

# Kryptographie

## AES und Galois-Körper



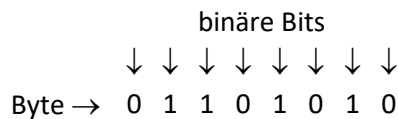
pixabay

# Inhalt

1	Endliche Körper – Der Galois-Körper $GF(2^8)$ .....	2
2	AES (Advanced Encryption Standard) .....	2
3	Der Begriff „Körper“ .....	4
4	Rechnen in $GF(2^n)$ mit $\oplus$ und $\odot$ .....	5
4.1	Das Problem der Umkehrbarkeit.....	5
4.2	Bitweise Addition modulo 2 im binären Zahlenbereich .....	6
5	Die Probleme mit der Multiplikation .....	7
5.1	Bitweise Multiplikation modulo 2 im binären Zahlenbereich .....	7
5.2	Irreduzible Binärzahlen.....	8
6	Eine Alternative – Der Polynomring $\mathbb{Z}_2[X]$ .....	11
7	Vergleich $GF(2^n)$ versus $\mathbb{Z}_2[X]$ .....	12
8	Anhang .....	14
	Übungen .....	14

# 1 Endliche Körper – Der Galois-Körper $GF(2^8)$

Moderne Kryptosysteme sind digitale Algorithmen zur Verschlüsselung elektronischer Daten und gehorchen den Gesetzen der Bits und Bytes. Die Bytes sind die Zahlen, die Bits ihre Ziffern.



Von der kleinsten Zahl 0000 0000 über Zahlen wie 01101010 bis zur größten Zahl 1111 1111 sind es insgesamt  $2^8 = 256$  Zahlen. Es handelt sich also um einen begrenzten (endlichen) Zahlenbereich in dem addiert und multipliziert werden soll.

Ein endlicher algebraische Zahlenbereich mit den angegebenen Eigenschaften wird nach dem französischen Mathematiker Évariste Galois (1811-1832) „Galois-Körper“ oder „Galois-Field“ bezeichnet.

## 2 AES (Advanced Encryption Standard)

AES ist ein Verschlüsselungsverfahren, welches eine öffentliche Ausschreibung des National Institute of Standards and Technology (NIST) gewann und im Jahr 2000 als neuer US-amerikanischer Standard bekanntgegeben wurde. AES wird weltweit in Software und Hardware implementiert, um sensible Daten zu verschlüsseln und gilt als sicher.



Abb. 1: Joan Daemen und Vincent Rijmen [\(Quelle\)](#)

Kernstück des von Joan Daemen und Vincent Rijmen entwickelten Kryptosystems ist der sogenannte Rijndael-Algorithmus. Er verwendet variable, voneinander unabhängige Block- und Schlüssellängen und verschlüsselt dabei in mehreren Durchgängen (Runden).

Jede Runde besteht aus mehreren Verarbeitungsschritten, die das Ersetzen, Transponieren und Mischen des eingegebenen Klartexts umfassen, um ihn zu verschlüsseln.

Dazu werden die Daten in Blöcke zu je 16 Byte (128 Bit) in quadratische 4x4-Blöcke geschrieben, die dann den Verarbeitungsschritten unterworfen werden.

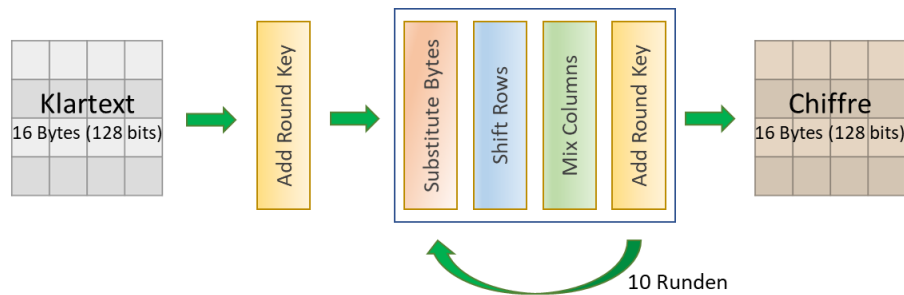
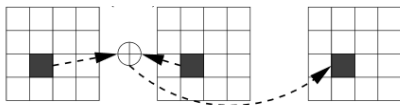
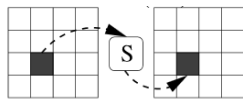


