International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 1
ISSN: 2454-4248
12 – 15

# Finite Files and Irreducible Polynomials

Dr. K. Selvaraj
M.Sc.,M.Phil., Ph.D.,
Assistant Professor, Department of Mathematics,
PRIST University,Vallam, Thanjavur

A. Usha
M.Phil - Research Scholar, Department of Mathematics,
PRIST University, Vallam, Thanjavur

**ABSTRACT:** In this thesis we related the notion on constructions of irreducible polynomials over finite fields. A polynomial with integer coefficients or more generally, with coefficients in a unique factorization domain is sometimes said to be irreducible if it is an irreducible element of the polynomial ring. That is, not invertible, not zero and cannot be factored into the product of two non-invertible polynomials with coefficients. The estimates for the preprocessing time depend on unproven conjectures.

***Key words:*** *Polynomials, irreducible element, finite fields, invertible, not-invertible, deterministic.*

*****

## I. INTRODUCTION

Within the framework of polynomial time, the major remaining theoretical challenge is to remove probabilistic choice from the algorithms.

We address this challenge for the problem of finding irreducible polynomials over finite fields, and given some deterministic methods for computing such polynomials.

These polynomials provide the field extensions required in several algorithms, such as factoring multivariate polynomials (Chistov&Grigoyev [1982], von zurGathen [1985], Lenstra [1985], von zurGathen&Kaltofen [1985a, 1985b], and very fast parallel arithmetic polynomials (Eberly [1984]).

Rabin [1980] gives a probabilistic method for finding irreducible polynomials (see also Calmet& Loos [1980]); Camion [1983] shows how to obtain deterministically large irreducible polynomials from small ones.

The irreducible polynomials that we consider in this paper are very easy to compute, in linear time.

After learning the present results, Adleman&Lenstra [1986] proposed differnet methods for computing irreducible polynomials.

In this dissertation we are going to see about finite fields, irreducible Polynomials over finite fields in detailed manner.

All the materials presented in here is expository and taken from the various sources, listed in the reference.

We also provided many examples throughout this dissertation.

This dissertation contains four chapters.

In first chapter contains some basic definition‘s and help to run the full project.

The second chapter deals with Finite fields and their characterization. We also see an important characterization theorem which says about the existence and uniqueness of finite fields. At the end of this chapter, we give a criterion for subfields.

The third chapter of this dissertation deals with irreducible polynomials over finite fields. In this we are going to see the theorems related to irreducible polynomials and the additive version of Moebius Inversion formula.

In the Fourth chapter, we are going to see the proof of Wedderburn’s Theorem, which says that a finite division ring is commutative. Also, this Chapter presents some importanttheorems of Artin, Zassenhaus and Cartan-Brauer-Hua.

### PREMILIARIES

**Definition 1.1**

A **Linear space** over a field F is a set v with the operation called vector addition defined on $V \times V \to V$ given by $(x, y) \to x + y$ and an operation called vector multiplication defined on $F \times V \to V$ given by $(\alpha, x) \to \alpha x$ satisfying the following conditions $\forall x, y, z \in V$ and $\alpha, \beta \in F$ .

i) $(x + y) + z = x + (y + z)$

ii) $x + y = y + x$

iii) there exists an element $0 \in V$ such that $x + 0 = 0 + x = x$

iv) for each $x \in V$ there exists an element $-x \in V$ such that

 ISSN: 2454-4248
12 – 15

$x+(-x)=(-x)+x=0$

v) $\alpha(x+y)=\alpha x+\alpha y$

vi) $(\alpha\beta)x=\alpha(\beta x)$

vii) $(\alpha+\beta)x=\alpha x+\beta x$

viii) $1.x=x$

**Definition 1.2**

Let $V$ be a vector space over $F$ and $W \subset V$ .Then $W$ is called a **subspace** of $V$ if

(i) $W$ is a subspace of the abelian group $V$ .

