Research of Irreducible Normal Polynomials Special Type over a Field of Characteristic 2

Sarsengali Abdymanapov, Umut Turusbekova, *Member, IAENG*, Alua Turginbayeva and Serik Altynbek

Abstract — **Such sections of algebra as the theory of finite fields and the theory of polynomials over finite fields have increasingly influence on the construction of various systems for protecting information, encoding and decoding information. In the last two decades, polynomials, especially irreducible polynomials, have played a significant role in computer cryptography. Using the properties of irreducible polynomials maximizes the efficient computer implementation of arithmetic in finite fields, which is of particular importance for cryptography and coding theory.**

The present paper is devoted to the study of irreducible polynomials of a special type. Namely, explicit root polynomial formulas for third-degree cyclic polynomials over a field of characteristic 2 are obtained. A review of known results on irreducible normal polynomials and sets of their root polynomials over arbitrary fields is also given. In addition, the problem of finding irreducible polynomials is considered. The results of the work can be used in cryptographic applications and coding theory.

Index Terms — **Irreducible polynomial, Normal polynomial, Root polynomial, Finite field.**

I. Introduction

The theory of finite fields was built in the works of Fermat, Euler, Legendre, Gauss, Galois, Dixon and other outstanding scientists, and until the last quarter of the 20th century developed as a field of pure mathematics, but due to the needs of coding and cryptography, the applied aspects of the theory are now actively developing. Many works and special books are devoted to the effective implementation of arithmetic in finite fields [1]-[3].

The theory of polynomials of degree *n* in one variable, irreducible over finite fields F_p, present of significant interest both for studying the algebraic structure of finite fields $F_p{}^n$, and for numerous applications in the modern theory of information transfer. Irreducible polynomials whose roots form the basis for representing elements of finite fields are analogous to primes. They have found their application in various fields of mathematics, information technology and information security. There is no specific algorithm for finding such polynomials, so their construction is performed by selection, i.e. probabilistic algorithms, which requires time and volumetric calculations. The coefficients of polynomials, as elements of finite fields of characteristic two, can be interpreted in multibit sequences for transmission over modern communication channels.

Therefore, the use of irreducible polynomials of large degrees defining these fields becomes an important problem.

The relevance of the study of irreducible polynomials over simple and extended Galois fields is due to their diverse application in various fields of science and technology. A fundamental review of results on finite field theory, including the theory of irreducible polynomials, is given in [4]-[9]. However, despite the successes achieved in the theory of irreducible polynomials, there are a number of important problems that still cannot be resolved. One of them is the problem of constructing irreducible polynomials of a given degree in explicit form, as well as determining the root polynomials of these polynomials.

The main purpose of this research is to study, construct and use the properties of irreducible polynomials over finite fields. The paper gives an explicit form of cyclic polynomials of the third degree over a field *F* of characteristic 2 that admit cyclic extensions of degree 3 and their root polynomials are described. In addition, the problem of searching for irreducible polynomials was considered in the current work.

II. Preliminaries

Here are the basic definitions and information considered [1], [2].

Let *F* be a field and $\overline{F}$ a algebraic closure of a field *F*. Recall that an *irreducible* polynomial is a polynomial that does not decompose into lower degree factors. A unitary polynomial (a polynomial with a leading coefficient equal to 1) $f(x)$ from $F[x]$ is called normal over *F* if all its roots are rationally expressed over *F* through any root of the polynomial $f(x)$.

Let $f(x)$ be a normal polynomial over *F*, that is,

$$f(x) = (x-\xi_1)(x-\xi_2)...(x-\xi_n),$$

where $\xi_i \in \overline{F}$ and $\xi_i = g_i(x)$ for all *i* = 1, 2, ..., *n*, where $g_i(x)$ are polynomials from $F[x]$ of degree less than *n*.

The polynomials $g_i(x)$ are uniquely determined by the polynomial $f(x)$. If it is irreducible in $F[x]$, then they are called *root polynomials* for $f(x)$.

Manuscript received December 25, 2019; revised July 7, 2020.

Sarsengali Abdymanapov is Academician of the International Academy of Higher Education, Kazakh University of Economics, Finance and International Trade.

Umut Turusbekova and Serik Altynbek are with Department of Information Systems and Technologies, Kazakh University of Economics, Finance and International Trade, Nur-Sultan, Kazakhstan. *E-mail: umut.t@mail.ru (Corresponding author).

Alua Turginbayeva is Doctoral Student of the L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan.