Abb. 2

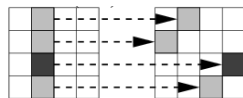
1. Key Expansion: Aus dem Hauptschlüssel werden mehrere 128bit Rundenschlüssel generiert.
2. AddRoundKey: Addition  $\oplus$  jedes Bytes im Block mit einem Teil des Schlüssels.



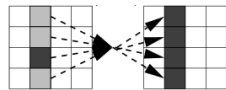
3. Die Runden:
  - a. SubBytes: Ersetzt jedes Byte nach einem gewissen Algorithmus.



- b. ShiftRows: Verschiebung der Bytes einer Spalte durch Matrixmultiplikation  $\odot$ .



- c. MixColumns: Nur in den Runden 1 bis 9. Mischt in den Spalten.



- d. AddRoundKey: Addition des Rundenschlüssels

AES ist ein symmetrisches Verschlüsselungsverfahren. Daher muss jeder Schritt eindeutig umkehrbar sein.

AES verwendet den endlichen Zahlenbereich von 256 Bytes und eigene Formen der Addition  $\oplus$  und Multiplikation  $\odot$ . Dieser Zahlenbereich ist ein sogenannter Galois-Körper.

$$GF(2^8) = GF(256) = (\{00000000, 00000001, \dots, 01111111, 10000000\}; \oplus, \odot)$$

### 3 Der Begriff „Körper“

Unter dem algebraischen Begriff „Körper“ versteht man einen Rechenbereich mit zwei Rechenarten (Addition und Multiplikation), in dem man, wie mit den reellen Zahlen gewohnt, rechnen kann. Das sind folgende Rechengesetze:

- ❖ Zuerst einmal dürfen Addition bzw. Multiplikation nicht aus dem Zahlenbereich hinausführen. Zwei Zahlen addiert oder multipliziert ergeben wieder eine Zahl aus dem Zahlenbereich. (**Abgeschlossenheit**)
- ❖ Sowohl Addition als auch Multiplikation haben ein **neutrales Element**.  
Bei der Addition in  $\mathbb{R}$  ist es die Null (z.B.:  $7,12 + 0 = 7,12$ ).  
Bei der Multiplikation ist es die Eins (z.B.:  $7,12 \cdot 1 = 7,12$ ).
- ❖ Jede Addition kann durch eine weitere Addition wieder rückgängig gemacht werden.  
z.B.:  $7,12 + 2,5 + (-2,5) = 7,12$ . Dabei ist  $(-2,5)$  die „**additiv Inverse**“ zu  $(+2,5)$ .  
ADDITION MIT DER INVERSEN ENTSpricht DER SUBTRAKTION.
- ❖ Jede Multiplikation, außer mit der Null, kann durch eine weitere Multiplikation wieder rückgängig gemacht werden.  
z.B.:  $7,12 \cdot 2,5 \cdot 0,4 = 7,12$ . Dabei ist  $0,4 = \frac{1}{2,5} = 0,4^{-1}$  die „**multipl. Inverse**“ zu 2,5.  
MULTIPLIKATION MIT DER INVERSEN ENTSpricht DER DIVISION.
- ❖ Es gelten die **Kommutativ-** und **Assoziativgesetze** und das **Distributivgesetz**.

Um **uneingeschränkt** und vor allem **umkehrbar** rechnen zu können, muss der gewählte Rechenbereich die Eigenschaften eines algebraischen **Körpers** besitzen!!!

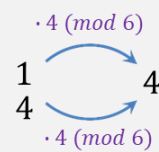
## 4 Rechnen in $GF(2^n)$ mit $\oplus$ und $\odot$

### 4.1 Das Problem der Umkehrbarkeit

Restklassenringe  $(\mathbb{Z}_m, +, \cdot)$  mit normaler Addition und Multiplikation sind für symmetrische Kryptosysteme vielfach unbrauchbar, da sie algebraisch meist keine Körper sind. Etliche Elemente von  $\mathbb{Z}_m$  haben bezüglich der Multiplikation nämlich keine Inverse. Multiplikationen lassen sich dann nicht zurückrechnen, was aber für das Entschlüsseln in symmetrischen Kryptosystemen essenziell ist.

