sich betrachtet, wiederholt sich ab dem Element $u^{16} = u^{15} \cdot u^1 = u \mod g(x)$

Verfahren 3.2: (Berechnung aller Wurzeln eines Polynomes)

a) Ein gegebenes beliebiges Polynom g(x) wird zunächst gemäß dem Verfahren 3.1 aus dem Beweis zu Satz 3.9 in eindeutige irreduzible Faktoren zerlegt von der Form $g(x) = g_1(x) \cdot \ldots \cdot g_r(x)$.

b) Sind alle Faktoren $g_i(x)$ linear, dann ist r = m, alle Wurzeln $r_i(u)$ liegen im Grundkörper GF(p) und $g(x) = (x - r_1(u)) \cdot \ldots \cdot (x - r_m(u))$.
In dieser linearisierten Form können die Wurzeln direkt aus der Darstellung von g(x) abgelesen werden.

c) Lässt sich g(x) nicht vollständig linearisieren, so sei $g_i(x)$ der erste nichtlineare Faktor von g(x) mit Grad($g_i(x)$) = $m_i > 1$. Dann liegen alle Wurzeln von $g_i(x)$ im Erweiterungskörper $GF(p^{m_i})$, welcher der Einfachheit halber von $g_i(x)$ selbst erzeugt werden möge. Damit besitzt $g_i(x)$ gemäß Satz 3.10 die Wurzel $u = u^{p^0}$ und gemäß Satz 3.22a die weiteren Wurzeln $u^{p^1},...,u^{p^{m_i-1}} \in GF(p^{m_i})$. Also lässt sich $g_i(x)$ linearisieren in der Form $g_i(x) = (x - u^{p^0}) \cdot \ ... \ \cdot (x - u^{p^{m_i-1}})$.
Vorsicht! Bei Rechnungen erfolgen hier die Reduktionen jeweils modulo $g_i(x)$.

d) Besitzt g(x) weitere nichtlineare Faktoren, so wird Schritt c) wiederholt. Andernfalls endet das Verfahren.

B Minimalpolynome zu Wurzeln

Def. 3.19: Minimalpolynom m(x) einer Wurzel r(u)$\in$GF(p^m)

$:=$ das normierte Polynom $m(x) = 1 \cdot x^i + c_{i-1} \cdot x^{i-1} + ... + c_0 \cdot x^0$ von minimalem Grad i über dem GF(p), welches r(u) als Wurzel besitzt, d. h. mit m(r(u)) = 0.

Satz 3.23: (Irreduzible Minimalpolynome)

Das Minimalpolynom m(x) jedes beliebigen Elementes r(u)$\in$GF(p^m) ist über dem GF(p) irreduzibel.

Beweis (indirekt):

Wäre m(x) nicht irreduzibel, so gäbe es Polynome g(x), q(x) höheren Grades als 0 und geringeren Grades als m(x) mit $m(x) = g(x) \cdot q(x)$, und es wäre entweder g(r(u)) = 0 oder q(r(u)) = 0 im Widerspruch zu Definition 3.19.

Satz 3.24: (Maximaler Grad von Minimalpolynomen)

Für jedes Minimalpolynom m(x) einer Wurzel r(u) aus einem Erweiterungskörper $GF(p^m)$ ist Grad(m(x)) = $i \leq m$.

Beweis:

Die Potenzen von u, welche in den m + 1 Potenzen $r(u)^0$, ... , $r(u)^m$ einer gegebenen Wurzel r(u) vorkommen, besitzen im $GF(p^m)$ maximal die Ordnung m-1.

Also sind $r(u)^0$, ... , $r(u)^m$ linear abhängig, und demgemäß existiert im Erweiterungskörper $GF(p^m)$ eine Linearkombination von der Form $c_m \cdot (r(u))^m + ... + c_1 \cdot (r(u))^1 + c_0 \cdot (r(u))^0 = m(r(u))$, d. h. so, dass r(u) eine Wurzel des Polynomes $g(x) = c_m \cdot x^m + ... + c_1 \cdot x^1 + c_0 \cdot x^0$ ist.