Note that $g_1(x)=x$, we form the set of root polynomials $M=\{g_1(x)=x, g_2,..., g_n\}$. Let a degree *f*(*x*) equal to *n* be greater than two and *F* be a formally real field. In this case, H. Kleiman [10] proved the following theorems.

Theorem 1. The normal polynomial $f = x^n + \sum_{j=0}^{n-1} a_{(n-1)-j} x^{(n-1)-j}$ with coefficients in a formally real field *F* is uniquely determined by the set *S*={*M*, a_{n-2}}, where *M* is the set of root polynomials for *f* (*x*). In addition, the set *M* contains at least one nonlinear polynomial, provided that *n*> 2. If the set *M* contains a root polynomial of degree two, then the normal polynomial *f*(*x*) is uniquely determined by the set *M*.

Let $\Phi_n(x)$ be a circular polynomial of order *n*, *n*>6, therefore, the degree of the polynomial $\Phi_n(x)$ is greater than or equal to 4.

Theorem 2. Each polynomial in the class of circular polynomials of degree ≥ 4 is uniquely determined by its root polynomials.

Theorem 3. Let *F* be a field of characteristic 0. Let $f(x) \in F(x)$ - an irreducible polynomial over *F* and all roots of the polynomial *f*(*x*) are linear functions of a single root α. Then the decomposition field of the polynomial *f*(*x*) is a cyclic extension of the field *F* and the field *F* contains a primitive root of degree *n* of unity.

H. Muthsam proved the following assertion [11].

Theorem 4. Let *F* be a formally real field, *f*(*x*) - an irreducible normal polynomial of degree $n>1$ from *F*[*x*], whose roots are linearly independent over *F*. Then the set *M* of root polynomials for *f*(*x*) uniquely determines *f*(*x*).

K. Girstmair [12] investigated normal polynomials of the third degree (that is, cyclic polynomials) over fields *F* of a characteristic unequal 2 and 3.

Let $f(t)=t^3+a_1t^2+a_2t+a_3$ is a cyclic polynomial from $F(x)$ with discriminant *D*(*f*) and root polynomials:

$$z_1=t,\ z_2=w_{22}t^2+w_{21}t+w_{20},\ z_3=w_{32}t^2+w_{31}t+w_{30},$$

where $z_2, z_3 \in F[x]$, $w_{22} \neq 0$, $w_{32} \neq 0$. Then the following theorem is valid [10].

Theorem 5. Cyclic cubic polynomial $f(t) \in F[t]$ uniquely determined by its root polynomials.

If for simplicity we denote a non-trivial root polynomial z_2 in the form of

$$z_2 = w_2t^2+w_1t+w_0,$$

then the coefficients of the cyclic polynomial $f(t)=t^3+a_1t^2+a_2t+a_3$ can be find from ratios:

$$a_1=-(w_{20}+w_{30}),\ a_2=\frac{a_1^2w_2+a_1(1-w_1)+3w_0}{2w_2},$$

$$a_3=a_1a_2-\frac{a_1^3}{3}+\frac{a_1^2w_1-a_2(1+2w_1)-a_1w_0}{3w_2}.$$

With these conditions, the theorem [10] is valid.

Theorem 6. Let *F* be a field of characteristic that is unequal to 2 and 3, and not containing the roots of the third degree of unity. Then square polynomial $z=w_2t^2+w_1t+w_0$, where $w_2 \neq 0$, $w_2, w_1, w_0 \in F$, is the root polynomial of some cyclic cubic polynomial *f* (*x*) only if the element

$$s(z)=(w_1-1)^2-4w_0w_2-8$$

is a square in the field *F*: $s(z)=r^2$, $r \in F$. In this case, there are two polynomial $f_i(t)=t^3+a_{i1}t^2+a_{i2}t+a_{i3}$, $i=1,2$ with the root polynomial *z*:

$$a_{11}=\frac{3w_1+1+r}{2w_2},\ a_{21}=\frac{3w_1+1-r}{2w_2}$$

and the coefficients a_{i2}, a_{i3}, $i=1,2$ are determined using a_{11}, a_{21} and *z* from relations of the theorem 5.

III. ARITHMETIC OF FINITE FIELDS

Such sections of algebra as the theory of finite fields and the theory of polynomials over finite fields have increasingly influence the construction of various systems for protecting information, encoding and decoding information. In particular, there appeared algorithms for cyclic redundant codes [13], which use polynomials over a fields F_p.