**BEISPIEL:**  $(\mathbb{Z}_6, +, \cdot)$

Sowohl  $1 \cdot 4 \equiv 4$  als auch  $4 \cdot 4 = 16 \equiv 4$ . Wird mit  $(\cdot 4) \bmod 6$  verschlüsselt, so ist das bei der Entschlüsselung fatal.



Es gibt aber Ausnahmen. Alle Restklassenringe  $(\mathbb{Z}_p, +, \cdot)$  mit einer Primzahl  $p$  als Modulus erfüllen sämtliche Körpereigenschaften, sind also immer auch Restklassenkörper.

Da 10 keine Primzahl ist, ist folglich das Rechnen modulo 10 in  $(\mathbb{Z}_{10}, +, \cdot)$  für Kryptosysteme unbrauchbar.

Das Gleiche gilt für die digital relevante Zahl 256. Somit wäre  $(\mathbb{Z}_{256}, +, \cdot)$  ebenfalls für Kryptosysteme unbrauchbar und ist es auch.

Allerdings haben Restklassen der Form  $\mathbb{Z}_{p^n}$  mit  $n \in \mathbb{N}, p \dots$  prim eine Sonderstellung. Mit geeigneten Rechnungsarten lassen sich damit nämlich Restklassenkörper konstruieren.

**SATZ:**

Für alle Restklassenringe der Form  $(\mathbb{Z}_{p^n}, +, \cdot)$  ( $n, p \in \mathbb{N}, p \dots$  prim) existiert ein Erweiterungskörper  $(\mathbb{Z}_{p^n}, \oplus, \odot)$  mit geeigneten Rechnungsarten  $\oplus$  und  $\odot$ .

Damit ist  $\mathbb{Z}_{256}$  wieder im Rennen,  $256 = 2^8$  ist ja eine Potenz der Primzahl 2. Für  $\mathbb{Z}_{2^8}$  muss es also Rechenarten geben, mit denen man uneingeschränkt vorwärts und rückwärts „rechnen“ kann. Und diese sind die bitweise Addition und Multiplikation modulo 2.

## 4.2 Bitweise Addition modulo 2 im binären Zahlenbereich

### Byte und „Half-Byte“

Um es ein bisschen einfacher und übersichtlicher zu machen, reduzieren wir die Anzahl der Stellenwerte von 8 auf 4. Nennen wir es ein Half-Byte (HByte).

$$1 \text{ Byte} = 8 \text{ Bit} \rightarrow 1 \text{ HByte} = 4 \text{ Bit}$$

ADDITION

$$\begin{array}{r} 1\ 1\ 0\ 1 \\ \oplus\ 1\ 0\ 1\ 1 \\ \hline 0\ 1\ 1\ 0 \end{array}$$

UMKEHRUNG: SUBTRAKTION

$$\begin{array}{r} 1\ 1\ 0\ 1 \\ \ominus\ 1\ 0\ 1\ 1 \\ \hline 0\ 1\ 1\ 0 \end{array}$$

**BEMERKUNG:**

- Bei bitweisem Rechnen mit Binärzahlen ist das Ergebnis von  $\oplus$  und  $\ominus$  das Gleiche:

$$a \oplus b = a \ominus b$$

$$(\text{z.B.: } 0 \ominus 1 \equiv 2 \ominus 1 = 1 \text{ bzw. } 0 \oplus 1 = 1)$$

Somit ist bei der Addition  $\oplus$  das inverse Element von  $a$  wieder  $a$ !

**Die bitweise Addition modulo 2 im binären Zahlenbereich ist umkehrbar!!!**

Verschlüsselung durch Addition des Schlüssels, Entschlüsselung durch abermalige Addition des Schlüssels.

