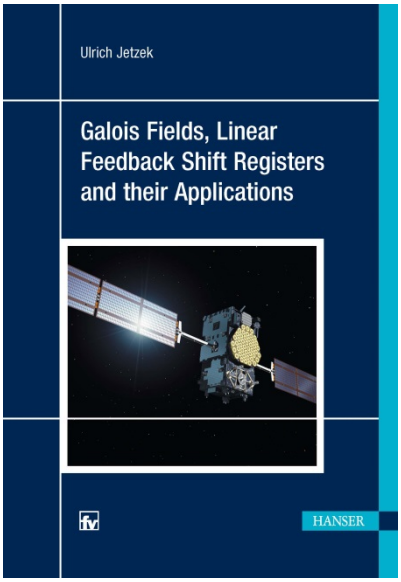
HANSER



Galois Fields, Linear Feedback Shift Registers and their Applications

With 85 illustrations as well as numerous tables, diagrams and examples

by Ulrich Jetzek

ISBN (Book): 978-3-446-45140-7
ISBN (E-Book): 978-3-446-45613-6

For further information and order see
http://www.hanser-fachbuch.de/978-3-446-45140-7

Acknowledgements

First of all, I would like to thank all the students I have been working with. All their questions, comments and remarks during my various lectures showed an intense interest in Galois Fields, Linear Feedback Shift Registers and their applications. This was a strong motivation moment to write this book.

Furthermore, I am grateful for the cooperation I had with the editor of Hanser Fachbuchverlag, Mrs. Mirja Werner. From the very beginning she had trust in my idea about this book and always supported me in writing this book. We had several fruitful discussions regarding structure, content and details of this book. I would also like to thank the editor, Mrs. Natalia Silakova, who accompanied me in the finalization phase of this book.

Many other people contributed to this book. Therefore, I would also like to thank all those people who are not mentioned explicitly in this section.

Finally, my thanks go to my family – my wife Carola and my children Julia, Franziska and Christian. They always showed lots of understanding while I was writing this book. And they had lots of patience when I (unfortunately) had no time to share and enjoy together with them.

Remark: *The author of this book has written and described the entire content of this book to his best knowledge. However, the author does not take any responsibility for any developments and/or products which may have been developed based on the content of this book. The book is intended as a textbook to get acquainted with Galois Fields, Linear Feedback Shift Registers and their applications. Therefore, the reader is required to make sure by himself whether any software or hardware implementation or any product derived from the content of this book works as wanted.*

Contents

1. Isolation:
   a) $\forall a, b \in F$ it holds that $a + b = c \in F$
   b) $\forall a, b \in F$ it holds that $a \cdot b = d \in F$
2. Associativity:
   a) $\forall a, b, c \in F$ it holds that $(a + b) + c = a + (b + c)$
   b) $\forall a, b, c \in F$ it holds that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Neutral element:
   a) Regarding addition, there exists an element $0 \in F$, so that $a + 0 = a \in F \, \forall a \in F$
   b) Regarding multiplication, there exists an element $1 \in F$, so that $a \cdot 1 = a \in F \, \forall a \in F$
4. Inverse element:
   a) For each element $a \in F$ there exists an additive inverse element $(-a)$, so that $a + (-a) = 0$ (neutral element of addition).
   b) For all elements $a \in F \backslash 0$ there exists a multiplicative inverse element $a^{-1} \in F$ so that $a \cdot a^{-1} = 1 \in F$.
5. Distributivity law: a field F obeys the distributivity law, i.e. $\forall a, b, c \in F$: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Examples

The set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$ each form a field. Both fields have an infinite number of elements.

2.3 Galois Fields

In the last section we defined the algebraic structures of groups, rings and fields. These definitions are valid for element sets with an infinite number as well as for those with a finite number. Fields based upon a finite number of elements are of particular interest when it comes to technical applications in cryptography, channel coding, mobile communication or navigation systems. Therefore, in the following sections we will focus on such finite fields, which are called Galois Fields.