Because the finite field is a set with a finite number of elements, the operations of addition, subtraction, multiplication and division can be performed in accordance with the axioms of the field [1]. Since the finite fields are closed with respect to the above operations, i.e. for any two elements of the field $a, b \in F_p$, then when any of the operations are performed, the result is an element belonging to this field $c \in F_p$. It should be borne in mind that all calculations in finite fields are made modulo *p*, which is a characteristic of a finite field and is a prime number.

The simplest example of a finite field is the ring of residue classes *Z*/(*p*) modulo *p* a prime number, which can be identified with a Galois field $F_p = GF(p)$ of order *p* [1]. According to the theorem on the existence and uniqueness of finite fields, for every prime number *p* and natural number *n*, there exists a finite field of p^n elements. To construct a field F_{p^n}, it is necessary to find a polynomial *P*(*x*) of degree *n* irreducible over a field F_p. Such a field is represented by polynomials over F_p a degree not higher *n*−1. A peculiarity of irreducible polynomials is that, being irreducible in one field, a polynomial turns out to be reducible in another field, which has found application in the theory of coding and information protection systems.

The search for irreducible polynomials is a difficult-to compute problem, especially over fields of large dimension. The procedure for finding irreducible polynomials requires efficient algorithms and large computational resources, as in the case of finding prime numbers [14]. At the moment, there are no effective algorithms for searching for irreducible polynomials, there are only criteria for irreducibility and verification methods for irreducibility. The search is carried out by examining the multibodies and checking each individually for irreducibility. To check the polynomial *P*(*x*) of degree *n* ≥ 2 on irreducibility over a field of characteristic there exists the following algorithm [15]:

1) The initial value of a polynomial is initialized $G_0(x)=x$.

2) The following value is calculated $G_1(x)=G_0(x)^p \bmod S(x)$.

3) The greatest common divisor (GCD) between $S(x)$ and ($G_1(x)-x$) is calculated. If the GCD is not equal to one, then this polynomial is reducible. Otherwise, the next value is calculated according to the recurrence formula $G_i(x)=G_{i-1}(x)^p \bmod S(x)$, where $i=\overline{1,\ \lfloor n/2 \rfloor}$, $\lfloor\ \rfloor$ is the operation of taking the whole part of the number.

4) If the GCD $S(x)$ and each one ($G_i(x)-x$) equal to one, then the polynomial $S(x)$ is irreducible.

The disadvantage of such an algorithm is the low computation speed for sufficiently large values, since at each step the operation of raising and finding the GCD is performed.

For computations in finite fields, polynomial arithmetic is used. The addition in the field F_{p^n} corresponds to the usual addition of polynomials modulo *p*. Multiplication is performed in two steps - first as a simple multiplication of polynomials, and then the remainder from division into an irreducible polynomial is calculated, with which the field F_{p^n} is constructed. For example, fields of the same dimension can be constructed in different ways, depending on the choice of an irreducible polynomial. They are of the same order and are isomorphic to each other. This follows from the fact that for the characteristic *p* field there are several irreducible polynomials of degree *n*. Examples of irreducible polynomials for a field F_2 are given in TABLE I [16].

TABLE I
Irreducible polynomials over a field of characteristic 2

Power	Irreducible polynomials
2	x^2+x+1
3	$x^3+x^2+1,\ x^3+x+1$
4	$x^4+x^3+x^2+x+1,\ \ x^4+x^3+1,\ x^4+x+1$
5	$x^5+x^2+1,\ x^5+x^3+x^2+x+1,$ $x^5+x^4+x^3+x+1,\ x^5+x^4+x^3+x^2+1,$ $x^5+x^4+x^2+x+1$

Elements of the normal basis $\{\alpha,\ \alpha^2\ \alpha^4,\ ...,\ \alpha^{2n-1}\}$ are the roots of the same polynomial of degree *n* irreducible over F_2, this is due to the fact that the squaring operation is an automorphism of the field. Therefore, we can pose the problem of finding polynomials, whose roots form the basis for solving specific problems in finite fields, in particular, finding the roots of quadratic equations.

Let's consider the solution of the equation $x^2+x=z$, where *z* is the root of the irreducible polynomial *f*, i.e. *f* (*z*)=0 of degree *m*. The solution of this equation gives the following *operation P*:

$$Pf(t)=G(t)=f(t^2+t).$$

If *x* is the root of the irreducible polynomial *G*(*x*) = 0 lies in the field $F_2{}^m$, then the polynomial obtained from the polynomial *f* by the operation *P* is reduced: *G*(*t*) = *p*(*t*) *q* (*t*), deg *p*=deg *q*=*m*, where the element *x* is the root of one of two irreducible polynomials of the same degree *m* connected by the relation *p*(*t* +1)=*q*(*t*); *q*(*t* +1)=*p*(*t*) and *tr*(*f*) = 0.

