CERTAIN CONSTRUCTION OF FINITE FIELDS

August 03, 2012
S. M. TUDUNKAYA[1] AND S. O. MAKANJUOLA[2]
Kano University of Science and Technology, Wudil, Nigeria[1]
University of Ilorin, Ilorin, Nigeria[2]
E-mail: *tudunkayaunique@yahoo.com*[1] *somakanjuola@unilorin.edu.ng*[2]

Abstract

In this piece of note, certain new concepts were introduced in the algebra of rhotrices and these concepts were used to construct some mathematical structures over which polynomials were defined. With the aid of these innovations, some existing mathematical concepts that are related to construction of finite fields were discussed.

Subject classification: 12E05, 12E20

Key words: Rhotrix, Ring, Integral domain, Polynomial, Field.

1 Introduction

Traditionally, polynomials were mostly defined over rings as real numbers, rational numbers, Z_n, Z_p for a prime p, where these rings may at times be integral domains or even fields. Upon these definitions, constructions may take place, for example, the construction of finite fields. This note, presents a new but interesting idea in this respect, polynomials were defined over the field $F_p[R]$ of rhotrices of the same cardinality under the operations of rhotrix addition and multiplication. The roots of the irreducible polynomials over these fields were used to generate the elements of a certain multiplicative group, which together with the zero rhotrix give entire elements of a particular finite field. The operations of rhotrix addition and multiplication with that of polynomials addition and multiplication together with addition and multiplication mod p were used. The hope is that, this achievement may bring new research opportunities in the areas of polynomials, fields and finite fields.

Ajibade [1], defined rhotrix as an element of the set

$$R = \left\{ \left\langle \begin{matrix} a \\ b\ c\ d \\ e \end{matrix} \right\rangle : a, b, c, d, e \in \Re \right\} \qquad (1)$$

The name rhotrix was as a result of the rhomboid nature of the object. Also the heart of a rhotrix R given as $h(R)$, was defined as the entry at the perpendicular intersection of the two diagonals of a rhotrix, that is c in the case above. The operation of addition was defined as follows:

$$R + Q = \left\langle \begin{matrix} a \\ b\ h(R)\ d \\ e \end{matrix} \right\rangle + \left\langle \begin{matrix} f \\ g\ h(Q)\ j \\ k \end{matrix} \right\rangle = \left\langle \begin{matrix} a+f \\ b+g\ \ h(R)+h(Q)\ \ d+j \\ e+k \end{matrix} \right\rangle \qquad (2)$$

Also, since

$$A + (-A) = \left\langle \begin{matrix} a \\ b\ h(R)\ d \\ e \end{matrix} \right\rangle + \left\langle \begin{matrix} -a \\ -b\ -h(R)\ -d \\ -e \end{matrix} \right\rangle = \left\langle \begin{matrix} 0 \\ 0\ 0\ 0 \\ 0 \end{matrix} \right\rangle \qquad (3)$$

which is the additive identity, $-A$ was given as the additive inverse of A. It was also shown that $\{R,+\}\cup 0$ where $0=\left\langle \begin{matrix} 0 \\ 0\ 0\ 0 \\ 0 \end{matrix} \right\rangle$ is a commutative group. Scalar multiplication was defined as follows:

$$\alpha R = \alpha \left\langle b\ \begin{matrix} a \\ h(R) \\ e \end{matrix}\ d \right\rangle = \left\langle \alpha b\ \begin{matrix} \alpha a \\ \alpha h(R) \\ \alpha e \end{matrix}\ \alpha d \right\rangle \qquad (4)$$

Multiplication can be defined in many ways, but the following multiplication method was given:

$$R \bullet Q = \left\langle b\ \begin{matrix} a \\ h(R) \\ e \end{matrix}\ d \right\rangle \bullet \left\langle g\ \begin{matrix} f \\ h(Q) \\ k \end{matrix}\ j \right\rangle = \left\langle \begin{matrix} ah(Q)+fh(R) \\ bh(Q)+gh(R)\ \ h(R)h(Q)\ \ dh(Q)+jh(R) \\ eh(Q)+kh(R) \end{matrix} \right\rangle \qquad (5)$$

This multiplication method was adopted in this work. It was given that the set R is a commutative algebra. The multiplicative identity of R was given as:

$$I = \left\langle \begin{matrix} 0 \\ 0\ 1\ 0 \\ 0 \end{matrix} \right\rangle \qquad (6)$$