For that purpose, we will now have a closer look at element sets of the form $\mathbb{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}$. If we apply modulo-m-addition and modulo-m-multiplication, such a set will always obey the isolation property, i.e. the result of any operation will always be within the given set of elements. In addition, it is obvious

that such sets contain the neutral element of addition, namely '0', as well as the neutral element of multiplication, namely '1'. Without proof it shall be stated that associativity, commutativity as well as the distributivity law are fulfilled.

However, one question remains: For which elements of $\mathbb{Z}_m$ does a multiplicative inverse exist? In order to answer this question, let us first consider the case in which m is a composite number, i.e. m is the product of at least two primes p_1 and p_2.

$$m = p_1 \cdot p_2 \tag{2.1}$$

Since the condition $2 \leq p_1, p_2 \leq m-1$ holds, p_1 and p_2 themselves are elements of $\mathbb{Z}_m$. Suppose we want to check if p_1 has a multiplicative inverse w.r.t. modulus m. According to the definition of the multiplicative inverse, the following condition must hold:

$$p_1 \cdot p_1^{-1} \bmod m \equiv 1 \tag{2.2}$$

Looking for the multiplicative inverse of p_1 means looking for some element $p_1^{-1} \in \mathbb{Z}_m$ so that the Equation (2.2) is fulfilled. Therefore, if we check the multiples of p_1, i.e. $p_1, 2p_1, 3p_1, \ldots$, these will be greater than p_1 itself as long as the product is smaller than m. If we multiply p_1 by p_2 or calculate p_1^2, the result *modular m* is identical to 0. However, if we multiply p_1 by $(p_2 + 1)$ or calculate $p_1 \cdot (p_1 + 1)$ and assume that $p_1 = 2$ or $p_2 = 2$, i.e. the smallest prime, then the product *modular m* will be at least 2. Hence, no multiplicative inverse exists in this case. Therefore, it is impossible to build a field on any composite integer m. A finite set of elements $\mathbb{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}$, where m is composite, will *always* form a ring together with the two operations 'addition' and 'multiplication'.

An element a has a multiplicative inverse a^{-1} mod m if and only if the greatest common divisor (gcd) of m and a is equal to one, i.e. if m and a are said to be relatively prime, $\gcd(m, a) = 1$.

Let us look at an example.

Example: Suppose $m = 6$. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

The multiplication table for this $\mathbb{Z}_6$ is given by:

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

With respect to the given example, it is obvious that for $m = 6 = 2 \cdot 3$, the elements 2 and 3 are not relatively prime with respect to $m = 6$ and therefore do NOT have a multiplicative inverse. (Neither does the element 4 have a multiplicative inverse, since the gcd $(m = 6, 4) = 2$ is also greater than one.

2.3.1 Prime Fields

In order to better understand the structure and handling of prime fields, we need to answer a few questions. For which primes does a finite field exist? What is a 'generator' of a field? The answers are provided in the following sections.

2.3.1.1 Existence of Prime Fields

An essential message about the existence of Prime Fields is stated within the following theorem, namely, that we can generate a Prime Field over any prime integer p.

Theorem: Existence of Prime Fields

The set of elements $GF(p) = \{0, 1, 2, 3, \ldots, p-1\}$, where p is a prime, forms a field.

$GF(p)$ is named Galois Field or Prime Field with characteristic p.

Hence, the smallest field that exists is $GF(2) = \{0, 1\}$.

Table 2.1 Addition and Multiplication Table of $GF(2)$

Addition mod 2				Multiplication mod 2		
+	0	1		·	0	1
0	0	1		0	0	0
1	1	0		1	0	1

If we want to implement modular-2-arithmetic in a digital circuit, it is interesting to see that modular-2-addition directly corresponds to an exclusive-OR, XOR-operation, while modular-2-multiplication directly corresponds to an AND-operation.

Let us look at another example: $GF(7) = \{0, 1, 2, 3, 4, 5, 6\}$, where $p = 7$ is a prime

Example:

$GF(7) = \{0,1,2,3,4,5,6\}$, where $p = 7$ is a prime

Table 2.2 Addition Table of $GF(7)$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

One aspect which can be directly derived from Table 2.2 is that the additive inverse $(-a)$ of any element a is not a negative integer, but rather the element which adds up to zero modulus 7. If $a = 2$, then $(-a) = -2 \bmod 7 \equiv 5$, since $2 + 5 \bmod 7 \equiv 0$.