If *x* is the root of the irreducible polynomial *G*(*x*)=0 obtained from *f* by the operation *P* lies in the extended field $F_2{}^{2m}$ and *tr*(*f*)=1, then the polynomial *G* of degree 2*m* is irreducible and periodic with a period equal to unit, i.e. *G*(*t*+1)=*G*(*t*).

The phased application of operation *P* allows us to generate all irreducible polynomials of degree 2^n, which can be represented as a complete binary tree (Fig 1.). Let's denote with bold arrows the application of operation *P*, ordinary arrows factorize the reducible polynomial, reducible polynomials with the empty dots, shaded – irreducible.

Through a polyquadratic extension, it is possible not only to calculate the characteristic polynomial of an element from an expanded field, but also from an expandable one, i.e. tree movement is possible both up and down. In order to "go down" along the tree, it is necessary to apply operation *P*, and to "go up" along the tree up, perform the inverse operation P^{-1}.

Operation *P* allows us to generate all irreducible polynomials of degree 2^n.

IV. Construction of root polynomials for some cubic cyclic polynomial over a field F of characteristic 2

Let *F* be a field and $f(x)=x^3+ax+b$ be the irreducible polynomial over *F* with the cyclic Galois group C_3, that is, any two roots of this polynomial are rationally expressed over the field *F* through the third remaining root. Let α,β,γ be the roots of *f*(*x*), then:

$$\beta=s_2(\alpha)=A\alpha^2+B\alpha+C,$$
$$\gamma=s_3(\alpha)=A_1\alpha^2+B_1\alpha+C_1 \qquad (1)$$

where $A,B,C,A_1,B_1,C_1\in F$.

Theorem. Let *F* be a field of the characteristic 2 that admits cyclic extensions of degree 3. Then cyclic polynomials of the third degree have the form

$$f(x)=x^3+\frac{B^2+B+1}{A^2}x+\frac{B^2+B+1}{A^3} \qquad (1')$$

or

$$f(x)=x^3+\frac{B^2+B+1}{A^2}x+\frac{B^2+B}{A^3}=$$
$$=x^3+(B^2+B+1)C^2x+(B^2+B)C^3 \qquad (1'')$$

and for polynomials of the form (1'), the root polynomials are described by equalities

$$s_2(x)=Ax^2+Bx,\ s_3(x)=Ax^2+(B+1)x,$$

and for polynomials of the form (1"), the root polynomials are determined by equalities

