A STUDY ON FINITE FIELDS, IRREDUCIBLE POLYNOMIALS

A. Dinesh Kumar*, M. Vasuki & R. Prabhakaran*****

* Assistant Professor, Department of Mathematics, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Mathematics, Srinivasan College of Arts and Science, Perambalur, Tamilnadu

*** Assistant Professor, Department of Mathematics, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Cite This Article: A. Dinesh Kumar, M. Vasuki & R. Prabhakaran, "A Study on Finite Fields, Irreducible Polynomials", International Journal of Applied and Advanced Scientific Research, Page Number 85-93, Volume 1, Issue 1, 2016

Introduction:

In this paper we are going to see about finite fields, irreducible polynomials over finite fields, the proof of Wedderburn's little theorem and describe them in detail. All the materials presented in here are expository and taken from the various sources, listed in the reference. However, we have made effort to collect the basic concepts and results needed to understand the contents of the chapters and presented them in a self contained exposition. Also, we have provided, wherever we thought necessary, explanation and proofs for the results mentioned with very brief details in the source material. We also provided many examples throughout this paper.

Finite Fields:

Lemma 1:

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 $b_1, \dots, b_m$. Every element of F can be uniquely represented in the form $k_1b_1+\dots+k_mb_m$ (where $k_1, \dots, k_m \in K$). 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?"

Theorem 1:

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 4.5, and so contains p elements. Applying Lemma 6.1 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. The following two lemmas will help us to characterize fields using root adjunction.

Lemma 2:

If F is a finite field with q elements, then every $a \in F$ satisfies $a^q = a$.

Proof:

Clearly $a^q = a$ is satisfied for $a = 0$. The non-zero elements form a group of order $q - 1$ under multiplication. Using the fact that $a^{|G|} = 1_G$ for any element a of a finite group G, we have that all $0 \neq a \in F$ satisfy $a^{q-1} = 1$, i.e. $a^q = a$.

Lemma 3:

If F is a finite field with q elements and K is a subfield of F, then the polynomial $x^q - x$ in K[x] factors in F[x] as $x^q - x = \prod_{a \in F} (x - a)$ and F is a splitting field of $x^q - x$ over K.

Proof:

Since the polynomial $x^q - x$ has degree q, it has at most q roots in F. All the elements of F are roots of the polynomial, and there is q of them. Thus the polynomial splits in F as claimed, and cannot split in any smaller field. We are now ready to prove the main characterization theorem for finite fields.

Theorem 2: (Existence and Uniqueness of Finite Fields)

For every prime p and every positive integer n, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over F_p.

Proof:

(Existence) For q = p^n, consider $x^q - x$ in $F_p[x]$, and let F be its splitting field over F_p. Since its derivative is $qx^{q-1} - 1 = -1$ in $F_p[x]$, it can have no common root with $x^q - x$ and so, by Theorem 3.15, $x^q - x$ has q distinct roots in F. Let S = {a ∈ F : $a^q - a = 0$}. Then S is a subfield of F since

- S contains 0;
- $a, b \in$ S implies (by Freshmen's Exponentiation) that $(a-b)^q = a^q - b^q = a-b$, so $a-b \in$ S;
- for $a, b \in$ S and $b \neq 0$ we have $(ab^{-1})^q = a^q b^{-q} = ab$−1,

so $ab^{-1} \in$ S. On the other hand, $x^q - x$ must split in S since S contains all its roots, i.e its splitting field F is a subfield of S. Thus F = S and, since S has q elements, F is a finite field with $q = p^n$ elements. (Uniqueness) Let F be a finite field with $q = p^n$ elements. Then F has characteristic p and so contains F_p as a subfield. F is a splitting field of $x^q - x$. The result now follows from the uniqueness (up to isomorphism) of splitting fields. As a result of the uniqueness part of Theorem 6.5, we may speak of *the* finite field (or *the* Galois field) of q elements. We shall denote this field by F_q, where q denotes a power of the prime characteristic p of F_q.

Example 1:

- We constructed a field L = $F_3(\theta)$ of 9 elements, where θ is a root of the polynomial $x^2 + x + 2 \in F_3[x]$. L is *the* field of 9 elements, i.e. F_9.
- We constructed a field L = $F_2(\theta)$ of 4 elements, where θ is a root of the polynomial $x^2 + x + 1 \in F_2[^x]$. L is *the* field of 4 elements, i.e. F_4.
- We can also completely describe the subfields of a finite field F_q.