Wird g(x) durch den Koeffizienten der höchsten von 0 mverschiedenen Potenz von x dividiert, so entsteht aus g(x) ein normiertes Polynom m(x) vom Grad(m(x)) $\leq$ m.

Satz 3.25: (Wurzeln von Minimalpolynomen und ihren Vielfachen)

Ist r(u) eine Wurzel eines Polynomes g(x) und ist m(x) das Minimalpolynom zu r(u), so ist m(x) ein Teiler von g(x), d. h. dann existiert ein weiteres Polynom q(x), das auch den Grad 0 besitzen darf, mit $g(x) = q(x) \cdot m(x)$.

Beweis (indirekt):

Sei, entgegen der Aussage von Satz 3.25, $g(x) = q(x) \cdot m(x) + h(x)$ mit $h(x) \neq 0$ und $0 \leq \text{Grad}(h(x)) < \text{Grad}(m(x))$.

Dann folgt aus der in Satz 3.25 enthaltenen Voraussetzung $g(r(u)) = m(r(u)) = 0 = q(r(u)) \cdot m(r(u)) + h(r(u))$ und damit $h(r(u)) = 0$.

Dies führt zu einem **Widerspruch** mit Definition 3.19, denn dann ergibt sich r(u) als eine Wurzel des Polynomes h(x), d. h. eines Polynomes von kleinerem Grad als das Minimalpolynom. Also muss h(x) = 0 sein, und Satz 3.25 gilt doch.

Sonderfall: q(x) ist vom Grad 0 und ist eine Einheit des GF(p).

Satz 3.26: (Eindeutigkeit von Minimalpolynomen)

Das Minimalpolynom m(x) einer Wurzel $r(u) \in GF(p^m)$ über einem Koeffizientenkörper GF(p) ist eindeutig, d. h. kein anderes normiertes irreduzibles Polynom g(x) besitzt r(u) als Wurzel.

Beweis (indirekt):

Seien sowohl m(x) als auch g(x) Minimalpolynome zu r(u) vom selben Grad i. Dann ist r(u) eine Wurzel des Polynomes m(x) - g(x), das, im **Widerspruch** zu Definition 3.19, vom Grad kleiner als i ist, weil sich die höchsten Potenzen von x in m(x) und g(x) wegen der Normierheit wegheben. Also gilt Satz 3.26 doch.

Bemerkungen:

a) Ist m(x) das Minimalpolynom einer Wurzel r(u) vom Grad i, so liegen gemäß Satz 3.22 alle Wurzeln von m(x) im Wurzel-Zyklus $r(u) = r(u)^{p^0}, r(u)^{p^1}, \ldots, r(u)^{p^{i-1}}$.

b) Gilt a), so ist m(x) gemäß Satz 3.22 und Satz 3.23 auch das Minimalpolynom zu $r(u)^{p^1}, \ldots, r(u)^{p^{i-1}}$.

c) Weiter ist m(x) ein Teiler des Polynomes $(x^{p^i} - x)$ (siehe Satz 3.31).

d) Wurzeln bzw. Minimalpolynome dienen in Kapitel 4 zur Definition spezieller Arten zyklischer Codes.

Verfahren 3.3: (Berechnung von Minimal-Polynomen durch Probieren)

a) **Aufgabenstellung**:

Gegeben sei eine Wurzel r(u), die in einem Erweiterungskörper $GF(p^m)$ aber nicht im Grundkörper GF(p) liege, wobei m evtl. unbekannt ist.

Gesucht sei das Minimalpolynom m(x) zur gegebenen Wurzel r(u), bei dessen Berechnung die Reduktion mod p und, falls f(x) bekannt ist, auch die Reduktion mod f(x) streng durchzuführen sind.