$$s_2(x)=\frac{1}{C}x^2+Bx+C,\ s_3(x)=\frac{1}{C}x^2+(B+1)x+C.$$

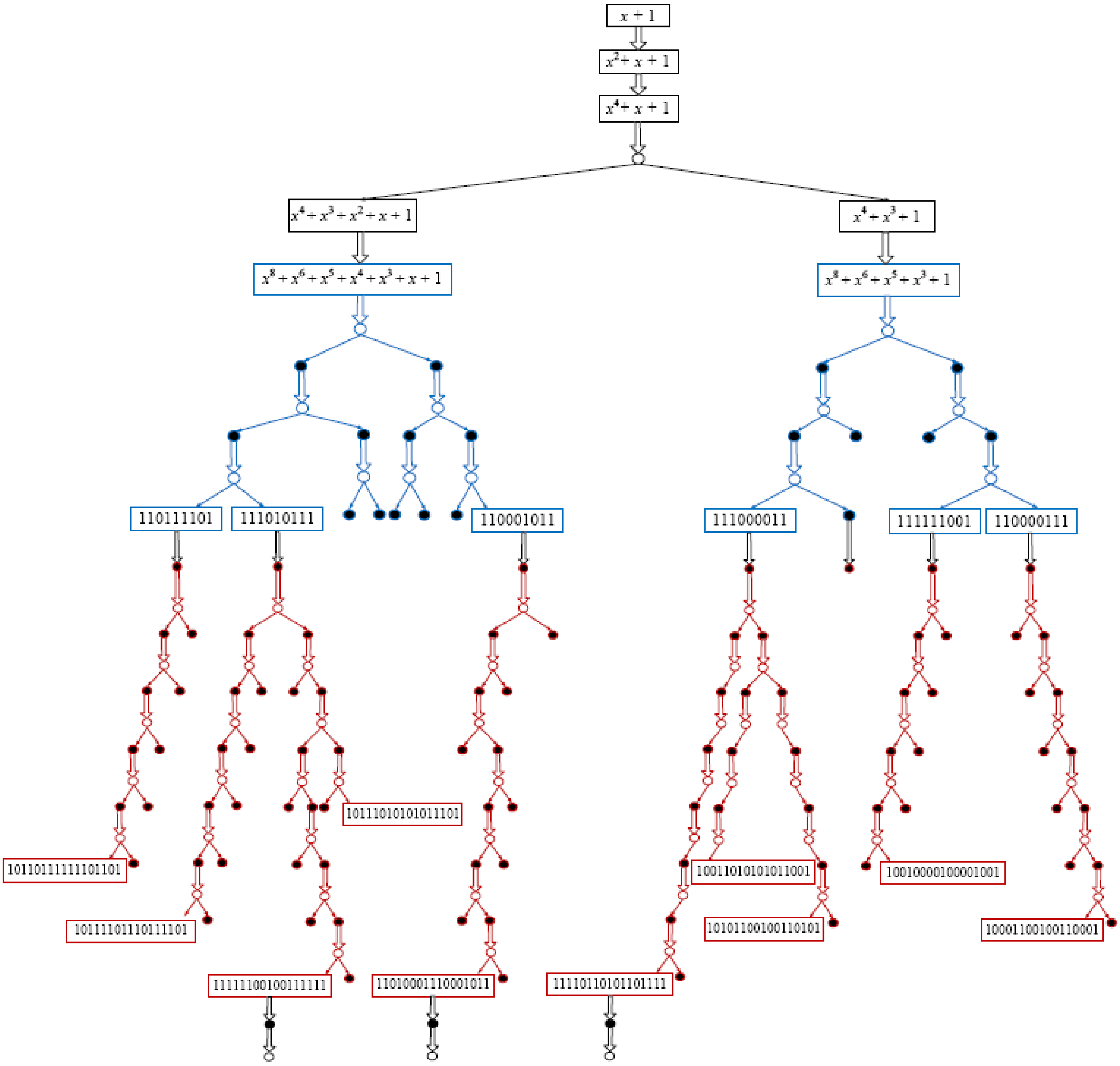

Fig 1. Extending fields through operation *P*

Proof. It is easy to prove that in the case of the irreducibility of the polynomial *f*(*x*), the coefficients *A* and A_1 are unequal to zero, while the polynomials $s_2(x)$ and $s_3(x)$ have the form:

$$s_2(x)=Ax^2+Bx+C,\ s_3(x)=A_1x^2+B_1x+C_1 \qquad (2)$$

and they are called root polynomials for a cyclic polynomial *f*(*x*).

Let *D*(*f*) be the discriminant of a polynomial $f(x)=x^3+ax+b$, that is:

$$D(f)=-4a^3-27b^2.$$

In the case of a cyclic polynomial *f*(*x*), the discriminant $D(f)=d^2$, $d\in F$, and for a field *F* the characteristics are unequal 2 and 3, Girstmair [12] proved that in equalities (1) and (2) we have:

$$s_2(x)=-\frac{2a^2}{d}+\left(\frac{9b}{2d}-\frac{1}{2}\right)x-\frac{3a}{d}x^2$$

$$s_3(x)=\frac{2a^2}{d}+\left(\frac{9b}{2d}-\frac{1}{2}\right)x+\frac{3a}{d}x^2. \qquad (3)$$

Formulas (3) give the explicit form of root polynomials for *f*(*x*), but these formulas do not make sense if the field *F* has characteristic 2 or 3.

Let us further consider the case when the field *F* has characteristic 2 and in *F*[*x*] there exist cyclic polynomials of third degree.

Every third degree polynomial over a field *F* with the help the corresponding linear substitution can be reduced to the form:

$$f(x)=x^3+ax+b. \qquad (4)$$

In [17], it was proved that an irreducible polynomial over *F* of type (4) has a cyclic Galois group over a field *F* of characteristic 2, only if equation:

$$y^2+by+a^3+b^2=0$$

has roots in the field *F*.