Theorem 3: (Subfield Criterion)

Let F_q be the finite field with $q = p^n$ elements. Then every subfield of F_q has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there is exactly one subfield of F_q with p^m elements.

Proof:

Clearly, a subfield K of F must have order p^m for some positive integer $m \leq n$. By known Lemma, $q = p^n$ must be a power of p^m, and so m must divide n. Conversely, if m is a positive divisor of n, then p^m−1 divides p^n−1, and so $x^{p^m-1} - 1$ divides $x^{p^n-1} - 1$ in $F_p[x]$. So, every root of $x^{p^m} - x$ is a root of $x^q - x$, and hence belongs to F_q. It follows that, F_q must contain a splitting field of $x^{p^m} - x$ over F_p as a subfield, and such a splitting field has order p^m. If there were two distinct subfields of order p^m in F_q, they would together contain more than p^m roots of $x^{p^m} - x$ in F_q, a contradiction. So, the unique subfield of F_pn of order p^m, where m is a positive divisor of n, consists precisely of the roots of $x^{p^m} - x$ in F_pn.

Example 2:

Determine the subfields of the finite field $F_2{}^{30}$. To do this, list all positive divisors of 30. The containment relations between subfields are equivalent to divisibility relations among the positive divisors of 30. (For diagram, see lectures!)

We can also completely characterize the multiplicative group of a finite field. For the finite field F_q, we denote the multiplicative group of non-zero elements of F_q by F^*_q .

Theorem 4:

For every finite field F_q, the multiplicative group F^*_q of nonzero elements of F_q is cyclic.

Proof:

We may assume $q \geq 3$. Set $h = q - 1$, the order of F^*_q, and let $h = p^{r1}{}_1\, p^{r2}{}_2 \ldots p^{rm}{}_m$ be its prime factor decomposition. For each i, $1 \leq i \leq m$, the polynomial $x^{h/pi} - 1$ has at most h/pi Roots in F_q. Since $h/pi < h$, it follows that there are nonzero elements of F_q which are not roots of this polynomial. Let a_i be such an element, and set $b_i = a_i^{h/\ pi^{ri}} = 1$. Now, $b_i^{pi^{ri}} = 1$, so the order of b_i divides p_i^{ri} and so has the form p_i^{si} for some $0 \leq s_i \leq r_i$. On the other hand, $b_i^{p_i^{r_i-1}} = a_i^{h/\ p_i} \neq 1$ so the order of b_i is precisely p_i^{ri} . Let $b = b_1 b_2 \ldots b_m$. We claim: b has order $h(= q - 1)$, i.e. is a generator for the group. Suppose, on the contrary, that the order of b is a proper divisor of h. It is therefore a divisor of at least one of the m integers h/p_i, $1 \leq i \leq m$; wlog, say of h/p_1. Then $1 = b^{h/p1} = b_1^{h/p1}\, b_2^{h/p1} \cdot \cdot \cdot\, b_m^{h/p1}$. Now, if $2 \leq i \leq m$, then p_i^{ri} divides h/p_1, and so $b_i^{h/p1} = 1$. This forces $b_1^{h/p1} = 1$. Thus the order of b_1 must divide h/p_1, which is impossible since the order of b_1 is p_1^{r1}. Thus F^*_q is a cyclic group with generator b.

Definition 1: A generator of the cyclic group F^*_q is called a *primitive element* of F_q. By Theorem 1.13, F_q contains ø(q − 1) primitive elements, where ø is Euler's function: the number of integers less than and relatively prime to q −1. Recall that, if the integer n has the prime factorization $p_1^{k1} p_2^{k2} \ldots p_r^{kr}$, then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}).....(1 - \frac{1}{p_r}).$$

Example 3:

- F_5 has Φ (4) = 2 primitive elements, namely 2 and 3.
- F_4 has Φ(3) = 2 primitive elements. Expressing F_4 as $F_4(\theta)=\{0,1,\theta,\theta+1\}$, where $\theta^2+\theta+1=0$, we find that both θ and θ + 1 are primitive elements.

We are now ready to prove an important result.

Theorem 5:

Let F_q be a finite field and F_r a finite extension field. Then

- F_r is a simple extension of F_q, i.e F_r = $F_q(\beta)$ for some β ∈ F_r;
- Every primitive element of F_r can serve as a defining element β of F_r over F_q.