Liegt noch kein irreduzibles Hauptpolynom vom Grad m vor, so kann, falls m wenigstens bekannt ist, für die Rechnung die Beziehung $u^{p^m-1} = 1$ verwendet werden.

b) **Berechnung durch Probieren** (vgl. /13/):

Für kleine Werte von m genügt es, nacheinander für i = 1, 2, ... , m zu prüfen, ob die Potenzen $r(u)^0, r(u)^1, r(u)^2, \ldots, r(u)^i$ linear abhängig sind, d. h. ob eine Linearkombination $(1, c_{i-1}, \ldots, c_0)$ existiert, die ein Polynom kleinsten Grades i mit

$r(u)^i + c_{i-1} \cdot r(u)^{i-1} + \ldots + c_1 \cdot r(u)^1 + c_0 \cdot r(u)^0 = 0$ erzeugt.

Beispiel 3.9: (Berechnung von Minimal-Polynomen durch Probieren)

Seien z. B. das Hauptpolynom $f(x) = x^3 + x + 1$ sowie die Wurzel r (u) = u gegeben. Dann ergibt sich m(x) aus folgender Tabelle:

i	$c_i \cdot r(u)^i$ in Koeffizientenschreibweise und mod g(x)	Linearkombinationen sind von der Form	lineare Abhängigkeit
0	$c_0 \cdot u^0 \equiv 0 \quad 0 \quad c_0$	(c_0)	unmöglich
1	$c_1 \cdot u^1 \equiv 0 \quad c_1 \quad 0$	$(c_1 , \quad c_0)$	unmöglich
2	$c_2 \cdot u^2 \equiv c_2 \quad 0 \quad 0$	$(c_2 , \quad c_1 , \quad c_0)$	unmöglich
3	$c_3 \cdot u^3 = c_3 \cdot (u+1) \equiv 0 \quad c_3 \quad c_3$	$(c_2 , (c_3+c_1) , (c_3+c_0))$	möglich (*)

(*): Lineare Abhängigkeit besteht für $c_2 = 0$; $c_3 = c_1 = c_0 = 1 \mod 2$, d. h. für $m(x) = f(x) = x^3 + x + 1$.

Verfahren 3.4: (Systematische Berechnung von Minimal-Polynomen)

Aufgabenstellung: wie in Verfahren 3.3.

Systematische Berechnung von Minimal-Polynomen (vgl. /2/):

a) Liegt nur **eine** Wurzel $r(u) \in GF(p^m)$ vor, so ist dessen Minimalpolynom m(x) auch das Minimalpolynom der zu r(u) **konjugierten** Wurzeln $r(u)^{p^1}, \ldots , r(u)^{p^{i-1}} \in GF(p^m)$. Dabei ist Grad(m(x)) = i > 0 der kleinste Wert mit $r(u)^{p^i} = r(u)$ und $m(x) = (x - r(u)^1) \cdot \ldots \cdot (x - r(u)^{p^{i-1}})$. Ist m unbekannt, so muss m durch Probieren ermittelt werden.

b) Sind **mehrere** Wurzeln $r_1(u), \ldots , r_s(u)$ gegeben, so müssen nacheinander für $r_1(u), \ldots , r_s(u)$ mit dem unter a) beschriebenen Verfahren die Mengen der konjugierten Wurzeln sowie die zugehörigen irreduziblen Minimalpolynome $m_1(x), \ldots , m_s(x)$ bestimmt werden, wobei auch einige der vorgegebenen Wurzeln bereits zueinander konjugiert sein können.

   Das gemeinsame Minimalpolynom aller gegebener Wurzeln lautet dann $m(x) = kgV(m_1(x), \ldots , m_s(x))$.

Beispiel 3.10: (Systematische Berechnung von Minimal-Polynomen)

Seien das primitive Hauptpolynom $f(x) = x^4 + x + 1$ aus Beispiel 3.8 mit der Periode $s = s_{max} = 15$ sowie die Wurzel $r(u) = u^3$ aus dem $GF(2^4)$ gegeben.