Also, if

$$R \bullet Q = \left\langle b\ \begin{matrix} a \\ h(R) \\ e \end{matrix}\ d \right\rangle \bullet \left\langle g\ \begin{matrix} f \\ h(Q) \\ k \end{matrix}\ j \right\rangle = \left\langle \begin{matrix} 0 \\ 0\ 1\ 0 \\ 0 \end{matrix} \right\rangle \qquad (7)$$

Then

$$Q = R^{-1} = -\frac{1}{h(R)^2} \left\langle b\ \begin{matrix} a \\ -h(R) \\ e \end{matrix}\ d \right\rangle, \quad h(P) \neq 0 \qquad (8)$$

Later, Mohammed [2], provide a generalised definition of a rhotrix A of dimension n under the same operation, as:

$$A(n) = \left\langle \begin{matrix} & & & a_1 & & \\ & & a_2 & a_3 & a_4 & \\ & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{\left\{\frac{(t+1)}{2}\right\}-\frac{n}{2}} & \cdots & \cdots & a_{\left\{\frac{(t+1)}{2}\right\}} & \cdots & \cdots\ a_{\left\{\frac{(t+1)}{2}\right\}+\frac{n}{2}} \\ & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & a_{t-3} & a_{t-2} & a_{t-1} & \\ & & & a_t & & \end{matrix} \right\rangle \qquad (9)$$

Where and henceforth $t=\frac{(n^2+1)}{2},\ n\epsilon 2Z^+ + 1$ and $\frac{n}{2}$ is the integer value upon division of n
Define a modulo rhotrix as a rhotrix

$$M[R_{z^t}] = \left\{ \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & a_{\beta} & \cdots & \cdots \; 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \right\} \qquad (10)$$

Where, addition (+) and multiplication (•) are done modulo n under the addition and multiplication of rhotrices. Here, $\alpha = \frac{n^2-2n+5}{4}$, $\beta = \frac{1}{4}(n^2+3)$, $\pi = \frac{n^2+2n+1}{4}$
The additive identity is

$$0 = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & 0_{\beta} & \cdots & \cdots \; 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \qquad (11)$$

The multiplicative identity is

$$I = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & 1_{\beta} & \cdots & \cdots \; 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \qquad (12)$$

And if $n = p$, the multiplicative inverse of

$$A = \left\langle \begin{matrix} & & a_1 & & \\ & a_2 & a_3 & a_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{\alpha} \cdots & \cdots & a_{\beta} & \cdots & \cdots \; a_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & a_{t-3} & a_{t-2} & a_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \qquad (13)$$

will be

$$B = \left\langle \begin{array}{ccccccc} & & & b_1 & & & \\ & & b_2 & b_3 & b_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ b_\alpha & \cdots & \cdots & b_\beta & \cdots & \cdots & b_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & b_{t-3} & b_{t-2} & b_{t-1} & & \\ & & & b_t & & & \end{array} \right\rangle \tag{14}$$

such that,

$$\begin{aligned} a_\beta\, b_\beta &\equiv 1 \bmod p \\ a_1\, b_\beta + b_1\, a_\beta &\equiv 0 \bmod p \\ a_2\, b_\beta + b_2\, a_\beta &\equiv 0 \bmod p \\ a_3\, b_\beta + b_3\, a_\beta &\equiv 0 \bmod p \\ a_4\, b_\beta + b_4\, a_\beta &\equiv 0 \bmod p \\ &\cdots \\ &\cdots \\ &\cdots \\ a_{t-3}\, b_\beta + b_{t-3}\, a_\beta &\equiv 0 \bmod p \\ a_{t-2}\, b_\beta + b_{t-2}\, a_\beta &\equiv 0 \bmod p \\ a_{t-1}\, b_\beta + b_{t-1}\, a_\beta &\equiv 0 \bmod p \\ a_t\, b_\beta + b_t\, a_\beta &\equiv 0 \bmod p \end{aligned}$$

A field is by definition a set of elements that is closed under the ordinary operations of addition, subtraction, multiplication and division (except by zero). A field is said to be finite if it has finite number of elements. Also recall that, the prime subfield of a field, is isomorphic either to the rationals Q, where its characteristic will be 0 or to the finite field F_p for a prime p, where it will have characteristic p. Any field of characteristic 0 is infinite because it contains Q. Now since a finite field is a field that has finite number of elements, it can not contain Q, so it has a prime subfield of the form F_p for some prime p. Also, every field is a subfield of itself. Let

$$F_p[R] = \left\{ \left\langle \begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha & \cdots & \cdots & a_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & a_t & & & \end{array} \right\rangle \right\} \tag{15}$$

$F_p[R]$ together with the operations of rhotrix addition (+) and multiplication(•) under addition and multiplication $mod\ p$ is a field.