(ii) For each $a \in F$ and $w \in W$ , $aw \in W$

It is clear from the definition that $W$ is closed for addition and scalar multiplication and that the axioms for a vector space are satisfied .Thus $W$ is also a vector space over $F$

**Definition 1.3**

For any subset S of V, the intersection of all subspaces of V containing S is called the **subspace generated** by S. It is usually denoted by the symbol $L(s)$ .

**Definition 1.4**

If U and V are vector space over a field F then the mapping T of U into V is said to be a **Homomorphism** if,

i) $(u_1+u_2)T=u_1T+u_2T,\ \forall u_1,u_2 \in V$

ii) $(\alpha u_1)T=\alpha(u_1T)\ and \alpha \in F$

**Definition 1.5**

If T: U→V is homomorphism and one to one then T is called an **Isomorphism**.

**FINITE FIELDS**

**Definition 2.1**

A **field** is a set F with two binary operations + and × such that:

1. (F,+) is a commutative group with identity element 0.
2. (F-{0},×) is a commutative group with identity element 1.
3. The distributive law a(b+c)=ab+ac holds $\forall a,b,c \in F.$

**Example:**

R,Q,C,$Z_p$ for p a prime are fields with the usual operations of addition and multiplication.

**Definition 2.2**

A **subfield** of a field F is a subset of F which is itself a field with the same operations as F.

**Example:**

Q is a subfield of R. R is a subfield of c. $Z_p$ has no subfields (other than itself).

**Note 2.3**

1) The smallest positive number of 1's whose sum is 0 is called the **Characteristic** of the field.
2) The smallest subfield of a field is called the **Prime subfield** and it is either a $Z_p$ or a Q.
3) The number of elements in a field is the **Order** of that field.

**Definition 2.4**

A **Splitting field** for the polynomial p(X) over a field K is defined as, the smallest extension of K in which the polynomial can be completely factored into linear factors.

 ISSN: 2454-4248
12 – 15

**Lemma: 2.5**

Let F be a finite field containing a subfield K with q elements. Then F has $q^m$ elements, where $m = [F : K]$.

**Proof:**

F is a vector space over K, finite-dimensional since F is finite.

Denote this dimension by *m*.

Then F has a basis over K consisting of m elements, say $b_1, \ldots, b_m$.

Every element of F can be uniquely represented in the form $k_1b_1 + \cdots + k_mb_m$ (where $k_1, \ldots, k_m \in K$).

Since each $k_i \in K$ can take q values, F must have exactly $q^m$ elements.

We are now ready to answer the question:

"What are the possible cardinalities for finite fields?"

Hence the proof.

**Theorem: 2.6**

Let F be a finite field. Then F has $p^n$ elements, where the prime *p* is the characteristic of F and n is the degree of F over its prime subfield.

**Proof:**

Since F is finite, it must have characteristic *p* for some prime *p*.

Thus the prime subfield K of F is isomorphic to $F_p$.

By Theorem, and so contains *p* elements.

Applying Lemma yields the result.

So, all finite fields must have prime power order - there is no finite field with 6 elements, for example.

We next ask: does there exist a finite field of order $p^n$ for every prime power $p^n$? How can such fields be constructed?

We saw, in the previous chapter,

That we can take the prime fields $F_p$ and construct other finite fields from them by adjoining roots of polynomials.

If $f \in F_p[x]$ is irreducible of degree *n* over $F_p$, then adjoining a root of f to $F_p$ yields a finite field of $p^n$ elements.

However, it is not clear whetherwe can find an irreducible polynomial in $F_p[x]$ of degree *n*, for *every* integer *n*.

Hence the proof.

**IRREDUCIBLE POLYNOMIALS**

**Lemma: 3.1**

Let $f \in F_q[x]$ be an irreducible polynomial over $F_q$ of degree m.Then f divides $x^{q^n} - x$ if and only if mdivides n.

**Proof:**

First, suppose f divides $x^{q^n} - x$.

Let α be a root of f in the splitting field of fover $F_q$.

Then $\alpha^{q^n} = \alpha$, so $\alpha \in F_{q^n}$.

Thus $F_q(\alpha)$ is a subfield of $F_{q^n}$.