Proof:

Let α be a primitive element of F_r. Clearly, $F_q(\alpha)$ ⊆ F_r. On the other hand, since $F_q(\alpha)$ contains 0 and all powers of α, it contains all elements of F_r. So F_r = $F_q(\alpha)$. So, we can express *any* finite field K with subfield F, by adjoining to F a root β of an appropriate irreducible polynomial f, which of course must have degree d = [K : F]. Although the proof of Theorem 6.12 uses a β which is a primitive element of K, it is not in fact necessary for β to be a multiplicative generator of K^*, as the next example shows.

Example 4:

Consider the finite field F_9. We can express F_9 in the form $F_3(\beta)$, where β is a root of the polynomial x^2+1, irreducible over F_3. However, since β^4 = 1, β does not generate the whole of F_9^*, i.e. β is not a primitive element of F_9.

Corollary 1:

For every finite field F_q and every positive integer n, there exists an irreducible polynomial in $F_q[x]$ of degree n.

Proof:

Let F_r be the extension field of F_q of order q^n, so that [F_r : F_q] = n. By Theorem 6.12, F_r = $F_q(\alpha)$ for some $\alpha \in F_r$. Then, by properties of minimal polynomials, the minimal polynomial of α over F_q is an irreducible polynomial in $F_q[x]$ of degree n.

Irreducible Polynomials:

Lemma 4:

Let $f \in F_q[x]$ be an irreducible polynomial over a finite field F_q and let α be a root of f in an extension field of F_q. Then, for a polynomial $h \in F_q[x]$, we have h(α) = 0 if and only if f divides h.

Proof:

The minimal polynomial of α over F_q is given by $a^{-1}f$, where a is the leading coefficient of f (since it is a manic irreducible polynomial in $F_q[x]$ having α as a root). The proposition then follows from part (ii) of known theorem.

Lemma 5:

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 m divides n.

Proof:

First, suppose f divides $x^{q^n}-x$. Let α be a root of f in the splitting field of f over 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 6.7, F_{q^n} contains F_{q^m} as a subfield. Let α be a root of f in the splitting field of f over 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 7.1, f divides $x^{q^n}-x$. We are now ready to describe the set of roots of an irreducible polynomial.

Theorem 6:

If f is an irreducible polynomial in $F_q\left[x\right]$ 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 m distinct 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 f over 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 β^q is also a root of f. Write $f=a_mx^m+.....+a_1x+a_0(a_i \in F_q)$. 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 6.3 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 ≤ j < k ≤ 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 7.1 that f divides $x^{q^{m-k+j}}-x$. By Lemma 7.2, 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.

Corollary 2:

Let f be an irreducible polynomial in $F_q\left[x\right]$ of degree m. Then the splitting field of f over F_q is F_{q^m}.

Proof:

Theorem 7.3 shows that f splits in F_{q^m}. To see that this is the splitting field, note that $F_q(\alpha,\alpha^q,....,\alpha^{q^{m-1}})=F_q(\alpha)=F_{q^m}$.

Corollary 3:

Any two irreducible polynomials in $F_q\left[x\right]$ of the same degree have isomorphic splitting fields. As we shall see later, sets of elements such as those in Theorem 7.3 appear often in the theory of fields.

Theorem 7:

For every finite field F_q and every n ∈ N, the product of all monic irreducible polynomials over F_q whose degrees divide n is equal to $x^{q^n}-x$.

Proof:

By Lemma 7.2, the monic irreducible polynomials over F_q which occur in the canonical factorization of $g=x^{q^n}-x$ in $F_q\left[x\right]$ are precisely those whose degrees divide n. Since g′ = −1, by Theorem 3.15 g has no multiple roots in its splitting field over F_q. Thus each monic irreducible polynomial over F_q whose degree divides n occurs exactly once in the canonical factorization of g in $F_q\left[x\right]$.

Example 5:

Take q = n = 2; the monic irreducible polynomials over $F_2\left[x\right]$ whose degrees divide 2 are $x, x+1$ and $x^2, x+1$. It is easily seen that $x(x+1)(x^2+x+1)=x^4+x=x^4-x$

Corollary 4:

If $N_q(d)$ is the number of monic irreducible polynomials in $F_q\left[x\right]$ of degree d, then

$q^n=\sum_{d/\,n} dN_q(d)$ for all $n \in N$, where the sum is extended over all positive divisors d of n.