The additive identity is

$$0 = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & 0_{\beta} & \cdots & \cdots \; 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \tag{16}$$

The multiplicative identity is

$$I = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & 1_{\beta} & \cdots & \cdots \; 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \tag{17}$$

And the multiplicative inverse of

$$A = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & a_{\beta} & \cdots & \cdots \; 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & 0_t & & \end{matrix} \right\rangle \tag{18}$$

will be

$$B = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & b_{\beta} & \cdots & \cdots \; 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & 0_t & & \end{matrix} \right\rangle \tag{19}$$

such that,

$$a_{\beta}\, b_{\beta} \equiv 1 \; mod \; p$$

Now, define

$$F_{p^n}[R] = \left\{ \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha \cdots & \cdots & a_\beta & \cdots & \cdots \; 0_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \forall\, a \in Z_{p^n} \right\} \qquad (20)$$

2 Polynomials over $F_{p^n}[R]$

Here, the possibility of carrying over the properties polynomials defined over the ring Z_{p^n} to polynomials over $F_{p^n}[R]$ was looked into. This is because; it is easier to show that $F_{p^n}[R]$ and Z_{p^n} are isomorphic. Define a polynomial in the indeterminate$x$, over $F_{p^n}[R]$ as an expression of the form

$$f(x) = A_0 + A_1 x + \cdots + A_{m-1}x^{m-1} + A_m x^m \qquad (21)$$

where $A_i \in F_{p^n}[R]$ and m is a positive integer. The set of all polynomials of this form will be denoted by $F_{p^n}[R](x)$. m is the degree of f, if $A_m \neq 0$ (the zero of $F_{p^n}[R]$) and if

$$A_m = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha \cdots & \cdots & 1_\beta & \cdots & \cdots \; 0_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \qquad (22)$$

then f is monic and A_m is called the leading coefficient of f. Also, define

$$f = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha \cdots & \cdots & 0_\beta & \cdots & \cdots \; 0_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \qquad (23)$$

as the zero polynomial.

Now by the regular addition and multiplication of polynomials as discussed in Brent [3], if

$$f = \sum_{i=0}^{n} A_i x^i \qquad (24)$$

And

$$g = \sum_{i=0}^{m} B_i x^i \qquad (25)$$

Then

$$f + g = \sum_{i=0}^{\max(n,m)} (A_i + B_i) x^i \tag{26}$$

And

$$fg = \sum_{k=0}^{n+m} C_k x^k \tag{27}$$

Where

$$C_k = \sum_{i+j=k} A_i B_j \tag{28}$$

The operation of the coefficients is that defined on the elements of the ring $F_{p^n}[R]$.

Note before we move further that, by scalar multiplication of rhotrices,

$$\left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha \cdots & \cdots & a_\beta & \cdots & \cdots \; 0_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle x^n$$

$$= \left\langle \begin{matrix} & & 0_1 x^n & & \\ & 0_2 x^n & 0_3 x^n & 0_4 x^n & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha x^n \cdots & \cdots & a_\beta x^n & \cdots & \cdots \; 0_\pi x^n \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} x^n & 0_{t-2} x^n & 0_{t-1} x^n & \\ & & a_t x^n & & \end{matrix} \right\rangle$$

$$\left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha \cdots & \cdots & a_\beta x^n & \cdots & \cdots \; 0_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle$$

where $a \in Z_{p^n}$ let us denote this by aAx^n so that

$$A = \left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & 1_{\beta} & \cdots & \cdots\ 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle \tag{29}$$

Also, by multiplication of rhotrices,

$$\left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & x_{\beta} & \cdots & \cdots\ 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle^{n}$$

$$\left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & x_{\beta} & \cdots & \cdots\ 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle n - times$$

$$\left\langle \begin{matrix} & & 0_1 & & \\ & 0_2 & 0_3 & 0_4 & \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_{\alpha} \cdots & \cdots & x_{\beta}^{n} & \cdots & \cdots\ 0_{\pi} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & a_t & & \end{matrix} \right\rangle$$

With this, the following results will follow:

2.1 Theorem

$(F_{p^n}[R](x), +)$ is a commutative group.