Table 2.3 Multiplication Table of $GF(7)$

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Since each row of the multiplication table contains a '1' as a result, each element of the given set has a multiplicative inverse. Choose an element a by selecting a specific row, then find the '1'-entry of multiplication. The corresponding column contains the multiplicative inverse $a^{-1} \bmod 7$.

For larger values of primes p it may, of course, not be so convenient to write down the multiplication table. Therefore, in general, the multiplicative inverse $a^{-1} \bmod p$ can be calculated by means of the so-called Extended Euclidean Algorithm (EEA). For a detailed description of the EEA the interested reader is referred to e.g. [1]

2.3.1.2 Generators of Prime Fields

Within this section we will see that there exists a second method to determine the multiplicative inverse of any element a of $GF(p)$. The idea of this method is to make use of a generator or a primitive element of $GF(p)$.

Suppose we calculate the different powers of an element α of the prime field $GF(p)$:

$$y = \alpha^i \bmod p \text{ with } i = 1,2,3,\ldots,p-1 \tag{2.3}$$

Since multiplication is done with modulus p, we can be sure that y will be an integer of $GF(p)$ for each i.

Definition: Generator or primitive element of $GF(p)$

An element α for which *all* powers $\alpha^i \bmod p$ with $i = 1,2,3,\ldots,p-1$ yield *all* elements of $GF(p)$ except 0, is called a generator or a primitive element of $GF(p)$.

According to [2] the following statement applies.

Theorem: Existence of generators for Prime Fields $GF(p)$

Every prime field or Galois Field $GF(p) = \{0,1,2,3,\ldots,p-1\}$ contains at least one generator or primitive element.

At the same time, it needs to be noted that not all elements of $GF(p)$ are generators of the field.

Since $a^0 \bmod p \equiv 1$, there must exist an integer $i_0 \neq 0$, so that $a^{i_0} \bmod p \equiv 1$. The smallest positive integer i_0 for which the given condition is fulfilled is called the order of the element a, ord(a). Therefore, if and only if an element a has the order $p-1$, this element is a generator of $GF(p)$.

Table 2.4 shows the powers of all elements of $GF(17)$. The first column shows the increasing exponent while the first row lists all elements of $GF(17)$. In a specific column the various powers of the element a shown in the top row, i.e. $a^i \bmod 17$, are presented in the table. The bottom row shows the order for each element a.

One important observation is that the element orders are different from the elements of $GF(17)$. Another point to note is that in total 8 elements $(3,5,6,7,10,11,12,14)$ with the element order equal to 16 exist. Each of these elements is a generator of $GF(17)$.

Example: Galois Field $GF(17)$

Table 2.4 Element orders of $GF(17)$

$a =$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
i	$a^i \bmod 17$														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	4	9	16	8	2	15	13	13	15	2	8	16	9	4	**1**
3	8	10	13	6	12	3	2	15	14	5	11	4	7	9	
4	16	13	**1**	13	4	4	16	16	4	4	13	**1**	13	16	
5	15	5		14	7	11	9	8	6	10	3		12	2	
6	13	15		2	8	9	4	4	9	8	2		15	13	
7	9	11		10	14	12	15	2	5	3	7		6	8	
8	**1**	16		16	16	16	**1**	**1**	16	16	16		16	**1**	
9		14		12	11	10			7	6	5		3		
10		8		9	15	2			2	15	9		8		
11		7		11	5	14			3	12	6		10		
12		4		4	13	13			13	13	4		4		
13		12		3	10	6			11	7	14		5		
14		2		15	9	8			8	9	15		2		
15		6		7	3	5			12	14	10		11		
16		**1**		**1**	**1**	**1**			**1**	**1**	**1**		**1**		
ord(a) =	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

Therefore, if we identify a generator α of $GF(p)$, we may create a lookup table containing all powers of α, i.e. all elements of $GF(p)$.