Let us find in this case the explicit form of root polynomials. Let be α is an arbitrary root of the polynomial $f(x)=x^3+ax+b$ from *F*, the characteristic of the field *F* is 2 and the Galois group of the polynomial *f*(*x*) is third-order cyclic. Then the polynomial *f*(*x*) takes the form:

$$f(x)=x^3+ax+b=(x-\alpha)(x^2+\alpha x+a+\alpha^2).$$

Let the remaining two roots α_2 and α_3 of the polynomial *f*(*x*) be represented as:

$$\alpha_2=A\alpha^2+B\alpha+C\,,\ \alpha_3=K\alpha^2+L\alpha+N$$

where the coefficients $A,B,C,K,L,N\in F$, α_2 and α_3 are the roots of the polynomial $g(x)=x^2+\alpha x+a+\alpha^2$. Therefore, the following relations are true:

$$\alpha_2+\alpha_3=\alpha,\ \ \alpha_2\cdot\alpha_3=a+\alpha^2. \qquad (5)$$

From (5), due to the irreducibility of the polynomial *f*(*x*) over the field *F*, we have: $B+L=1,\ \ C+N=0,\ \ A+K=0$, whence *C*= *N*, *L*= *B* +1, *A*=*K*. Thus,

$$\alpha_2=A\alpha^2+B\alpha+C\,,\ \alpha_3=A\alpha^2+(B+1)\alpha+C\,.$$

Since $g(\alpha_2)=(A\alpha^2+B\alpha+C)^2+\alpha(A\alpha^2+B\alpha+C)+$ $a+\alpha^2=0$, we have:

$$A^2\alpha^4+B^2\alpha^2+C^2+A\alpha^3+B\alpha^2+C\alpha+a+\alpha^2=0.$$

Considering the ratio

$$\alpha^3=a\alpha+b,\ \ \alpha^4=a\alpha^2+b\alpha$$

we get the following equality:

$$A^2(a\alpha^2+b\alpha)+B^2\alpha^2+C^2+A(a\alpha+b)+$$
$$+B\alpha^2+C\alpha+a+\alpha^2=0\,.$$

From here we have the equation system:

$$\begin{cases} C^2+Ab+a=0, \\ A^2b+C+Aa=0, \\ B^2+A^2a+B+1=0. \end{cases} \qquad (6)$$

From the third equation of the system we get

$$a=\frac{B^2+B+1}{A^2},$$

and since $A\neq 0$, then from the second equation of system (6) we have:

$$b=\frac{C+Aa}{A^2}=\frac{C+\dfrac{B^2+B+1}{A}}{A^2}=\frac{AC+B^2+B+1}{A^3}\,.$$

Then, from the first equation of system (6) follows the equality

$$C^2+A\cdot\frac{AC+B^2+B+1}{A^3}+\frac{B^2+B+1}{A^2}=0\,.$$

Simplifying the last equality, we get:

$$AC(AC+1)=0\,.$$

From the last equality, considering that $A\neq 0$, we have only two possibilities for *C*: or *C*= 0, or $C=\dfrac{1}{A}$. In the first case $a=\dfrac{B^2+B+1}{A^2}$, $b=\dfrac{B^2+B+1}{A^3}$ and then, the polynomial *f*(*x*) has the form:

$$f(x)=x^3+\frac{B^2+B+1}{A^2}x+\frac{B^2+B+1}{A^3}\,. \qquad (7)$$

In this case, the root polynomials are:

$$s_2(x)=Ax^2+Bx\,,\ s_3(x)=Ax^2+(B+1)x\,.$$

If a polynomial *f*(*x*) of the form (7) with given $A,B\in F$ is irreducible over *F*, then this is a cyclic polynomial.

In the second case, when $C=\dfrac{1}{A}$ we have $a=\dfrac{B^2+B+1}{A^2}$, $b=\dfrac{B^2+B+1}{A^3}$ and the polynomial *f*(*x*) takes the form:

$$f(x)=x^3+\frac{B^2+B+1}{A^2}x+\frac{B^2+B}{A^3}=$$
$$=x^3+(B^2+B+1)C^2x+(B^2+B)C^3\,. \qquad (8)$$

In this case, the root polynomials are:

$$s_2(x)=\frac{1}{C}x^2+Bx+C\,,\ s_3(x)=\frac{1}{C}x^2+(B+1)x+C\,.$$

If the polynomial *f*(*x*) of the form (8) with given $B,C\in F$ is irreducible over *F*, then this is a cyclic polynomial.□

Consider some examples.