Proof:

The additive identity is $0A = 0$ and the additive inverse of

$f = \sum_{i=0}^{n} A_i x^i = -\sum_{i=0}^{n} A_i x^i = -f$ ■

The proof of (2.2) below is now trivial.

2.2 Theorem

$(F_{p^n}[R](x), +, \bullet)$ is a ring.

2.3 Theorem

$(F_{p^n}[R](x), +, \bullet)$ is an integral domain.

Proof:

It is enough to show that if $f, g \in F_{p^n}[R](x)\ and\ fg = o,\ then\ either\ f = 0\ or\ g = 0\ or\ f = g = 0$ ■

Note that $F_{p^n}[R](x)$ is the set of all polynomials over $F_{p^n}[R]$. Define a polynomial $f \in F_{p^n}[R](x)$ to be irreducible in $F_{p^n}[R]$ if it can not be expressed as a product of two non scalar polynomials in $F_{p^n}[R]$. This means any root α of f will not be in $F_{p^n}[R](x)$, hence there is a smallest field extension $F_{p^n}[R]^*$ that contains α. These roots are called conjugates. If f is irreducible in $F_{p^n}[R]$, then the ideal generated by f denoted by $\langle f \rangle$ is a principal ideal such that $F_{p^n}[R]^*$ is isomorphic to $F_{p^n}[R](x)/\langle f \rangle$. If the degree of f is m, then $\left|F_{p^n}[R]^* : F_{p^n}[R]\right| = m$ and the basis of $F_{p^n}[R]^*$ over $F_{p^n}[R]$ contains elements $\alpha^0 = 1, \alpha, \alpha^1, \ldots, \alpha^{m-1}$. Also, $F_{p^n}[R]^* = F_{p^n}[R](\alpha)$, when $F_{p^n}[R]^*$ is regarded as avector space over $F_{p^n}[R]$.

Test for irreducibility:

To test the irreducibility of the polynomial f over $F_{p^n}[R]$, one of the following methods will be used:
(i) every polynomial f that can be expressed over $F_{p^n}[R]$ as the product of linear factors $(x - A_{i's})$ where $A_i \in F_{p^n}[R]$, is reducible in $F_{p^n}[R]$, otherwise it is irreducible.
(ii) If at least one substitution of the elements $F_{p^n}[R]$ for x in the polynomial f evaluates to zero, then f is reducible over $F_{p^n}[R]$, otherwise it is irreducible.

The smallest field in which the polynomial f is reducible, is called the splitting field of f. Theorems (2.4), (2.5), (2.6) and (2.7) will just be stated without proofs.

2.4 Theorem

If f is irreducible in $F_{p^n}[R]$ its splitting over $F_{p^n}[R]$ exist and are isomorphic.

2.5 Theorem

The degree of the polynomial f in $F_{p^n}[R]$ is the same as the degree of its splitting field over $F_{p^n}[R]$.

The formal derivative of a polynomial $f(x) = A_m x^m + A_{m-1}x^{m-1} + \cdots + A_1 x + A_0$ where $A_i \in F_{p^n}[R]$ is $f'(x) = mA_m x^{m-1} + (m-1)A_{m-1}x^{m-2} + \cdots + A_1$ of degree $m - 1$,which can be zero even if f is not a constant polynomial.

If f and g are polynomials in $F_{p^n}[R]$ such that $deg\ f > deg\ g$, then by the Euclidean algorithm, there exists two polynomials q and r such that $f = qg + r$, where r may be zero and $deg\ r < deg\ g$ and the greatest common divisor (gcd) of f and g denoted by $(f,g) = af + bg$ for some $a, b \in F_{p^n}[R](x)$.

2.6 Theorem

If f and g are in $F_{p^n}[R](x)$ and $F_{p^n}[R]^*$ an extension of $F_{p^n}[R]$, then
(a) $(f,g)= d$ in $F_{p^n}[R](x)$ iff $(f,g)= d$ in $F_{p^n}[R]^*(x)$
(b) f/g in $F_{p^n}[R](x)$ iff f/g in $F_{p^n}[R]^*(x)$
(c) f has multiple zero iff $(f,g)\neq 1$

2.7 Theorem

Every $f \in F_{p^n}[R](x)$ of degree m has at most m zeros in $F_{p^n}[R]^*$.