**BEISPIEL:**

**VERSCHLÜSSELUNG:** Addition des Schlüssels **1011**

Klartext: **1101**  $\rightarrow$  Geheimtext: **1101**  $\oplus$  **1011** = **0110**

**ENTSCHLÜSSELUNG:** Addition des Schlüssels **1011**

Geheimtext: **0110**  $\rightarrow$  Klartext: **0110**  $\oplus$  **1011** = **1101**

## 5 Die Probleme mit der Multiplikation

### 5.1 Bitweise Multiplikation modulo 2 im binären Zahlenbereich

MULTIPLIKATION

$$\begin{array}{r} 0110 \odot 1101 \\ \hline 0110 \\ 0110 \\ 0000 \\ 0110 \\ \hline 101110 \end{array}$$

$\mathbb{Z}_{2^4}$  ist ein endlicher Zahlenbereich und umfasst nur 16 vierstellige Binärzahlen. Die Multiplikation

$$0110 \odot 1101 = 101110$$

ist 6-stellig und führt somit aus dem Bereich hinaus.  $\mathbb{Z}_{2^4}$  und auch allgemein  $\mathbb{Z}_{2^n}$  sind bezüglich der Multiplikation  $\odot$  nicht abgeschlossen.

Die „Caesar-Chiffre“, die bei der Verschlüsselung jeden Buchstaben um einen gewissen Wert im Alphabet verschiebt (z.B.: „N“  $\xrightarrow{+3}$  „Q“), beginnt hinter „Z“ wieder mit „A“ und rechnet so modulo 26.

Ähnlich dem Caesar-Algorithmus wird auch in  $\mathbb{Z}_{2^n}$  bzw. in  $GF(2^n)$  durch Rechnen in Restklassen die Abgeschlossenheit erzwungen.

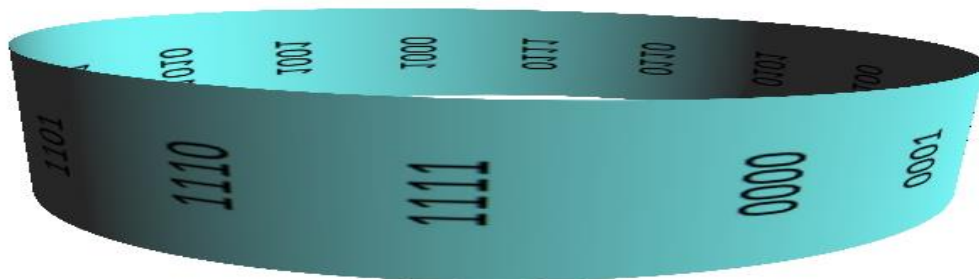


Abb. 3: Restklasse modulo  $10000_{\text{bin}}$  ( $16_{\text{dez}}$ )

Der logische Modulus  $16 \hat{=} 10000$ , wie in Abb. 3 angedeutet eignet sich dafür, es geht aber besser! **Wir brauchen Abgeschlossenheit und Umkehrbarkeit!**



## 5.2 Irreduzible Binärzahlen

### Anforderungen an den Modul

- ❖ Der Modul muss eine Stelle mehr besitzen, also 5-stellig sein.  
(Möchte man im dekadischen System 1-stellig bleiben, so muss man modulo 10 rechnen. Der Modul 10 ist zwar 2-stellig, die Reste aber dann 1-stellig. Z.B.:  $56 \bmod 10 = 6$ )
- ❖ Damit  $GF(2^4)$  mit der beschriebenen Addition  $\oplus$  bzw. Multiplikation  $\odot$  algebraisch wirklich alle Körpereigenschaften besitzt, muss sich der Modul bezüglich  $\odot$  wie eine Primzahl verhalten. Er darf sich nicht faktorisieren lassen, außer mit  $0001 \cong 1$  und sich selbst. So ist 10000 eben nicht geeignet, da  $10000 = 1000 \odot 0010$  faktorisierbar ist. Es gibt aber sogenannte irreduzible Binärzahlen, die dafür geeignet sind.