2.3.1.3 Multiplicative Inverses in Prime Fields

In order to find the multiplicative inverse for a specific element a we can make use of the power laws of modulus p. For any multiplicative inverse the following condition must hold:

$$a \cdot a^{-1} \bmod p \equiv 1 \equiv \alpha^i \cdot \alpha^j \bmod p \equiv 1 \tag{2.4}$$

Since α is a generator, $\alpha^{p-1} \bmod p \equiv 1$. Therefore, if we want to identify the multiplicative inverse for any element $a \equiv \alpha^i \bmod p$, the exponent of the mulitplicative inverse $a^{-1} \bmod p \equiv \alpha^j \bmod p$ can easily be calculated by using the condition

that $i + j \equiv p - 1$ and therefore

$$j = (p - 1) - i \tag{2.5}$$

Example

Suppose we want to determine the multiplicative inverse of $a = 13$ in $GF(17)$.

Case 1: As a generator we will use the element $\alpha = 3$.

$a = 13 \equiv 3^4 \bmod 17$

According to Equation (2.5) the generator exponent j of the multiplicative inverse is equal to: $j = (17 - 1) - 4 = 12$. Therefore, the multiplicative inverse can be found in the lookup table as:

$\alpha^{12} \bmod 17 \equiv 3^{12} \bmod 17 \equiv 4$

Case 2: As a generator we will use the element $\alpha = 10$

$a = 13 \equiv 10^{12} \bmod 17$

According to Equation (2.5) the generator exponent j of the multiplicative inverse is equal to: $j = (17 - 1) - 12 = 4$. Therefore, the multiplicative inverse can be found in the lookup table as:

$\alpha^4 \bmod 17 \equiv 10^4 \bmod 17 \equiv 4$

Therefore, if it is possible to generate a lookup table, as shown for the powers of all elements of $GF(17)$ in Table 2.4, it is easy to find the multiplicative inverse for any element a of $GF(p)$.

It should, however, be noted that, for example in cryptographic applications, prime fields with a large characteristic p are needed. "Large" in this case means primes consisting of 300 or more decimals. In such cases it will, of course, not be possible to create a lookup table. However, a different way of finding the multiplicative inverse for an element a in $GF(p)$ is to use the Extended Euclidean Algorithm. For a detailed description regarding this algorithm, the reader is referred to [1].

2.3.1.4 Cyclic Structure of Prime Fields

It is important to note that with respect to a generator α of a Prime Field $GF(p)$, a cyclic structure is created in the following way:

$$
\begin{aligned}
\alpha^0 &\equiv 1 \bmod p \\
\alpha^1 &\equiv \alpha \cdot \alpha^0 \bmod p \\
\alpha^2 &\equiv \alpha \cdot \alpha^1 \bmod p \\
\alpha^3 &\equiv \alpha \cdot \alpha^2 \bmod p \\
\alpha^4 &\equiv \alpha \cdot \alpha^3 \bmod p \\
&\vdots \\
\alpha^{p-2} &\equiv \alpha \cdot \alpha^{p-3} \bmod p \\
\alpha^{p-1} &\equiv \alpha \cdot \alpha^{p-2} \bmod p \equiv 1 \\
\alpha^{p} &\equiv \alpha \cdot \alpha^{p-1} \bmod p \equiv \alpha \\
\alpha^{p+1} &\equiv \alpha \cdot \alpha^{p} \bmod p \equiv \alpha^2
\end{aligned}
$$

Figure 2.3 Exponents of the primitive element α

A graphical representation of this cyclic structure is shown in Figure 2.4 for the Prime Field $GF(17)$ using the generator $\alpha = 3$. Within the figure each arrow denotes the following: take the element at the beginning of the arrow, multiply this element with the generator modulus p (in the given example: $\cdot 3 \bmod 17$.). The result yields the end of the arrow.