Also recall that an isomorphism $\gamma: F_1 \to F_2$ is a one-to-one mapping of the field F_1 onto the field F_2 such that $\gamma(a+b)=\gamma(a)+\gamma(b)$ and $\gamma(ab)=\gamma(a)\gamma(b)$ for all $a,b \in F_1$. If $F_1 = F_2$ then γ is an automorphism. The set γ of all automorphisms of a field forms a group under composition and distinct isomorphisms $\gamma_1, \gamma_2, \dots, \gamma_k$ of F_1 onto F_2 are linearly independent over F_2 such that if $\gamma(a_i) = b_i \in F_2$ then $a_1b_1 + a_2b_2 + \cdots + a_kb_k = 0$ only if all $a_i = 0$. Under field automorphism, the elements of the prime subfield are left fixed.

3 Properties of $F_{p^n}[R]$

Let

$$F_{p^n}[R] = \left\{ \left\langle \begin{matrix} & & & 0_1 & & \\ & & 0_2 & 0_3 & 0_4 & \\ & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha & \cdots & \cdots & a_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & & a_t & & \end{matrix} \right\rangle \forall\, a \in Z_{p^n} \right\}$$

Since finite fields are of prime power order, we consider the ring $F_{p^n}[R]$, where n is any positive integer.

3.1 Theorem

The characteristic of $F_{p^n}[R]$ is p.

Proof:

Take an arbitrary element $\mu \in F_{p^n}[R]$, then $0 = \mu + \mu + \mu + \cdots + \mu \;\; p - times$ ■

3.2 Theorem

The prime subfield of $F_{p^n}[R]$ is $F_p[R]$.

Proof:

Suppose there exists $S_p[R]$ such that $S_p[R] \subseteq F_p[R]$, then if $S_p[R] = F_p[R]$

we are done. Also, $S_p[R] \subset F_p[R]$ means $\exists$ an element $\beta \in F_p[R] \ni \beta \notin S_p[R]$ which means $S_p[R]$ will not be a field since β is either additive or multiplicative identity, or the inverse of some element ■

3.3 Theorem

$F_{p^n}[R]$ is a vector space over $F_p[R]$

Proof:

Since $F_{p^n}[R]$contains a copy of $F_p[R]$, then $F_{p^n}[R]$ can be regarded as a field extension of $F_p[R]$ which proves the theorem ■

3.4 Theorem

$\left|F_{p^n}[R]\right| = p^n$

Proof:

This is because $F_{p^n}[R]$ can be regarded as a vector space over $F_p[R]$ of finite dimension n with characteristic p ■

3.5 Theorem

$F_{p^n}[R]$ is the splitting field for $Ax^{p^n} - Ax$.

Proof:

Recall that if $F_{p^n}[R]$ has characteristic p and a prime subfield $F_p[R]$, then it will be the splitting field for $Ax^{p^n} - Ax$ iff it has p^n elements and (3.4) proved this. Hence, the result follows ■

3.6 Corollary

For any prime p and any positive integer n, $F_{p^n}[R]$ exists.

Proof:

The proof follows from (2.4) and (3.5) ■

3.7 Theorem

$(F_{p^n}[R],\bullet)$ is cyclic.

Proof:

If m is the highest order of an element in $(F_{p^n}[R],\bullet)$, then from the fact that in any finite abelian group, the order of all elements divide the maximal order it means $\lambda \in (F_{p^n}[R],\bullet)$ implies $\lambda^m = A$, this means all elements in $(F_{p^n}[R],\bullet)$ are roots of $Ax^m - A$.

Now, let $r = |F_{p^n}[R]|$ since the number of roots of a polynomial defined over a ring is at most the degree of the polynomial and $Ax^m - A$ has $r-1$ roots in $F_{p^n}[R]$, therefore $r-1 \leq m$. Also, since m is the order of an element in $(F_{p^n}[R],\bullet)$, $\frac{m}{r} - 1$ then $m \leq r-1$. Hence, $m = r-1$ ■

Recall that an element that generates a cyclic group is called primitive element.

3.8 Theorem

Over any field $F_p[R]$, $(Ax^m - A)$ / $(Ax^k - A)$ iff m/k.

