

---

---

Lecture Notes on

# Algorithmic Algebra

---

---

Jayalal Sarma M. N.  
Department of Computer Science and Engineering  
IIT Madras, Chennai 600036

Draft—August 7, 2015 and forever

# List of Scribes

Lecture 1	<i>Student</i>	1
Lecture 2	<i>Student</i>	7
Lecture 3	<i>Student</i>	9
Lecture 4	<i>Student</i>	14
Lecture 5	<i>stud</i>	15
Lecture 6	<i>stud</i>	16
Lecture 7	<i>stud</i>	17
Lecture 8	<i>stud</i>	18
Lecture 9	<i>stud</i>	19
Lecture 10	<i>stud</i>	20
Lecture 11	<i>stud</i>	21
Lecture 12	<i>stud</i>	22
Lecture 13	<i>stud</i>	23
Lecture 14	<i>stud</i>	24
Lecture 15	<i>stud</i>	25
Lecture 16	<i>stud</i>	26
Lecture 17	<i>stud</i>	30
Lecture 18	<i>stud</i>	31
Lecture 19	<i>stud</i>	32
Lecture 20	<i>stud</i>	33

# Table of Contents

<b>Lecture 1</b>	<b>Introduction, Motivation and the Language</b>	<b>1</b>
1.1	Overview of the course. Administrative, Academic policies . . . . .	1
1.2	The Basis Objects - Polynomials. . . . .	2
1.3	Three Representative Applications . . . . .	3
1.3.1	From Graph Algorithms : Perfect Matching . . . . .	3
1.3.2	From Number Theory : Primality Checking . . . . .	4
1.3.3	From Robotics : Robot motion planning. . . . .	5
1.4	Overview of the course . . . . .	6
<b>Lecture 2</b>	<b>Informal View and the Basic Algebraic Structures</b>	<b>7</b>
2.1	Another Example Application - Geometric Theorem Proving . . . . .	7
2.2	An Informal View . . . . .	8
2.3	Algebraic Preliminaries . . . . .	8
<b>Lecture 3</b>	<b>Polynomial Rings in one variable</b>	<b>9</b>
3.1	Ideals . . . . .	9
3.2	Polynomial Rings in one variable . . . . .	10
3.3	Polynomial division algorithm. . . . .	11
3.4	All Ideals in $F[x]$ are principal ideals . . . . .	12
<b>Lecture 4</b>	<b>GCD and the Generator of the Ideal</b>	<b>14</b>
4.1	Arriving at the definition of GCD and properties . . . . .	14
4.2	Euclidean Algorithm . . . . .	14
4.3	Termination & Correctness . . . . .	14
4.4	Solution to Ideal Membership Problem . . . . .	14
4.5	Monomial Ideals . . . . .	14
4.6	Dickson's Lemma . . . . .	14
<b>Lecture 5</b>	<b>Multivariate Multipolynomial Division and Applications</b>	<b>15</b>
5.1	Another Example Application - Geometric Theorem Proving . . . . .	15
5.2	An Informal View . . . . .	15
5.3	Algebraic Preliminaries . . . . .	15
<b>Lecture 6</b>	<b>From Dickson's Lemma to Hilbert Basis Theorem</b>	<b>16</b>
6.1	From Multivariate Polynomial Division Algorithm to Ideal Membership Problem . . . . .	16
6.2	Proof of Hilbert Basis Theorem . . . . .	16
6.3	Grobner Conditions for Basis . . . . .	16

6.4	Ideal Membership Problem with Grobner basis as Input . . . . .	16
<b>Lecture 7</b>	<b>Buchberger's Algorithm</b>	<b>17</b>
7.1	Constructing Counter-Examples to Grobner condition . . . . .	17
7.2	$S$ -polynomials and Buchberger's Criterion . . . . .	17
7.3	Buchberger's Algorithm - Correctness & Termination . . . . .	17
7.3.1	Ascending Chain Condition for Ideals . . . . .	17
7.4	Proof of Buchberger's criterion. . . . .	17
7.4.1	A structure Lemma for counter examples for Grobner condition . . . . .	17
<b>Lecture 8</b>	<b>Proof of Buchberger's criterion.</b>	<b>18</b>
8.1	A Structure Lemma . . . . .	18
8.2	A Proof by Contradiction . . . . .	18
<b>Lecture 9</b>	<b>Minimality, Elimination Theory</b>	<b>19</b>
9.1	Minimal and Reduced Grobner Basis . . . . .	19
9.2	Uniqueness of Reduced Grobner basis . . . . .	19
9.3	Elimination Theory and Elimination Ideals . . . . .	19
9.4	Grobner Basis for the Elimination Ideals . . . . .	19
<b>Lecture 10</b>	<b>An application of Monomial ordering</b>	<b>20</b>
10.1	Applications of Grobner Basis . . . . .	20
10.1.1	3-coloring via Grobner Basis . . . . .	20
10.2	Integer Programming . . . . .	20
10.2.1	Formulation as polynomials . . . . .	20
10.2.2	$\mathbb{F}$ -algebra homomorphism . . . . .	20
10.2.3	Kernel . . . . .	20
10.2.4	Testing membership in the image . . . . .	20
10.2.5	Bringing in optimisation . . . . .	20
<b>Lecture 11</b>	<b>Integer Programming using Grobner Basis</b>	<b>21</b>
11.1	Characterizing the Image . . . . .	21
11.2	Observations on the Grobner Basis . . . . .	21
11.3	Bringing in Optimality . . . . .	21
11.4	Remarks about generalizations . . . . .	21
<b>Lecture 12</b>	<b>From Root Finding to Factorization</b>	<b>22</b>
12.1	Number of Roots . . . . .	22
12.2	A Linear Algebraic Method - The companion Matrix . . . . .	22
12.3	From Roots to Factorization . . . . .	22
12.4	Informal Answers and the road ahead . . . . .	22
<b>Lecture 13</b>	<b>Unique Factorization Domains</b>	<b>23</b>
13.1	Irreducible vs Prime Elements of an Integral Domain . . . . .	23
13.2	A characterization of Unique Factorizability . . . . .	23
13.3	A Non-trivial Application - All Principal Ideal Domains are Unique Factorization Domains . . . . .	23