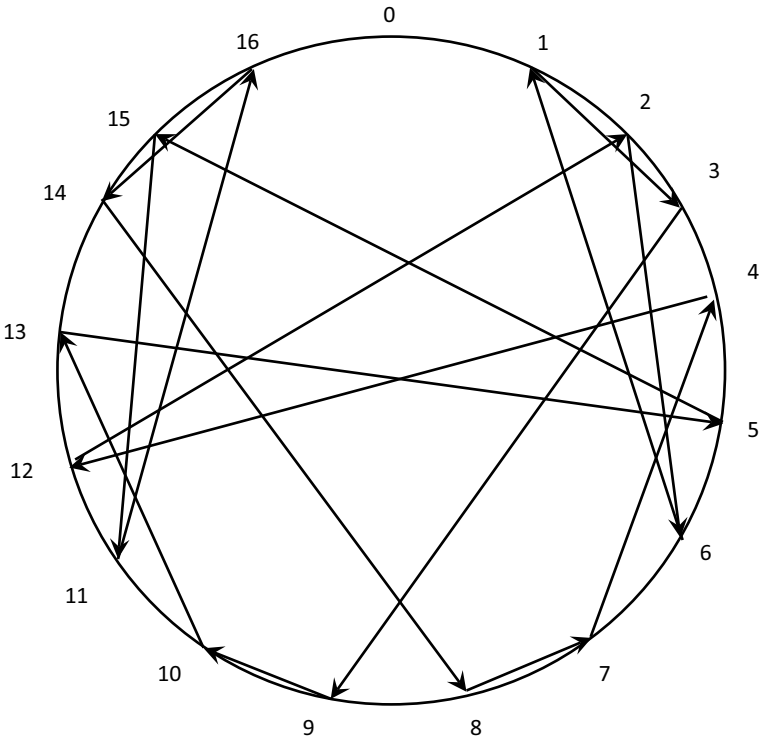


Figure 2.4 Cyclic structure of Prime Field $GF(17)$, generator: $\alpha = 3$

One important property of this cyclic structure is the fact that the element '0' is *never* part of the described cyclic structure.

2.3.2 Extension Fields

In Section 2.3.1 we introduced the smallest Prime Field, namely $GF(2)$ containing only the elements {0,1}. Although digital systems are based on the mentioned element set {0,1}, we usually work with larger numbers represented in binary format. Therefore, two questions arise. Is it advantageous to work with Prime Fields in technical systems? Which disadvantages do we need to take into account?

Let us have a look at a simple example. Suppose we work with the Prime Field $GF(67)$. Since p=67 is a prime number, the set of elements $\{0,1,2,3,\ldots,65,66\}$ definitely forms a field, i.e. we can perform addition and multiplication within the field. While the modular operation is performed, the field is closed, i.e. the result of any addition or multiplication will result in an element of the Prime Field $GF(67)$. Associativity and commutativity are fulfilled, and finally each element a contains an additive inverse $-a \equiv (-a+p) \bmod p$ and a multiplicative inverse $a^{-1} \bmod p$.

However, if we represent each element of this prime field in binary format, e.g. in order to implement our Galois Fields operations in software or hardware, we need to note the following (see Figure 2.5):

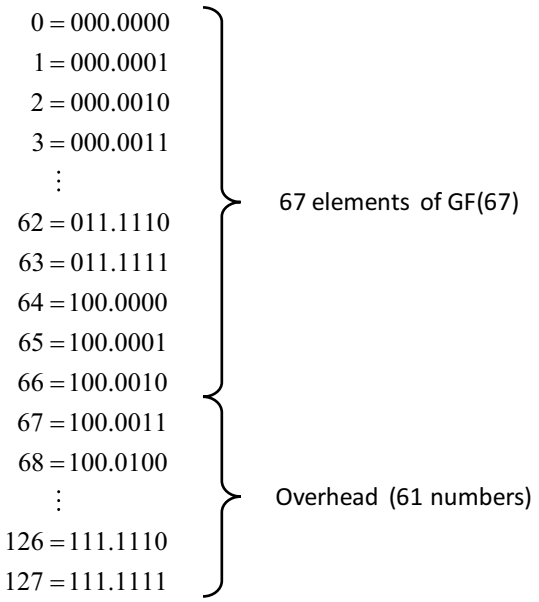


Figure 2.5 7-Bit representation needed for $GF(67)$

Since $p = 67$ is larger than $64 = 2^6$, we need 7 bits to represent all elements of $GF(67)$. However, in the case of 7-bit representation it is possible to handle 128

different numbers, hence 61 numbers are not used, and we need to accept a large overhead.

If we look at technical systems, in particular computer systems, data is most often arranged in bytes – whereas 8 bits form a single byte – or in multiple bytes, e.g. 16 or 32 bits. Therefore, the question is whether it is possible to generate fields which do not have a prime number of elements, but rather a power of 2 elements, i.e. 2^m elements.