Proof:
If $k = qr + r$, $r \leq m$, then $Ax^k - A = Ax^r(\sum_{i=0}^{q-1} x^{im})(Ax^m - A) + Ax^r$ implying
$(Ax^m - A)$ / $(Ax^k - A)$ iff x^r=1, $\Rightarrow r = 0$. Hence, $k = qm$ ■

3.9 Corollary

For any prime integer p, $(Ax^{p^m} - A)$ / $(Ax^{p^k} - A)$ iff m/k.

Proof:
The proof follows from (3.8) above.

3.10 Theorem

$F_{p^m}[R]$ is a subfield of $F_{p^n}[R]$ iff m/n.

Proof:

If $F_{p^m}[R] \subseteq F_{p^n}[R]$, then $F_{p^n}[R]$ can be regarded as a vector space over $F_{p^m}[R]$ with finite dimension l, then $p^n = p^{lm}$.
Also, if $m = n$, then $p^m = p^n$, by Sylow theorem, $F_{p^m}[R]$ exists ■

4 The construction

To illustrate the construction, method presented by Cherowitz[4] was applied.

4.1 Examples

Take the field $F_4[R] = F_{2^2}[R] \Rightarrow F_2[R]=\{0, A\}$ where

$$0 = \left\langle \begin{matrix} & & & 0_1 & & \\ & & 0_2 & 0_3 & 0_4 & \\ & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0_\alpha & \cdots & \cdots & 0_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & \\ & & & a_t & & \end{matrix} \right\rangle$$

is the prime subfield.

Now, the entire monic polynomials over $F_2[R]$ are 2^2 in number, that is

$$Ax^2$$
$$Ax^2 + A$$
$$Ax^2 + Ax$$
$$Ax^2 + Ax + A$$

by the test of irreducibility, the only irreducible one is

$$Ax^2 + Ax + A$$

and If μ is it's root,

$$A\mu^2 = A\mu + A$$

therefore,

$$A\mu = A\mu$$
$$A\mu^2 = A\mu + A$$
$$A\mu^3 = A\mu(A\mu + A)$$

these powers of μ together with

$$0 = \left\langle \begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha & \cdots & \cdots & 0_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & a_t & & & \end{array} \right\rangle$$

are the field elements. Note that $2 \equiv 0$ here and in any case, the left and the right representations are isomorphic.

4.2 Example

Suppose we consider $F_8[R] = F_{2^3}[R] \Rightarrow F_2[R]=\{0, A\}$ is the prime subfield, the monic polynomials are 2^3.

$$Ax^3$$
$$Ax^3 + A$$
$$Ax^3 + Ax$$
$$Ax^3 + Ax^2$$
$$Ax^3 + Ax + A$$
$$Ax^3 + Ax^2 + A$$
$$Ax^3 + Ax^2 + Ax$$
$$Ax^3 + Ax^2 + Ax + A$$

Observe that $Ax^3 + Ax + A$ is irreducible, taking ∂ to be its root implies

$$A\partial^3 = A\partial + A$$

therefore, we have:

$$A\partial = A\partial$$
$$A\partial^2 = A\partial^2$$
$$A\partial^3 = A\partial + A$$
$$A\partial^4 = A\partial(A\partial + A) = A\partial^2 + A\partial$$
$$A\partial^5 = A\partial(A\partial^2 + A\partial) = A\partial^3 + A\partial^2 + A\partial = A\partial + A + A\partial^2 + A\partial = A + A\partial^2$$

$$A\partial^6 = A\partial(A + A\partial^2) = A\partial^3 + A\partial$$

And

$$A\partial^7 = A\partial(A\partial^3 + A\partial) = A\partial^4 + A\partial^2 = A + A\partial^2 + A\partial^2 = A$$

these plus zero rhotrix gave the field.

The reader can try $F_{27}[R] = F_{3^3}[R] \Rightarrow F_3[R]=\{0, A, 2A\}$ is the prime subfield. There would be 3^3 monic polynomials over this field. If a root fails to generate the multiplicative group, try another one, because it may not be primitive.

References

[1] Ajibade, A.O., (2003). The concept of rhotrix in Mathematical enrichment, Int. J. Math. Educ. Sci. Technol., 34: 175-179.

[2] Mohammed, A. (20011). Theoretical Development and Application of Rhotrices, PhD Dissertation ABU Zaria. Amazon.com

[3] Brent, E.,2009. *Symmetries of equations :An introduction to Galois theory*: University of York, York Y010 5DD, England.

[4] Cherowitz, B.,2006. Introduction to
Finite Fields. (http://www.cudenver.edu/echeroni/vboutdrd/tin_lds.html)