Example 1. Let $F=Z_2(p)$, *B*= 1, $A=\dfrac{1}{p}$ then

$$f(x)=x^3+p^2x+p^3\,.$$

This polynomial is irreducible over $Z_2(p)$, since the elements 1, *p*, *p*^{2}, *p*^{3} are not its roots. Therefore, this polynomial is cyclic and its root polynomials have the form:

$$s_2(x)=x+\frac{1}{p}x^2\,,\ s_3(x)=\frac{1}{p}x^2\,.$$

Nontrivial automorphisms of the decomposition field of a polynomial *f*(*x*) over *F* are determined by the maps:

$$\sigma(k+l\alpha+m\alpha^2)=k+l\left(\alpha+\frac{1}{p}\alpha^2\right)+m\left(\alpha+\frac{1}{p}\alpha^2\right)^2=$$
$$=k+l\alpha+\frac{l}{p}\alpha^2+m\alpha^2+\frac{1}{p^2}m\alpha^4=$$
$$=k+l\alpha+\frac{l}{p}\alpha^2+m\alpha^2+\frac{m}{p^2}(p^2\alpha^2+p^3\alpha)=$$
$$=k+l\alpha+\frac{l}{p}\alpha^2+m\alpha^2+m\alpha^2+mp\alpha=$$
$$=k+(l+mp)\alpha+\frac{l}{p}\alpha^2=k+\frac{l}{p}\alpha^2+m\alpha^2+mp\alpha=$$
$$=k+(mp)\alpha+\left(\frac{l}{p}+m\right)\alpha^2,\ \ k,l,m\in F\,.$$

Example 2. Let the field $F=Z_2(p)$, *B*=*p*, *C*=1. Then from (8) we have

$$f(x)=x^3+(p^2+p+1)x+(p^2+p).$$

This polynomial is irreducible in $Z_2(p)$, since the elements 1, *p*, *p*+1 are not the roots of this polynomial, hence, this is a cyclic polynomial with root polynomials:

$$s_2(x)=1+px+x^2\,,\ s_3(x)=1+(p+1)x+x^2\,.$$

If α is one root of the polynomial *f*(*x*), then the other two roots of this there is a polynomial

$$\beta=s_2(\alpha)=1+p\alpha+\alpha^2\,,\ \gamma=s_3(\alpha)=1+(p+1)\alpha+\alpha^2$$

and the nontrivial automorphisms of the decomposition field of a polynomial *f*(*x*) over *F* are determined by the maps:

$$\sigma\left(k+l\alpha+m\alpha^2\right)=k+l\left(s_2(\alpha)\right)+m\left(s_2(\alpha)\right)^2,$$
$$\sigma^2\left(k+l\alpha+m\alpha^2\right)=k+l\left(s_3(\alpha)\right)+m\left(s_3(\alpha)\right)^2,$$

where $k,l,m\in F$.

Let *F* be the field of characteristic 2 over which there are cyclic extensions of degree 3, i.e. there are cyclic, irreducible over *F* cubic polynomials with coefficients from a field *F*. We will show that under certain conditions on a field *F* there are cyclic third degree polynomials do not have three linear root polynomials.

Let $f(x)=x^3+qx+r$ be irreducible over a cyclic field *F* polynomial and α, $a\alpha+b$, $c\alpha+d$ are its roots, i.e. *x*, *ax*+*b*, *cx*+*d*, where $a,b,c,d\in F$, are its root polynomials.

Since $\alpha+(a\alpha+b)+(c\alpha+d)=0$,then $a+c+1=0,\ b+d=0$, whence we get $c=a+1,\ b=d$, and therefore, α , $a\alpha+b$, $(a+1)\alpha+b$ are the roots of the polynomial *f*(*x*). Then

$$\alpha\cdot(a+\alpha)+\alpha\cdot((a+1)\alpha+b)+(a\alpha+b)((a+1)\alpha+b)=q.$$

Simplifying this equality, we get

$$\left(a^2+a+1\right)\alpha^2+b\alpha+b^2=q,$$

whence $b=0,\ q=0,\ a^2+a+1=0$.

So, in the case under consideration (when all three root polynomials of *f*(*x*) are cyclic), we have: $f(x)=x^3+r$ and the equation $x^2+x+1=0$ has a root in the field *F*.

The field $F=Z_2(p)$ admits cyclic extensions of the third degree and the equation $x^2+x+1=0$, obviously, has no roots in the field Z_2 (*t*). Thus, the cyclic polynomials of the third degree with coefficients from $Z_2(p)$ have one linear root polynomial *x* and two polynomials of the second degrees, since, obviously, two linear root polynomials and one of the second degree cannot have a cyclic polynomial of the third degree over a field of any characteristic.