#### DEFINITION:

Eine Binärzahl  $p$  heißt irreduzibel, wenn sie sich nicht als ein Produkt zweier Binärzahlen, abgesehen von 1 und  $p$  selbst, darstellen lässt.

Damit haben irreduzible Binärzahlen die Bedeutung von Primzahlen.

Ohne Beweis sind das für  $GF(2^4)$  die Zahlen

10011, 11001, 11111

Wir wählen eine der angeführten, z.B.:

$$p = 11111.$$

### Abgeschlossenheit durch modulo 11111

Um eine Zahl  $\geq 256$  binär modulo  $p$  zu reduzieren, muss  $p$  mehrfach von  $b$  subtrahiert und so der Rest  $r$  ermittelt werden. Das mehrfache Subtrahieren entspricht üblicherweise der Division. Also wird der Modul  $p$  bzw. ein Vielfaches des Moduls ( $p \cdot 100, p \cdot 10, \text{etc.}$ ) so lange subtrahiert (= addiert), bis ein 4stelliger Rest übrigbleibt. Führungsnollen können gestrichen werden.

Dadurch entsteht ein Zahlenbereich, der auch bezüglich der Multiplikation abgeschlossen ist. Bezeichnung:  $\mathbb{Z}_2^n/p$

Bei der Addition ändert sich durch die Restklassenbestimmung nichts, da die Ergebnisse dort nicht aus  $\mathbb{Z}_2^n$  hinausführen. (Analog zu  $205 + 120 = 325 \equiv 325 \bmod 1000$ )

BEISPIEL:  $1101100110 \equiv 0011 \pmod{11111}$

$$\begin{array}{r}
 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0 \\
 \oplus \\
 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0 \\
 \hline
 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0 \\
 \oplus \\
 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0 \\
 \hline
 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\
 \oplus \\
 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0 \\
 \hline
 0\ 0\ 0\ 0\ 0\ 1\ 1\ R
 \end{array}$$

BEISPIEL:  $10110 \equiv 1111 \pmod{11111}$

$$\begin{array}{r}
 1\ 0\ 1\ 1\ 1\ 0 \\
 \oplus \\
 1\ 1\ 1\ 1\ 1\ 0 \\
 \hline
 0\ 1\ 0\ 0\ 0\ 0 \\
 \oplus \\
 1\ 1\ 1\ 1\ 1 \\
 \hline
 0\ 1\ 1\ 1\ 1\ R
 \end{array}$$

Für das Problem der aus dem Zahlenbereich hinausschießenden Multiplikation

$$0110 \odot 1101 = 101110$$

aus der Einleitung, ergibt sich somit die Lösung

$$0110 \odot 1101 = 101110 \equiv 1111 \pmod{11111} \blacksquare$$

## Umkehrbarkeit durch modulo 11111

Die Multiplikationstabelle von  $GF(2^4)$  mit  $p = 11111$

$\odot$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
0001	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0000	0010	0100	0110	1000	1010	1100	1110	1111	1101	1011	1001	0111	0101	0011	0001
0011	0000	0011	0110	0101	1100	1111	1010	1001	0111	0100	0001	0010	1011	1000	1101	1110
0100	0000	0100	1000	1100	1111	1011	0111	0011	0001	0101	1001	1101	1110	1010	0110	0010
0101	0000	0101	1010	1111	1011	1110	0001	0100	1001	1100	0011	0110	0010	0111	1000	1101
0110	0000	0110	1100	1010	0111	0001	1011	1101	1110	1000	0010	0100	1001	1111	0101	0011
0111	0000	0111	1110	1001	0011	0100	1101	1010	0110	0001	1000	1111	0101	0010	1011	1100
1000	0000	1000	1111	0111	0001	1001	1110	0110	0010	1010	1101	0101	0011	1011	1100	0100
1001	0000	1001	1101	0100	0101	1100	1000	0001	1010	0011	0111	1110	1111	0110	0010	1011
1010	0000	1010	1011	0001	1001	0011	0010	1000	1101	0111	0110	1100	0100	1110	1111	0101
1011	0000	1011	1001	0010	1101	0110	0100	1111	0101	1110	1100	0111	1000	0011	0001	1010
1100	0000	1100	0111	1011	1110	0010	1001	0101	0011	1111	0100	1000	1101	0001	1010	0110
1101	0000	1101	0101	1000	1010	0111	1111	0010	1011	0110	1110	0011	0001	1100	0100	1001
1110	0000	1110	0011	1101	0110	1000	0101	1011	1100	0010	1111	0001	1010	0100	1001	0111
1111	0000	1111	0001	1110	0010	1101	0011	1100	0100	1011	0101	1010	0110	1001	0111	1000