Proof:

This follows immediately from Theorem, upon comparing the degree of $g = x^{q^n} - x$ with the total degree of the canonical factorization of g. This corollary allows us to obtain an explicit formula for the number of monic irreducible polynomials in $F_q[x]$ of a given degree. To do so, we need the following arithmetic function, which will also prove useful in the next chapter.

Definition 2: The Moebius function μ is the function on N defined by

$$\mu(n)=\begin{cases}1 & if\ n=1;\\ (-1)^k & if\ \ n\ \ is\ the\ \ product\ of\ k\ \text{distinct primes;}\\ 0 & \text{if n is divisible by the square of a prime;}\end{cases}$$

Example 6: μ(5) = −1; μ(35) = 1; (iii) μ(50) = 0.

Lemma 6:

For n ∈ N, the Moebius function satisfies $\sum_{d/n}\mu(d)=\begin{cases}1 & if\ \ n=1\\ 0 & if\ \ n>1.\end{cases}$

Proof:

The n = 1 case is immediate. For n > 1 we need only consider the positive divisors d of n for which μ(d) is non-zero, namely those d for which d = 1 or d is a product of distinct primes. If $p_1,......, p_k$ are the distinct prime divisors of n then

$$\sum_{d/n}\mu(d)=\mu(1)+\sum_{i=1}^{k}\mu(pi)+\sum_{1\le i_1<i_2\le k}\mu(pi_1pi_2)+.....+\mu(p1p2....pk)$$

$$=1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+......+\binom{k}{k}(-1)^k$$

$$=(1+(-1))^k=0.$$

Theorem 8: (Moebius Inversion Formula)

Additive Version: let h and H be two functions from N into an additively written abelian group G. Then $H(n)=\sum_{d/n}h(d)$ for all $n\in N$ ....(1) if and only if

$$h(n)=\sum_{d/n}\mu(\frac{n}{d})H(d)=\sum_{d/n}\mu(d)H(\frac{n}{d})\ \text{for all}\ \ n\in N\ \text{............(2)}$$

Multiplicative Version: let h and H be two functions from N into a multiplicatively written abelian group G. Then $H(n)=\prod_{d/n}h(d)$ for all $n\in N$ ....(3) if and only if

$$h(n)=\prod_{d/n}H(d)^{\mu(\frac{n}{d})}=\prod_{d/n}H(\frac{n}{d})^{\mu(d)}\ \ \text{for all}\ \ n\in N\ \ \text{...............(4)}$$

Proof:

Additive version: we prove the forward implication; the converse is similar and is left as an exercise. Assume the first identity holds. Using Lemma, we get

$$\sum_{d/n}\mu(\frac{n}{d})H(d)=\sum_{d/n}\mu(d)H(\frac{n}{d})=\sum_{d/n}\mu(d)\sum_{c/\frac{n}{d}}h(c)$$

$$=\sum_{c/n}\sum_{d/\frac{n}{c}}\mu(d)h(c)=\sum_{c/n}h(c)\sum_{d/\frac{n}{c}}\mu(d)=h(n)\ \text{for all n ∈ N.}$$

Multiplicative version: immediate upon replacing sums by products and multiples by powers.

Theorem 9:

The number $N_q(n)$ of monic irreducible polynomials in $F_q[x]$ of degree n is given by

$$N_q(n)=\frac{1}{n}\sum_{d/n}\mu(\frac{n}{d})q^d=\frac{1}{n}\sum_{d/n}\mu(d)q^{\frac{n}{d}}.$$

Proof:

Apply the additive case of the Moebius Inversion Formula to the group G = (Z, +). Take $h(n)=nN_q(n)$ and $H(n)=q^n$ for all n ∈ N. By Corollary 7.8, the identity (3.1) is satisfied, and so the result follows.

Remark: Since it is clear from this formula that $N_q(n)$ is greater than zero for all n, this gives an alternative proof of Theorem 9.

Example 7:

The number of monic irreducibles in $F_q\left[x\right]$ of degree 12 is given by

$$N_q(12) = \frac{1}{12}(\mu(1)q^{12} + \mu(2)q^{6} + \mu(3)q^{4} + \mu(4)q^{3} + \mu(6)q^{2} + \mu(12)q)$$
$$= \frac{1}{12}(1.q^{12} + (-1)q^{6} + (-1)q^{4} + 0.q^{3} + 1.q^{2} + 0.q)$$
$$= \frac{1}{12}(q^{12} - q^{6} - q^{4} + q^{2}) \cdot$$

We can also obtain a formula for the product of all monic irreducible polynomials in $F_q\left[x\right]$ of fixed degree.