V. Conclusion

From an algebraic point of view, the theory of expansion of finite fields is completed in its final form. In general terms, it is presented in Galois theory. However, from the point of view of discrete mathematics and cybernetics, many problems of constructing such extensions require more detailed development in order to obtain an efficient algorithmic implementation.

The paper deals with the arithmetic of finite fields. Root polynomials are constructed for some third-degree cyclic polynomial over the field F_2. In addition, all irreducible polynomials of degree 2^n over F_2 are generated by field extension operations, and a complete binary tree of such polynomials is constructed and their properties are studied.

The obtained results and methods can find both theoretical and practical applications, in addition to the number of the most detailed investigations of the theoretical and finite fields and the search results. Thus, the totality of the results obtained in the article can be qualified as a new contribution to the development and justification of mathematical principles aimed to the development of the theory of finite fields.

Acknowledgment

Authors are highly thankful to Muratbekov M. for their helpful remarks. Also thanks to the editor and anonymous reviewers who helped so that the article could be published in this journal.

References

[1] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, UK, 1994.

[2] V. V. Prasolov, *Mnogochleny*, M.: MTSNMO, 2003, pp. 58-72. [in Russian]

[3] N. Koblitz, *Algebraic aspects of Cryptography*, Springer-Verlag, Berlin, Heidelberg, 1998. -217 p.

[4] Hua Huang, Shanmeng Han, Wei Cao, ‘’Normal bases and irreducible polynomials’’, *Finite Fields Appl.*, 2018, vol. 50, pp. 272-278.

[5] K.L. Geut, S.S. Titov, “O generatsii neprivodimykh mnogochlenov prostykh poryadkov dlya postroyeniya diskretnykh ustroystv SZHATiS”,[On the generation of irreducible polynomials of simple orders for constructing discrete devices SZhATiS], *Transport Urala: nauch.-tekh. zhurnal. Yekaterinburg: UrGUPS*, 2014. vol. 1 (40). pp. 61–64. [in Russian]

[6] Ye. A. Khomich, ‘’Neprivodimyye mnogochleny nad konechnymi polyami i svyaz' s kriptografiyey’’, [Irreducible polynomials over finite fields and the connection with cryptography], *Akademicheskaya publitsistika*, 2017, vol. 3., pp.19-24. [in Russian]

[7] Lucas Reis, Qiang Wang, “The dynamics of permutations on irreducible polynomials”, *Finite Fields and Their Applications*, 2020, vol. 64, https://doi.org/10.1016/j.ffa.2020.10101664

[8] Kitae Kim, Ikkwon Yie, “A correspondence of certain irreducible polynomials over finite fields”, *Finite Fields and Their Applications* 2012, vol. 18, pp. 384–395.

[9] Shiv Gupta, “Irreducible Polynomials in ℤ[*x*] That Are Reducible Modulo All Primes”, *Open Journal of Discrete Mathematics*, 2019, vol. 9, pp. 52-61.

[10] H. Kleiman, ‘’Methods for polynomials and related theorems’’, *Monatshefte fur Mathematik*, vol. 73, 1969, pp. 63 - 68.

[11] H. Muthsam, ‘’Eine bemerkung uber die wurzelpolynome Galoiisscher gleichungen’’, *Monatshefte fur Mathematik*, vol. 83, 1977, pp. 155 - 157.

[12] K. Girstmair, ‘’On root polynomials of cyclic cubic equation’’, *Arch. Math*, vol. 36, 1981. pp. 313 - 326.

[13] S. Henry and Warren, Jr. *Hacker’s Delight*. - 3rd ed-Addison Wesley, 2013.- 816 p.

[14] U. Turusbekova, “Finding irreducible polynomials of a special type”, *Bulletin of Kazakh National Technical University, 2019*, vol. 6 (136), pp. 691-696.

[15] R.E. Crandall and C.B. Pomerance, *Prime Numbers: A Computational Perspective* , New York: Springer-Verlag, 2005.- 597 p.

[16] Sankhanil Dey, Amlan Chakrabarti, Ranjan Ghosh. ‘’4-bit crypto S-boxes: Generation with irreducible polynomials over Galois field GF(24) and cryptanalysis’’, *International Journal of Tomography & Simulation*, vol.32, no.3, 2019. pp.46-60.

[17] A. E. Sergeev, ‘’On the task of I. Kaplansky’’, *News of universities; North Caucasus region. Natural Sciences*. 2001. vol. 1. pp. 14 - 17.