Dann liegen alle Wurzeln des zur Wurzel u^3 gehörenden Minimal-Polynomes $m(x)$ im $GF(2^4)$, und sie lauten gemäß dem Satz 3.22 $u^6, u^{12}, u^{24} = u^9, u^{18} = u^3 \mod f(x)$ (ab hier wiederholen sich die Wurzeln zyklisch).

Dies führt, wenn bei der Reduktion die Potenzen von u aus Beispiel 3.8 verwendet werden, zum Minimal-Polynom

$$m(x) = (x - u^3) \cdot (x - u^6) \cdot (x - u^9) \cdot (x - u^{12})$$
$$= (x^2 - (u^3+u^{12}) \cdot x + 1) \cdot (x^2 - (u^6+u^9) \cdot x + 1) \qquad [u^{15} = 1 \mod f(x)]$$
$$= (x^2 - (u^2+u+1) \cdot x + 1) \cdot (x^2 - (u^2+u) \cdot x + 1) \qquad [\text{vgl. Beispiel 3.8}]$$
$$= (x^4 - ((u^2+u+1)+(u^2+u)) \cdot x^3 + (1+(u^2+u+1) \cdot (u^2+u)+1) \cdot x^2$$
$$- ((u^2+u+1)+(u^2+u)) \cdot x + 1)$$
$$= x^4 + x^3 + x^2 + x + 1 \qquad [\text{siehe Nebenrechnungen}]$$

NR.: $((u^2+u+1)+(u^2+u)) = 1 \mod 2;$
$1+(u^2+u+1) \cdot (u^2+u)+1 = 0 + (u^4+u^3+u^2)+(u^3+u^2+u)$
$= u^4+u = 1 \mod f(x).$

C Hauptpolynome der Form $f(x) = x^n - 1$

Satz 3.27: (Wurzeln von Polynomen $(x^{p^m-1} - 1)$ über einem GF(p))

Jedes Polynom $f(x) = (x^{p^m-1} - 1)$ über einem GF(p) besitzt als Wurzeln genau die $p^m - 1$ von Null verschiedenen Elemente des $GF(p^m)$.

Beweis:

a) Für **m = 1** bildet die Menge der p - 1 von Null verschiedenen Elemente des GF(p) eine zyklische multiplikative Gruppe, wobei nach Satz 3.18 (Sonderfall m = 1) die Ordnung e_i jedes Elementes $r_i \neq 0$ des GF(p) die Gruppen-Ordnung (p - 1) teilt.

Damit ist (vgl. Satz 3.29 weiter unten) $f(r_i) = (r_i^{p-1} - 1) = (r_i^{ei} - 1) = 0$, d. h. jedes Element $r_i \neq 0$ des GF(p) ist eine Wurzel von f(x).

Nach Bemerkung a) zu Satz 3.21 besitzt f(x) genau p - 1 Wurzeln. Es handelt sich dabei also genau um alle Elemente der multiplikativen Gruppe des GF(p).

b) Für **m > 1** gilt die selbe Schlussweise wie unter a), d. h. für jeden Erweiterungskörper $GF(p^m)$ sind dessen von 0 verschiedenen Elemente genau die Wurzeln des Polynomes $f(x) = (x^{p^m-1} - 1)$.

Def. 3.20: Zerfällungskörper K eines Polynomes f(x)

:= ein (Erweiterungs-)Körper K, der sämtliche Wurzeln $r_1(u), \ldots, r_m(u)$ eines Polynomes f(x) vom Grad m über einem Grundkörper GF(p) enthält.

Satz 3.28: (Erzeugendes Polynom eines Zerfällungskörpers)

Genau alle Wurzeln des Polynomes $(x^{p^m} - x) = (x^{p^m-1} - 1) \cdot (x - 0)$ über dem Grundkörper GF(p) bilden den Zerfällungskörper $GF(p^m)$ dieses Polynomes.

Beweis:

Das Polynom $(x^{p^m} - x)$ entsteht durch die Hinzunahme des Faktors $x = (x - 0)$ zu $(x^{p^m-1} - 1)$.