Theorem 10:

The product I(q, n; x) of all monic irreducible polynomials in $F_q\left[x\right]$ of degree n is given by:

$$I(q,n;x) = \prod_{d/\ n}(x^{q^{d}} - x)^{\mu(\frac{n}{d})} = \prod_{d/\ n}(x^{q^{\frac{n}{d}}} - x)^{\mu(d)} \cdot$$

Proof:

From Theorem 6 we know that $x^{q^{n}} - x = \prod_{d/\ n} I(q,d;x)$

Now apply Moebius Inversion in the multiplicative form to the multiplicative group G of non-zero rational functions over F_q . Take h(n) = I(q, n; x) and $H(n) = x^{q^{n}} - x$ to get the desired formula.

Example 8:

Take q = 2 and n = 4. Then the product of all monic irreducible quartics in $F_2\left[x\right]$ is:

$$I(2,4;x) = (x^{16} - x)^{\mu(1)}(x^{4} - x)^{\mu(2)}(x^{2} - x)^{\mu(4)}$$
$$= \frac{x^{16} - x}{x^{4} - x} = \frac{x^{15} - 1}{x^{3} - 1}$$
$$= x^{12} + x^{9} + x^{6} + x^{3} + 1$$

A New Proof of Wedderburn's Little Theorem: (A Finite Division Ring is Commutative)

We will prove the well know fact that a finite division ring is commutative along the following lines. We start with a minimal counterexample L, viz. a finite division ring which is not commutative but all its maximal division subrings are commutative. We then prove that not all maximally commutative subgroups in these maximal subfields are eigenheimers. (A subgroup H of a group G ≠ H is called an eigenheimer of G if N $_G$ (H) = H). For if we suppose moreover that all maximal subfields are conjugate then by a simple counting argument the number of elements in these maximal subfields don't add up to the number of elements of the finite division ring L and if we assume that there are at least two different classes of conjugate maximal subfields then we find also by a simple counting argument that there are too many elements. From these two contradictions we can thus assume further that at least one of the maximally commutative subgroups, let us say M $^{\times}$, has a normalizer different from M $^{\times}$ and M $^{\times}$ is thus not an eigenheimer of L $^{\times}$. Thus there exists a maximal subfield, let us say N ≠ M, whose cyclic group N $^{\times}$ contains an element x ∈ N − Z that lies in the normalizer of M $^{\times}$ but not in M. We prove that the whole subgroup N $^{\times}$ lies in the normalizer of M $^{\times}$ by defining a left vectorspace V over the maximal subfield M spanned by a set Q of independent powers of x. We will see that the sum but also the product of two vectors is in V. So we find V = L. We then express the conjugate bases $gQg^{-1}, g^{2}Qg^{-2}, \ldots.$ in matrix form and we prove the contradiction that $g \in N_{L^{\times}}(M^{\times})$. So M is a normal subfield. According to a theorem of Cartan-Brauer-Hua M is in the center of L. A contradiction.

Proof:

We give a combinatorial proof, without making use of the complex numbers or permutation theory, of the following

Theorem 11:

Wedderburn's Little Theorem "A finite division ring L is commutative".

Proof:

Let L be a finite division ring. By definition L is an additive group which is abelian, and with zero element 0, and $L^{\times} = L - \{0\}$ is a multiplicative group, which need not to be commutative, with identity element 1. In addition the multiplication is left as well as right distributive over the addition: a(b +c) = ab + ac and (b + c)a = ba + bc for all elements a, b, c ∈ L.A field is a commutative division ring. The center Z of L, consisting of all elements z ∈ L which commutes with all elements a ∈ L is a subfield. L can be considered as a left vector space over Z. Thus there exists a unique prime p and natural numbers z and ℓ such that $|Z| = p^{z}$ and $|L| = p^{l}$ and z|ℓ. We use induction on the number n of elements of finite division rings. The theorem is true for n = 2. L contains only the two elements 0 and 1 and the multiplication is commutative. So we assume the theorem is true for finite division rings with less than n elements and we put n ≥ 3. Before we proceed with the proof we prove a useful theorem.

Theorem 12:

Let G be a non-commutative group with center Z and H a maximally commutative subgroup. Then Z ⊂ H.