Since $[F_q(\alpha) : F_q] = m$ and $[F_{q^n} : F_q] = n$,

We have $n = [F_{q^n} : F_q(\alpha)]m$, so m divides n.

Conversely,

suppose m divides n.

Then by Theorem,

$F_{q^n}$ contains $F_{q^m}$ as a subfield. Let α be a root of f in the splitting field of fover $F_q$.

Then $[F_q(\alpha) : F_q] = m$, and so $F_q(\alpha) = F_{q^m}$.

Thus $\alpha \in F_{q^n}$, hence $\alpha^{q^n} = \alpha$, and so α is a root of $x^{q^n} - x \in F_q[x]$. Therefore, by Lemma,

f divides $x^{q^n} - x$.

 ISSN: 2454-4248
12 – 15

Hence the proof.

**Theorem: 3.2**

If f is an irreducible polynomial in $F_q[x]$ of degree m, then f has a root α in $F_{q^m}$. Moreover, all the roots of f are simple and are given by the mdistinct elements $\alpha, \alpha^q, \alpha^{q^2}, ....., \alpha^{q^{m-1}}$ of $F_{q^m}$.

**Proof:**

Let α be a root of f in the splitting field of fover $F_q$.

Then $[F_q(\alpha) : F_q] = m$

Hence $F_q(\alpha) = F_{q^m}$, and so $\alpha \in F_{q^m}$.

We now show that, if $\beta \in F_{q^m}$ is a root of f, then $\beta^q$ is also a root of f. Write $f = a_m x^m + ..... + a_1 x + a_0 (a_i \in F_q)$.

Then

$$f(\beta^q) = a_m \beta^{qm} + ..... + a_1 \beta^q + a_0$$
$$= a^q{}_m \beta^{qm} + ..... + a_1{}^q \beta^q + a^q{}_0$$
$$= (a_m \beta^m + ..... + a_1 \beta + a_0)^q$$
$$= f(\beta)^q = 0,$$

Using Lemma and Freshmen's Exponentiation.

Thus, the elements $\alpha, \alpha^q, \alpha^{q^2}, ....., \alpha^{q^{m-1}}$ are roots of f.

We must check that they are all distinct.

Suppose not, i.e. $\alpha^{q^j} = \alpha^{q^k}$ for some $0 \le j < k \le m-1$.

Raising this to the power $q^{m-k}$, we get $\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$.

It then follows from Lemma that f divides $x^{q^{m-k+j}} - x$.

By Lemma, this is possible only if m divides m − k + j, a contradiction since 0 < m − k + j < m.

This result gives us two useful corollaries.

Hence the theorem.

## II. CONCLUSION

While this results are related to finite fields, irreducible polynomials of finite fields and theorems of wedderburn, Artin, Zassenhaus and Carten-Brauer-Hua in a comprehensive manner.

Moreover, in this dissertation we have produced many facts, examples, wherever necessary, so that it will be easier to understand the concepts in the material.

We have given the list of references from where we have collected the details for this dissertation. I hope that the whatever the thing that are discussed in the dissertation will give be clear to the reader.

## BIBLIOGRAPHY

[1]. Emil Artin, ″ Uber einen Satz von Herrn J.H.MaclaganWedderburn, Hamb. Abb 5 (1928) pp. 245-250. Lang and J.T. Tate, Springer-Verlag, 1965, pp.301-306.

[2]. Loo-Keng Hua, Some Properties of a Sfield, Reprinted from the Proceedings of the National Academy of Sciences, vol. 35, no. 9, pp. 533-537.September, 1949, SELECTED PAPERS, Edited by H. Halberstam, Springer-Verlag, (1983), pp. 485-489.

[3]. Wedderburn's Theorem on Division Rings: A finite division ring is a field, http://math.colgate.edu/math320/dlantz/extras/wedderburn.pdf

[4]. Harry Goheen, The Wedderburn Theorem, Canadian Journal of Mathe-

a. matics, 1955, vol. 7, pp. 60-62.

[5]. L. Adleman, H. Lenstra, "Finding irreducible polynomials over finite fields", Proc. 18th Annual ACM Symp. on theory of computing, pp.350-355, 1986.