Als Wurzeln besitzt dieses Polynom gemäß Satz 3.27 alle Elemente der zyklischen multiplikativen Gruppe des $GF(p^m)$ und zusätzlich die 0 als Wurzel des Faktors (x - 0), also insgesamt alle Elemente des GF (p^m).

Damit ist das $GF(p^m)$ der Zerfällungskörper dieses Polynomes über dem GF(p).

Satz 3.29: (Teiler-Eigenschaft bei Polynomen der Form $x^n - 1$)

Ein Polynom $g(x) = (x^m - 1)$ ist genau dann ein Teiler-Polynom eines Polynomes $f(x) = (x^n - 1)$, wenn m ein Teiler von n ist.

Beweis:

Sei **n = m · d + s** mit $0 \leq s < d$. Dann ist einerseits

$(x^n - 1) = (x^{m \cdot d + s} - 1) = (x^{m \cdot d + s} - x^s + x^s - 1) = = x^s \cdot (x^{m \cdot d} - 1) + (x^s - 1)$.

Andererseits gibt es nach den Bemerkungen zu Satz 3.6 eindeutige Polynome q(x) und r(x) mit $0 \leq \text{Grad}(r(x)) < d$, so dass gilt

$(x^n - 1) = q(x) \cdot (x^d - 1) + r(x)$.

Der Vergleich der beiden Darstellungen für $(x^n - 1)$ ergibt

$$q(x) = \frac{x^s \cdot (x^{m \cdot d} - 1)}{(x^d - 1)} \quad \text{und} \quad r(x) = (x^s - 1) .$$

Dabei ist q(x) ein Polynom und $(x^d - 1)$ wegen $s < d$ kein Teiler von x^s.

Daraus folgt: $(x^m - 1) | (x^n - 1)$ gdw $r(x) = 0$ gdw $s = 0$ gdw $m | n$.

Satz 3.30: (Unterkörper GF(p^m) eines GF(p^n))

Jeder Erweiterungskörper GF(p^n) eines GF(p) enthält zu jedem Teiler m von n genau einen Erweiterungskörper GF(p^m) des GF(p), der als Zerfällungskörper von $(x^{p^m} - x)$ ein Unterkörper des GF(p^n) ist.

Beweis:

Nach Satz 3.28 ist jedes Element aus dem GF(p^m) bzw. aus dem GF(p^n) eine Wurzel von $(x^{p^m} - x)$ bzw. von $(x^{p^n} - x)$.

Weiter folgt aus Satz 3.29 für m|n:

$(x^m - 1) | (x^n - 1)$ bzw. (für x = p) $(p^m - 1) | (p^n - 1)$ bzw.

$(x^{p^{m-1}} - 1) | (x^{p^{n-1}} - 1)$ bzw. (um den Faktor x erweitert)

$(x^{p^m} - x) | (x^{p^n} - x)$.

Dabei enthält $(x^{p^n} - x)$ natürlich alle Wurzeln seines Teilers $(x^{p^m} - x)$.

Also ist der Erweiterungskörper GF(p^m) ein Unterkörper des GF(p^n).

Satz 3.31: (Faktoren eines Polynomes der Form ($x^{p^m} - x$))

Jedes irreduzible normierte Polynom g(x) vom Grad m über dem Koeffizientenkörper GF(p) ist ein Faktor bzw. ein Teiler des Polynomes $f(x) = (x^{p^m} - x)$.

Beweis:

a) Polynome vom **Grad 1** sind von der Form $g(x) = x + a$ mit $a \in GF(p)$, und sie besitzen die Wurzel $x = -a$ (speziell auch $-a = 0$). Jede dieser Wurzeln ist auch eine Wurzel von $f(x)$. Damit ist $g(x)$ ein Teiler von $f(x) = (x^p - x) = (x^{p-1} - x) \cdot x$ (vgl. Satz 3.27 mit $m = 1$).