Proof:

The subset HZ = ZH is a subgroup of G. Let $h_1, h_2 \in H$ and $z_1, z_2 \in Z$. Then $h_1z_1 \times h_2z_2 = h_1h_2z_1z_2 = h_3z_3 \in HZ$ and $(h_1z_1)^{-1} = z_1^{-1}h_1^{-1} = h_1^{-1}z_1^{-1} \in HZ$ and HZ is a subgroup of G. But HZ is also commutative for $h_1z_1 \times h_2z_2 = h_2z_2 \times h_1z_1$. Now H ⊂ HZ but H is a maximally commutative subgroup of G. Thus H = HZ and Z ⊂ H = HZ. We proceed with the main proof. We assume that L is a minimal counter example where the maximal division subrings of L are commutative and we that the groups of units are cyclic and by theorem 2 all the maximal division subrings contain the center Z of L. We see also that every element a ∈ L – Z lies in a unique maximal subfield (or otherwise it is an element of Z). We need a definition.

Definition 3: A subgroup H of a group G ≠ H is called an eigenheimer of G if the normalizer of H is equal to H: Thus $N_G(H) = H$.

Hypothesis 1:

For every maximal subfield M of L the normalizer of $M^{\times}$ in $L^{\times}$ is equal to $M^{\times}$, all the $M^{\times}$ are thus eigenheimers. We put for the moment |L| = ℓ, |M| = m, |N| = n, |Z| = z for division rings L,M,N,Z.

Contradiction: (i) Suppose that all maximal subfields are conjugate with M. Then

$$|L| = |Z| + \frac{l-1}{m-1}\,|M-Z| \ \text{ or } \ \ell = z + \frac{l-1}{m-1}\,(m-z) \text{ or } (\ell-z)(m-1) =$$

$$(\ell-1)(m-z) \text{ or } \ell m - \ell - zm + z = \ell m - \ell z - m + z \text{ or } \ell = m. \text{ But } \ell > m.$$

Contradiction: (ii) Suppose that there are two maximal subfields M and N which are not conjugate. Then

$$\begin{array}{ll} |L| \geq |Z| + \frac{l-1}{m-1}(m-z) + \frac{l-1}{n-1}(n-z) & \text{or} \\ \ell - z \geq 2\left(\frac{l-1}{m-1}\right)(m-z) & \text{or} \\ (\ell-z)(m-1) \geq 2(\ell-1)(m-z) & \text{or} \\ \ell m - \ell - zm + z \geq 2\ell m - 2\ell z - 2m + 2z & \text{or} \\ 2\ell z \geq \ell(m+1) + m(z-2) + z & \text{or} \\ 2\ell z \geq \ell(m+1) & \text{or} \\ 2z \geq m+1 > 2z & \text{or} \\ z > z. & \end{array}$$

But z = z. (We have assumed that $\frac{l-1}{m-1}(m-z) \leq \frac{l-1}{n-1}(n-z)$). From the contradictions (i) and (ii) it follows that Hypothesis 4 no longer holds and must be replaced by another hypothesis as we shall state in a moment. But first we prove a few group theoretic theorems:

Theorem 13:

Let G be a finite group and let H be a proper subgroup. Then $U_x \in G(xHx^{-1}) \neq G$

Proof:

Let |G| = g, |H| = h. Let $D = \bigcap_x \in G(xHx^{-1})$ and Let |D| = d ≥ 1.

Then |G : N $_G$ (H)| ≤ $\frac{g}{h}$ and thus (g − d) ≤ $\left(\frac{g}{h}\right)$(h − d) or h(g − d) ≤ g(h − d) or gd ≤ hd or g = h. A contradiction.

Theorem 14:

Let G be a finite non-commutative group. Then one of the maximally commutative subgroups is not an eigenheimer.

Proof:

Let H and K be maximally commutative subgroups of G and let H ≠ K. Let Z be the center of G. Then H ∩ K = Z. We call a subgroup H of a group G ≠ H an eigenheimer if the normalizer N $_G$ (H) = H. We assume that all maximally commutative subgroups are eigenheimers, otherwise we are done. Let |G| = g, |H| = h and |Z| = z. Suppose (i) that all maximally commutative subgroups are conjugate with H. Then (g–z) = $\frac{g}{h}$ (h–z) or g = h. A contradiction. Suppose (ii) that H and K are not congugate. We assume that the number $\left|U_x \in G(xHx^{-1})\right|$ is minimal. Then (g −z) ≥ $\frac{g}{h}$ (h–z) + $\frac{g}{k}$ (k −z) ≥ 2 $\frac{g}{h}$ (h −z) or h(g − z) ≥ 2g(h–z) or 0 ≥ hz +g(h–2z) ≥ hz. A contradiction. 3 From these two contradictions it follows that at least one of the maximally commutative subgroups, let us say H, is not an eigenheimer: N $_G$ (H) ≠ H.