2.3.2.1 Existence of Extension Fields

It is possible to generate such fields, these are called extension fields and the following theorem holds.

Theorem: Existence of Extension Fields

For any prime p and any positive integer m it is possible to generate a Galois Field $GF(p^m)$. We call this field an Extension Field with a characteristic p and an extension m. The Extension Field $GF(p^m)$ contains $n = p^m$ elements.

It should be noted that the above theorem is the generalization of the corresponding theorem stating the existence of Prime Fields (compare Section 2.3.1).

In Section 2.3.1 we saw that each element of a prime field $GF(p)$ is a single integer within the range $0, 1, 2, \ldots, p-1$. Since we extended the Pime Field $GF(p)$ by the exponent m, each element of an extension field is an m-elementary vector of the following format:

$$(a_{m-1}a_{m-2}a_{m-3}\ldots a_1 a_0) \quad \text{with} \quad a_i \in 0, 1, 2, \ldots, p-1 \quad \text{for} \quad i = 0, 1, 2, \ldots, m-1$$

A second interpretation of the field elements is to consider each element to be a polynomial of degree $m-1$.

$$\left(a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + a_{m-3}x^{m-3} + \cdots + a_1 x^1 + a_0 x^0\right) \quad \text{with} \quad a_i \in 0, 1, 2, \ldots, p-1 \quad \text{for} \quad i = 0, 1, 2, \ldots, m-1$$

Although the above theorem states that we may generate an extension field with the help of *any* prime p, in the following sections we will focus on extension fields with the characteristic $p = 2$, i.e. we will particularly look at the extension fields of the form $GF(2^m)$. The reason for this restriction is simple, namely that most applications of extension fields are implemented in digital systems and therefore we need to work with binary vectors of various lengths.

In the previous paragraph, we introduced two different representations of extension field elements.

It is important to see that even a single integer like '0' or '1' needs to be seen as a polynomial of degree $m-1$ if it is an element of an extension field. The same applies to terms like x or x^2.

Example

Let us have a look at the elements of the Extension Field $GF(2^4)$.

Vector representation ≡ Polynomial representation

$$
\begin{aligned}
0000 &\equiv 0x^3 + 0x^2 + 0x^1 + 0x^0 \\
0001 &\equiv 0x^3 + 0x^2 + 0x^1 + 1x^0 \\
0010 &\equiv 0x^3 + 0x^2 + 1x^1 + 0x^0 \\
0011 &\equiv 0x^3 + 0x^2 + 1x^1 + 1x^0 \\
0100 &\equiv 0x^3 + 1x^2 + 0x^1 + 0x^0 \\
&\vdots \\
1111 &\equiv 1x^3 + 1x^2 + 1x^1 + 1x^0
\end{aligned}
$$

We can see that in total $2^4 = 16$ elements exist in $GF(2^4)$.

2.3.2.2 Irreducible Polynomials

In order to work with the extension field elements, we need to understand how modular operations are performed within extension fields. In Section 2.3.1 we demonstrated that addition and multiplication in a prime field $GF(p)$ is done with *modulus p*, where p is, of course, a prime. Since the field elements of extension fields are polynomials, multiplication within an extension field $GF(p^m)$ is done modularly with a certain *polynomial* $p(x)$.

The largest field element of a prime field $GF(p)$ always is $p-1$, and the applied modulus must be larger than the greatest field element. Hence, we perform additions and multiplications in $GF(p)$ with modulus p. The analog regarding extension fields is that all elements of the extension field $GF(p^m)$ are polynomials of degree $m-1$. Hence the polynomial used for modular operations must be of a higher degree, namely of degree m.

The second aspect concerns the properties of the modulus. In a prime field $GF(p)$ the modulus p is a prime and is therefore only divisible by itself and by one. Let us recall why it is of significance that p is prime. Within a prime field it is possible to perform addition and multiplication and also to perform the *inverse functions*,

i.e. subtraction and *inverse multiplication*. Especially the latter operation requires that all elements of the prime field except '0' have a multiplicative inverse. This is the case *only* if all elements (except 0) are relatively prime w.r.t. p, i.e. the greatest common divisor for p and *any* prime field element a must be equal to one, i.e. the $\gcd(p, a) = 1$. The analog w.r.t. extension fields means that we need a modular polynomial $p(x)$, for which the following condition must hold.