b) Ist der **Grad m > 1**, so erzeugt $g(x)$ gemäß Satz 3.27 den Erweiterungskörper $GF(p^m)$, und die Restpolynome des $GF(p^m)$ mit Ausnahme der 0 bilden eine multiplikative Gruppe der Ordnung $p^m - 1$. Damit ist die Ordnung r jeder Wurzel $r(u)$ von $g(x)$ ein Teiler von $p^m - 1$ und weiter ist $r(u)^{p^m-1} - 1 = 0$. Also handelt es sich bei $r(u)$ (für $x = r(u)$ gesetzt) auch um eine Wurzel von $(x^{p^m-1} - 1)$ sowie von $(x^{p^m} - x)$.
Schließlich folgt aus Satz 3.28 $g(x) | (x^{p^m} - x)$.

Satz 3.32: (Grade von Teilerpolynomen)
- ausführlicher Beweis in /10/ -

Jedes irreduzible Teilerpolynom $g(x)$ von $(x^{p^m} - x)$ ist vom Grad $\leq m$.

Beweisskizze:

Jedes Polynom $g(x)$, das Teiler von $(x^{p^m} - x)$ ist, besitzt gemäß Satz 3.28 und Satz 3.22b ausschließlich Wurzeln aus dem Erweiterungskörper $GF(p^m)$. Für irreduzible Polynome vom $Grad(g(x)) = k$ ergeben sich gemäß Satz 3.22a Wurzeln der Form $r(u)^{p^0}, \ldots, r(u)^{p^{k-1}}$.
Weiter ist gemäß Satz 3.16 $r(u)^{p^m} = r(u)^{p^0}$, d. h. $g(x)$ besitzt maximal m verschiedene Wurzeln, d. h. $g(x)$ ist maximal vom Grad m.

Beispiel 3.11: (Teiler und Wurzeln des Hauptpolynomes $(x^{63} - 1)$)

a) Sei $f(x) = (x^{2^6-1} - 1) = (x^{63} - 1)$.
Dann bilden gemäß Satz 3.28 alle Wurzeln von $f(x)$ zusammen die multiplikative Gruppe des $GF(2^6)$, und $f(x)$ besteht ganz aus Linearfaktoren der Form $(x - r(u))$ mit $r(u) \in GF(2^6)$, d. h. es ergibt sich $f(x) = (x - 1) \cdot (x - u) \ldots (x - (u^5+u^4+u^3+u^2+u^1+1))$.

Weiter sind gemäß Satz 3.29 alle Polynome der Form $(x^m - 1)$ mit $m|63$ also mit $m \in \{1,3,7,9,21,63\}$ Teiler von f(x), und zu jedem dieser Teiler, der die Form $m = 2^k - 1$ besitzt, d. h. zu $k \in \{1,2,3,6\}$, gibt es gemäß Satz 3.28 Unterkörper des $GF(2^6)$, also die Unterkörper $GF(2^1)$, $GF(2^2)$, $GF(2^3)$, $GF(2^6)$.

b) Jede Wurzel von f(x) ist auch eine Wurzel von mindestens einem der Faktoren $(x^m - 1)$, und die Ordnung s der Wurzel ist jeweils ein Teiler der Länge des Hauptzyklusses dieser Faktoren.

c) Z. B. gilt für die Wurzeln, deren Ordnungen 1,3,9 Teiler von 9 sind:

Polynom	**Wurzel-Ordnung**	**Zyklen von Wurzeln $r(u)^{p^i}$** $[\neq r(u)^i]$
$(x - 1)$	1 (Teiler von 1)	1
$(x^3 - 1)$	1 (Teiler von 3) 3 (Teiler von 3)	1 u^{21}, u^{42} [mit $(u^{21})^3 = u^{63}$]
$(x^9 - 1)$	1 (Teiler von 9) 3 (Teiler von 9) 9 (Teiler von 9)	1 u^{21}, u^{42} [mit $(u^{21})^3 = u^{63}$] $u^7, u^{14}, u^{28}, u^{56}, u^{49}, u^{35}$ [mit $(u^7)^9 = u^{63}$]

d) Im Folgenden werden Polynome $f_1(x)$, $f_3(x)$, ... , $f_{63}(x)$ konstruiert der Art, dass jedes $f_i(x)$ als Wurzeln genau alle Elemente der Ordnung i aus dem $GF(2^6)$ besitzt.