Theorem 15:

Let G be a finite group and for every commutative subgroup H of G we have: N $_G$ (H) = C $_G$ (H). Then G is commutative.

Proof:

Suppose that G is non-commutative. Let H $_i$ be the maximally commutative subgroups of G. Then one of the maximally commutative subgroups, let us say H, is not an eigenheimer. Thus H < N $_G$ (H) = C $_G$ (H) ≠ H. Let c ∈ C $_G$ (H)–H then the group generated by H and c is commutative. Thus H is not maximally commutative. A contradiction. Thus G is commutative. We continue with the proof of theorem 1 by stating the following hypothesis which replaces hypothesis 4.

Hypothesis 2:

There exists a maximally commutative subgroup, let us say M $^\times$, whose normalizer N $_{L^\times}$ (M $^\times$) ≠ M $^\times$. Let x be an element of a maximal subfield N such that x ∈ N – Z and x is an element of N $_{L^\times}$ (M $^\times$). We call the smallest subfield of N containing x to be N $_1$. We are going to prove that N $_1$ = N but first we make a necessary detour. Now the commutative subgroup M $^\times$ is cyclic and is generated by an element, let us say m. Thus the elements $m, xmx^{-1} = m^i, x^2mx^{-2} = xm^ix^{-1} = (xmx^{-1})^i = m^{i^2}, ..., x^kmx^{-k} = m^{i^k}$ Are elements of M $^\times$ where k is minimal for x ^{k} to be an element of Z. Let n $_1$ be the multiplicative order of x. Thus $x^{n_1} - 1 = 0 = (x-1)(1 + x + x^2 + ... + x^{n_1-1})$, so the set of powers of x, $P = \{1, x, x^2, ..., x^{n_1-1}\}$ forms a dependent set of vectors in the space N $_1$ over Z. Let $Q = \{1, x, x^{i_3}, x^{i_4}, ..., x^{i_q}\}$ be a maximal independent set of vectors of P. which spans a left vector space N $_1$ over Z. Each power of x ∈ P can be written as a linear combination of the powers of x which are in Q. Then we consider the left vector space L over M with basis Q. So M ⊂ V ⊂ L. We shall prove V = L. Let V be the set of linear combinations $f(x) = \mu_1 + \mu_2 x + \mu_3 x^{i_3} + ... + \mu_q x^{i_q}$ with scalars from M. Let $g(x) = \mu'_1 + \mu'_2 x + \mu'_3 x^{i_3} + ... + \mu'_q x^{i_q}$ be a second linear combination with scalars from M. We define $(f+g)(x) := f(x) + g(x) = (\mu_1 + \mu'_1) + (\mu_2 + \mu_2')x + ... + (\mu_q + \mu'_q)x^{i_q}$ and we define $\mu f(x) := \mu\mu_1 + \mu\mu_2 x + ... + \mu\mu_q x^{i_q}$, where μ ∈ M, sothat V is a left vector space over M. To show that V is a division ring we see that the product f(x)g(x) is also a linear combination of the powers of x in Q after suitable simplifications: $f(x)g(x) = \sum\sum \mu_r x^{i_r} \mu'_s x^{i_s} = \sum\sum \mu'' x(i_r + i_s)$ where $\mu'' = \mu_r(x^{i_r}\mu'_s x^{-i_r})$. Now μ″∈ M and $x^{r+s} \in P$ and can thus be written as a linear combination of the powers of x which are in set

Q. We leave all the necessary details to the reader. V contains M and x and V = L. We now prove that N_1 = N. The maximal subfield N, which contains subfield N_1 has a cyclic subgroup $N-\{0\}$ which is generated by an element, let us say y. y is a linear combination of powers of x in Q with scalars in M. Let $y = \mu''_1 + \mu''_2 x + \mu''_3 x^{i_3} + ... + \mu''_q x^{i_q}$ y.