Tabelle 1

In jeder Spalte und jeder Zeile findet sich einmal die 0001, das neutrale Element der Multiplikation. Dazu gehören jeweils die beiden zueinander inversen Elemente.

**Die bitweise Multiplikation modulo 2** mit anschließendem Verringern der Stellenanzahl durch **modulo  $p$**  ( $p$  irreduzibel) im binären Zahlenbereich ist **umkehrbar!!!**

Verschlüsselung durch Multiplikation eines Schlüssels, Entschlüsselung durch Multiplikation der Inversen.

#### BEISPIEL:

**VERSCHLÜSSELUNG** durch Multiplikation des Schlüssels **1001**

Klartext: **1101** → Geheimtext: **1101**  $\odot$  **1001** = **0110**

**ENTSCHLÜSSELUNG** durch Multiplikation des Schlüssels **0111**

Geheimtext: **0110** → Klartext: **0110**  $\odot$  **0111** = **1101**

#### MATHEMATISCHER HINTERGRUND:

$$(T \odot S) \odot S^{-1} = T \odot (S \odot S^{-1}) = T \odot 1 = T$$

$$(1101 \odot 1001) \odot 0111 = 1101 \odot (1001 \odot 0111) = 1101 \odot 0001 = 1101$$

#### Zusammenfassung:

Die Restklassen  $\mathbb{Z}_{2^n}$  modulo  $p$  mit bitweiser Addition und Multiplikation modulo 2 und irreduziblem  $p$  (Bezeichnung  $\mathbb{Z}_{2^n}/p$ ) bilden einen Galois-Körper  $GF(2^n)$ , in dem Additionen und Multiplikationen umkehrbar sind.

Analoges gilt für den Advanced Encryption Standard AES, nur in der Erweiterung auf  $GF(256)$ . Als eine der möglichen irreduziblen Binärzahlen wurde für den AES die Zahl 100011010 festgelegt.

Die im Kryptosystem AES verwendeten 256 Bytes des Zahlenraums  $GF(2^8)$  sind die binären Restklassen modulo 100011010 einer bitweisen Addition und Multiplikation modulo 2.

## 6 Eine Alternative – Der Polynomring $\mathbb{Z}_2[X]$

In einem Stellenwertsystem haben die unterschiedlichen Stellenwerte unterschiedliche Bezeichnungen. Betrachten wir die Zahl 2357 im dekadischen Zahlensystem, so sind alternative Schreibweisen möglich.

$$2357 = 2T3H\ 5Z7E = 2T + 3H + 5Z + 7E = 2 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0$$

In der Schreibweise  $2357 = 2 \cdot X^3 + 3 \cdot X^2 + 5 \cdot X^1 + 7 \cdot X^0$  mag  $X$  für die römische Zehn stehen, könnte aber auch einfach symbolisch den Basis-Stellenwert darstellen.

Andererseits stellt  $2X^3 + 3X^2 + 5X^1 + 7X^0$  ein Polynom in  $X$  mit einstellig ganzzahligen Koeffizienten dar.

### DEFINITION:

Seien  $a_{n-1}, \dots, a_0$  die  $n$  Ziffern einer ganzen Zahl in einem Stellenwertsystem, so heißt das Polynom

$$a_{n-1}X^{n-1} + \dots + a_0X^0$$

die **Polynomdarstellung** der Zahl.