Als Ausgangspunkt dienen dabei die Polynome der Form $(x^i - 1)$, von denen jedes mindestens eine Wurzel der Ordnung i aufweist. Alle Wurzeln einer anderen Ordnung als i müssen dann nur noch eliminiert werden.

Damit ergeben sich (zum Teil reduzible) Teilerpolynome von f(x), die insgesamt genau alle Wurzeln aller Ordnungen von f(x) besitzen, wie folgt

$f_1(x) = (x - 1)$ vom Grad 1,

$$f_3(x) = \frac{(x^3 - 1)}{f_1(x)} = x^2 + x + 1 \quad \text{vom Grad 2,}$$

$$f_7(x) = \frac{(x^7 - 1)}{f_1(x)} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \quad \text{vom Grad 6,}$$

$$f_9(x) = \frac{(x^9 - 1)}{f_1(x)\cdot f_3(x)} = x^6 + x^3 + 1 \qquad \text{vom Grad 6,}$$

$$f_{21}(x) = \frac{(x^{21} - 1)}{f_1(x)\cdot f_3(x)\cdot f_7(x)} \qquad \text{vom Grad 12,}$$

$$f_{63}(x) = \frac{(x^{63} - 1)}{f_1(x)\cdot f_3(x)\cdot f_7(x)\cdot f_9(x)\cdot f_{21}(x)} \qquad \text{vom Grad 36.}$$

Damit besitzt also $(x^{63} - 1) = f_1(x)\cdot f_3(x)\cdot f_7(x)\cdot f_9(x)\cdot f_{21}(x)\cdot f_{63}(x)$ als Wurzeln alle Elemente des $GF(2^6)$ der Ordnungen 1,3,7,9,21,63.

d) Gemäß dem Beweis zu Satz 3.4b gibt es im $GF(2^6)$ mindestens ein primitives Element, das alle Elemente der multiplikativen Gruppe erzeugt und Wurzel eines primitiven Polynomes vom Grad 6 ist.

e) Diene $g(x) = x^6 + x + 1$ als primitives Polynom (vgl. /4/, Seite 82). Dann ergeben sich die Wurzeln von f(x), abhängig von der Wahl von g(x), als Wurzeln der Teiler $f_1(x)$, ... ,$f_{63}(x)$ wie folgt

Poly-nom	**Wurzel-Ordnung**	**Zyklus von Wurzeln $r(u)^{p^i}$** $[\neq r(u)^i]$	**Polynom ist irreduzibel**
$f_1(x)$	1	1	ja
$f_3(x)$	3	u^{21},u^{42}	ja
$f_7(x)$	7	u^9,u^{18},u^{36} bzw. u^{27},u^{54},u^{45}	nein (+)
$f_9(x)$	9	$u^7,u^{14},u^{28},u^{56},u^{49},u^{35}$	ja
$f_{21}(x)$	21	$u^3,u^6,u^{12},u^{24},u^{48},u^{33}$ bzw. $u^1,u^2,u^4,u^8,u^{16},u^{32}$	nein (+)
$f_{63}(x)$	63	$u^5,u^{10},u^{20},u^{40},u^{17},u^{34}$ bzw. $u^{11},u^{22},u^{44},u^{25},u^{50},u^{37}$ bzw. $u^{13},u^{26},u^{52},u^{41},u^{19},u^{38}$ bzw. $u^{15},u^{30},u^{60},u^{37},u^{51},u^{39}$ bzw. $u^{31},u^{62},u^{61},u^{59},u^{55},u^{47}$ bzw. $u^{53},u^{43},u^{23},u^{46},u^{29},u^{59}$	nein (++)

(+) / (++): 2 bzw. 6 Wurzelzyklen definieren 2 bzw. 6 irreduzible Teilerpolynome