If and only if the polynomial $p(x)$ is relatively prime in regard to all extension field elements $a(x)$ except the 0-polynomial, then for any extension field element $a(x)$ except the 0-polynomial a multiplicative inverse will exist.

Definition: Irreducible polynomial $i(x)$

A polynomial $i(x)$ of degree m is said to be irreducible if it *cannot* be expressed as the product of at least two polynomials of lower degree $k < m$.

Definition: Reducible polynomial $r(x)$

A polynomial $r(x)$ of degree m is said to reducible if it *can* be expressed as the product of at least two polynomials of lower degree $k < m$.

In order to continue with our analogies, we can state that an irreducible polynomial $i(x)$ in the world of extension fields is the analog of a prime in the world of prime fields, and that a reducible polynomial $r(x)$ in the world of extension fields is the analog of a composite number in the world of prime fields.

Let us have a look at an example for the extension field $GF(2^4)$.

Example

$$r(x) = x^4 + x^2 + x = x \cdot (x^3 + x + 1) \quad \Rightarrow r(x) \text{ is reducible}$$
$$p(x) = x^4 + x^3 + x^2 + x + 1 \quad \Rightarrow p(x) \text{ is irreducible}$$

For $r(x)$ it is obvious that a polynomial of degree one, namely x, is contained in each summand of the polynomial $r(x)$. Therefore x can be extracted, and we can rewrite $r(x)$ as a product of two polynomials of lower degree. It is therefore obvious that $r(x)$ is reducible.

Without proof, we can state that the polynomial $p(x)$ in the above example is irreducible.

If we look at $r(x)$ in the above example, we can directly conclude that it is a necessary condition that $p(x)$ does not contain any zeroes within $GF(p)$. This means that if we calculate the value of $p(x)$ for all possible values $0, 1, 2, \ldots, p-1$ and take

the result modulus p, the result will never be equal to zero. The question, however, remains if this condition is not only necessary, but also sufficient for a polynomial to be irreducible. Let us have a look at an example.

Example

$r(x) = x^4 + x^2 + 1$

For:

$x = 0$: $r(0) = 0^4 + 0^2 + 1 = 1 \bmod 2 \equiv 1$

$x = 1$: $r(1) = 1^4 + 1^2 + 1 = 3 \bmod 2 \equiv 1$

We have thus proven that $r(x)$ does not contain any zeroes within $GF(2)$. Hence, we might assume $r(x)$ to be irreducible. However, we can write $r(x)$ as:

$$\begin{aligned} r(x) &= (x^2 + x + 1) \cdot (x^2 + x + 1) \\ &= x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 \\ &= x^4 + 2x^3 + 3x^2 + 2x + 1 \\ &\equiv x^4 + x^2 + 1 \end{aligned}$$

The above equation shows the result if we square the term $(x^2 + x + 1)$. The second line shows all summands of the product. As we stated at the beginning of Section 2.3.2.1, the elements of an extension field, in our case $GF(2^4)$, are polynomials with coefficients of $GF(p)$, in our case coefficients of $GF(2) = \{0, 1\}$. Hence, for all resulting summands of our products, the coefficients are calculated with the help of modulus p, in our case, modulus 2. Therefore, $2x^3 \bmod 2 \equiv 0$, and $2x \bmod 2 \equiv 0$. And finally, $3x^2 \bmod 2 \equiv 1x^2$.

The above example proves that the condition that $p(x)$ does not contain any zeroes within $GF(p)$ is NOT sufficient to be sure that $p(x)$ is irreducible.

To summarize this section, we need to state the following points.

For an irreducible polynomial $i(x)$ it is a necessary, but not a sufficient condition that it does not contain any zeroes within $GF(p)$, i.e. it cannot be expressed as the product of at least two polynomials of lower degree.

An irreducible polynomial $i(x)$ of degree m over $GF(p)$ spans an extension field $GF(p^m)$ with p^m elements, where each element is a polynomial of degree $m - 1$.

Index