But $y = xyx^{-1} = (x\mu''_1 x^{-1}) + (x\mu''_2 x^{-1})x + (xm''_3 x^{-1})x^{i_3} + ... + (x\mu''_q x^{-1})x^{i_q})$. For all scalars μ″ r = xμ″ $\mu''_r = x\mu''_r x^{-1}$ sothat $\mu''_r \in Z$. All the scalars of y are in Z and y ∈ N_1. Thus N_1 = N. We make the last step in the main proof. Let $g \in L^\times - N_{L^\times}(M^\times)$. Recall that N ⊂ $N_{L^\times}(M^\times)$. Let $\underline{X} = \left[1, x, x^{i_3}, ..., x^{i_q}\right]^T$ and let $g\underline{X}g^{-1} = \left[1, gxg^{-1}, gx^{i_3}g^{-1}, ..., gx^{i_q}g^{-1}\right]^T$. Let $M_1 = \left[\mu^{(1)}{}_{ij}\right]$ be the matrix of order q × q with elements from M such that $M_1\underline{X} = g\underline{X}g^{-1}$. Let $M_i = \left[\mu^{(i)}{}_{ij}\right]$ be the matrix of order q×q with elements from M such that $M_i\underline{X} = g^i\underline{X}g^{-i}$. For i = 2 we have $M_2\underline{X} = g^2\underline{X}g^{-2} = g(g\underline{X}g^{-1})g^{-1} = g(M_1\underline{X})g^{-1} = gM_1g^{-1}(g\underline{X}g^{-1}) = gM_1g^{-1}M_1\underline{X}$. Because $\underline{X} \neq 0$ we have $M_2 = gM_1g^{-1}M_1$ so that $M_2M_1^{-1} = gM_1g^{-1}$. For $M_i = g^i\underline{X}g^{-i}$

We can write $M_i\underline{X} = g(g^{i-1}\underline{X}g^{-i+1})g^{-1} = gM_{i-1}\underline{X}g^{-1} = gM_{i-1}g^{-1}g\underline{X}g^{-1} = gM_{i-1}\underline{X}g^{-1}M_1\underline{X}$ and because $\underline{X} \neq 0$ we have: $M_i = gM_{i-1}g^{-1}M_1$. Thus $gM_{i-1}g^{-1}$ have only elements from M. Generally we have $M_{r+s} = g^sM_rg^{-s}M_s$ so that the elements of $g^sM_rg^{-s}$ are from M. Especially let H be the union of all the elements in the matrices $M_1, gM_1g^{-1}, g^2M_1g^{-2}, ...$ Then H ⊂ M and gHg^{-1} = H. Let H be the subgroup of $M^\times$ generated by the elements of H then H is cyclic and the only subgroup of $M^\times$ of order |H|. Besides gHg^{-1} = H. Every conjugate of $M^\times$ contains one conjugate of H and vice versa. Thus $N_{L^\times}(H) = N_{L^\times}(M^\times)$ so that $g \in N_{L^\times}(M^\times)$. A contradiction. Thus M is an normal subfield of L. However

Theorem 16:

Let L be a division ring with center Z and let M be a proper normal subfield of L. Then M ⊂ Z.

Proof:

Let ℓ ∈ L − M and m ∈ M − Z, then ℓm ≠ mℓ. Consider the following Identity of Hua (1949): $\ell = (m^{-1} - (\ell - 1)^{-1} m^{-1} (\ell - 1))(\ell^{-1} m^{-1} \ell - (\ell - 1)^{-1} m^{-1} (\ell - 1))^{-1}$ then we see that ℓ ∈ M sothat ℓm = mℓ. A contradiction. Thus L is commutative. By induction L is commutative.

Conclusion:

This paper provides the theorems related to finite fields, irreducible polynomials over finite fields and theorems of wedderburn, Artin, Zassenhaus and Carten-Brauer-Hua in a detailed manner. Also in this exposition we have seen many results on finite fields and irreducible polynomials. Moreover, in this paper we have produced many facts, examples, wherever necessary, so that it will be easier to understand the concepts in the material.

References:

1. Emil Artin, ″ Uber einen Satz von Herrn J. H. Maclagan Wedderburn, Hamb. Abb 5 (1928) pp. 245-250. I found it in Emil Artin Collected Papers, Edited by S. 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. I found it in Loo-Keng Hua, 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 Mathematics, 1955, vol. 7, pp. 60-62.
5. Michael Adam and Birte Julia Mutschler, On Wedderburn's Theorem about Finite Division Algebras, 23 Apr 2003, www.mathematik.uni-biele-feld.de/LAG/man/099.pdf