### BEISPIELE:

$$806152 \cong 8X^5 + 0X^4 + 6X^3 + 1X^2 + 5X^1 + 2X^0 = 8X^5 + 6X^3 + X^2 + 5X + 2$$

$$10110100 \cong X^7 + X^5 + X^4 + X^2$$

Im dekadischen System sind die Polynomdarstellungen Polynome in  $X$  mit der Koeffizientenmenge  $K = \{0,1,2,3,4,5,6,7,8,9\} = \mathbb{Z}_{10}$

Im binären System sind die Polynomdarstellungen Polynome in  $X$  mit der Koeffizientenmenge  $K = \mathbb{Z}_2$

### DEFINITION:

$K[X]$  bezeichnet die algebraische Struktur bestehend aus der Menge aller Polynome mit Koeffizienten aus  $K$  und der Variablen  $X$  zusammen mit der üblichen Addition und Multiplikation von Polynomen.

Je nachdem, ob  $(K, +, \cdot)$  algebraisch ein Ring oder ein Körper ist, bezeichnet man  $K[X]$  als Polynomring oder Polynomkörper.

## 7 Vergleich $GF(2^n)$ versus $\mathbb{Z}_2[X]$

### BEISPIELE:

Addition  $1011 \oplus 0110 = 1101$

$$(X^3 + X + 1) + (X^2 + X) = X^3 + X^2 + 2X + 1 \equiv_2 X^3 + X^2 + 1 \cong 1101$$

Multiplikation  $1011 \odot 0110 = 111010 \equiv_{1111} 0110$

$$\begin{aligned}(X^3 + X + 1) \cdot (X^2 + X) &= X^5 + X^4 + X^3 + 2X^2 + X = \\ &= X^5 + X^4 + X^3 + 2X^2 + X \equiv_2 X^5 + X^4 + X^3 + X \cong 111010\end{aligned}$$

Vergleicht man die Rechnungsarten in  $GF(2^n)$  mit denen in  $\mathbb{Z}_2[X]$ , so scheinen sie einander zu entsprechen.

$\mathbb{Z}_2[X]$  ist im Gegensatz zu  $GF(2^n)$  algebraisch nur ein Ring, es fehlt also die multiplikative Inverse. Außerdem ist  $\mathbb{Z}_2[X]$  bezüglich der Multiplikation nicht abgeschlossen. Genauso wie in  $GF(2^n)$  bedarf es einer Modulo-Rechnung mit einem irreduziblen Element.

### DEFINITION:

Ein Polynom  $p$  heißt irreduzibel, wenn es sich nicht als ein Produkt zweier Polynome, abgesehen von 1 und  $p$  selbst, darstellen lässt.

Die Restklassen werden hier durch die übliche Polynomdivision mit einem irreduziblen Polynom  $p$  ermittelt.

Beispiel:

$$1011 \odot 0110 \cong (X^3 + X + 1) \cdot (X^2 + X) \equiv_2 X^5 + X^4 + X^3 + X$$

Z.B.: Das irreduzible Polynom  $X^3 + X^2 + X + 1$  entspricht der irreduziblen Zahl 1111 für vierstellige Binärzahlen.

$$\begin{aligned}(X^5 + X^4 + X^3 + X) : (X^3 + X^2 + X + 1) &= X^2 \\ \pm X^5 \pm X^4 \pm X^3 \pm X^2 & \text{ (+ und - liefern dasselbe Ergebnis)} \\ 0 + 0 + 0 + X^2 + X & \text{ Restpolynom}\end{aligned}$$

$$\text{Lösung: } (X^3 + X + 1) \cdot (X^2 + X) \equiv_2 X^5 + X^4 + X^3 + X \equiv_p X^2 + X \cong 0110 \blacksquare$$

### BEZEICHNUNG:

$\mathbb{Z}_2[X]/p$  ist der über den Polynomring mit Hilfe des irreduziblen Polynoms  $p$  erzeugte endliche Polynom-Restklassenkörper.

$\mathbb{Z}_2[X]/p$  ist isomorph zu  $GF(2^n)$

**BEISPIEL:**

Die 16 Binärzahlen von  $GF(2^4)$  entsprechen den 16 Polynomen von  $\mathbb{Z}_2[X]/p$  mit  $p = X^3 + X^2 + X + 1$ .

Diese sind:  $\{0, 1, X, X^2, X^3,$

$X + 1, X^2 + 1, X^3 + 1, X^3 + X, X^3 + X^2, X^2 + X,$

$X^3 + X^2 + X, X^3 + X^2 + 1, X^3 + X + 1, X^2 + X + 1, X^3 + X^2 + X + 1\}$

## 8 Anhang

### Übungen

#### 01 Bitweise Addition

$$\oplus \begin{array}{|c|c|c|c|} \hline 0 & 1 & 1 & 0 \\ \hline 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 \\ \hline \end{array}$$

$$\oplus \begin{array}{|c|c|c|c|} \hline 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \\ \hline & & & \\ \hline \end{array}$$

$$\oplus \begin{array}{|c|c|c|c|} \hline 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \\ \hline & & & \\ \hline \end{array}$$

$$\oplus \begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline & & & & & & & \\ \hline \end{array}$$

$$\oplus \begin{array}{|c|c|c|c|c|c|c|c|} \hline 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ \hline & & & & & & & \\ \hline \end{array}$$

#### 02 Bitweise Multiplikation in $(\mathbb{Z}_4, \oplus, \odot)$

1	0	1	1	$\odot$	0	1	0	1
0	0	0	0					
	1	0	1	1				
		0	0	0	0			
			1	0	1	1		
	1	0	0	1	1	1		

1	1	0	0	$\odot$	1	0	1	1

0	1	1	1	$\odot$	0	1	1	0

#### 03 Bitweise Multiplikation in $(\mathbb{Z}_4/p, \oplus, \odot)$ mit $p = 11111$

1	0	1	1	$\odot$	0	1	0	1
	$\searrow$	$\searrow$	$\searrow$	$\searrow$	$\searrow$			
		1	0	0	1	1	1	
$\oplus 10p$	1	1	1	1	1	1	0	
		0	1	1	0	0	1	
$\oplus p$	1	1	1	1	1			
		0	0	1	1	0		

1	1	0	0	$\odot$	1	0	1	1
$\searrow$	$\searrow$	$\searrow$	$\searrow$	$\searrow$				

0	1	1	1	$\odot$	0	1	1	0
$\searrow$	$\searrow$	$\searrow$	$\searrow$	$\searrow$				

#### 04 Restklassen $(\mathbb{Z}_5, +, \cdot)$ versus $(\mathbb{Z}_6, +, \cdot)$

$$\mathbb{Z}_5 \quad +$$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3					
4					

$$\mathbb{Z}_5 \quad \cdot$$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3					
4					

$$\mathbb{Z}_6 \quad +$$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3						
4						
5						

$$\mathbb{Z}_6 \quad \cdot$$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3						
4						
5						

- Ergänze die Verknüpfungstabellen!
- Woran erkennt man die Kommutativität?
- Was ist das additiv inverse Element von „2“ in  $\mathbb{Z}_5$ ?
- Besitzt jedes Element in  $\mathbb{Z}_5$  eine additiv Inverse?
- Was ist die multiplikativ Inverse von „5“ in  $\mathbb{Z}_6$ ?
- Besitzt jedes Element in  $\mathbb{Z}_6$  eine multiplikativ Inverse?
- Besitzt jedes Element in  $\mathbb{Z}_5$  eine multiplikativ Inverse?

#### 04 Verschlüsseln und Entschlüsseln in $GF(2^4)$

Entnimm der Multiplikationstabelle (Tabelle 1) die gesuchten Schlüssel!

Encrypt Key	1001	0110	0011	0000		
Decrypt Key					1110	1111

#### 05 Schreibe folgende Binärzahlen in Polynomschreibweise!

1101	0110	0011	0100010
------	------	------	---------

#### 06 Führe die gegebenen Berechnungen im Polynomring $\mathbb{Z}_2[X]$ durch!

- $1010 \oplus 0111$
- $1010 \odot 0111$
- $01000100 \odot 10000001$

#### 07 Berechne Aufgabe 06b) im Polynomkörper $\mathbb{Z}_2[X]/p$ mit dem irreduziblen Polynom $p = x^4 + x + 1$ !