13.4 Gauss's Theorem . . . . .	23
13.4.1 All constant primes in $R$ are primes in $R[x]$ . . . . .	23
13.4.2 All non-constant irreducibles in $\mathbb{Z}[x]$ are irreducibles in $\mathbb{Q}[x]$ . . . . .	23
<b>Lecture 14 Irreducibility</b>	<b>24</b>
14.1 Completing Gauss's Theorem . . . . .	24
14.2 A Remark about Field of Fractions . . . . .	24
14.3 Eisenstein criterion for irreducibility . . . . .	24
<b>Lecture 15 Quotient Rings and First Isomorphism Theorem</b>	<b>25</b>
15.1 Quotient Rings and Irreducibility . . . . .	25
15.2 Quotient Rings and First Isomorphism Theorem . . . . .	25
15.3 Application 1 : Chinese Remaindering Theorem . . . . .	25
15.4 Application 2 : From Irreducibility to Field Extensions . . . . .	25
<b>Lecture 16 More on Fields</b>	<b>26</b>
16.1 Field Extensions as Vector Spaces . . . . .	26
16.1.1 Linear Independence, Basis, and Dimension . . . . .	26
16.1.2 Minimal Polynomials - viewing adjoining as a vector space . . . . .	27
16.2 Characteristic of Rings & Fields . . . . .	27
16.3 Sizes of Finite Fields . . . . .	28
16.4 Constructing Field Extensions . . . . .	28
16.5 Uniqueness of Fields up to isomorphism . . . . .	28
<b>Lecture 17 Warming up to Berlekamp's Factorization Algorithm</b>	<b>30</b>
<b>Lecture 18 Berlekamp's Lemma</b>	<b>31</b>
<b>Lecture 19 Berlekamp's Factorization Algorithm</b>	<b>32</b>
<b>Lecture 20 Berlekamp's Factorization Algorithm</b>	<b>33</b>
20.1 The Berlekamp Subalgebra $\mathbb{W}$ . . . . .	33
20.2 From Number of Irreducible Factors to Dimension . . . . .	33
20.3 Using $\mathbb{W}$ for factorization . . . . .	33
20.4 Constructing a basis for $\mathbb{W}$ - a linear algebraic approach . . . . .	33

# Preface

This lecture notes are produced as a part of the course *CS6842: Algorithmic Algebra* which was a course offered during August to November semester at IIT Madras.

## Acknowledgements

Thanks to Alexander Shrestov for creating a nice template for lecture notes which are being used in this document.

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* Student

*Date:* July 31, 2013

LECTURE

**1**

## Introduction, Motivation and the Language

General Comments.

### 1.1 Overview of the course. Administrative, Academic policies

## 1.2 The Basis Objects - Polynomials.



## 1.3 Three Representative Applications

### 1.3.1 From Graph Algorithms : Perfect Matching

### 1.3.2 From Number Theory : Primality Checking

### 1.3.3 From Robotics : Robot motion planning.

## 1.4 Overview of the course

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* Student

*Date:* Aug 2, 2013

LECTURE

**2**

## Informal View and the Basic Algebraic Structures

Preamble

### 2.1 Another Example Application - Geometric Theorem Proving

## **2.2 An Informal View**

## **2.3 Algebraic Preliminaries**

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* Student

*Date:* Aug 21, 2013

LECTURE

3

## Polynomial Rings in one variable

Preamble

### 3.1 Ideals

Examples. Principal Ideal. Polynomial Ideals.

## **3.2 Polynomial Rings in one variable**



Ideal generated by polynomials.

### **3.3 Polynomial division algorithm.**

### 3.4 All Ideals in $F[x]$ are principal ideals

Non-algorithmic proof. Need for an algorithm.

## GCD and the Generator of the Ideal

Preamble

4.1 Arriving at the definition of GCD and properties

4.2 Euclidean Algorithm

4.3 Termination & Correctness

4.4 Solution to Ideal Membership Problem

4.5 Monomial Ideals

4.6 Dickson's Lemma

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Aug 13, 2013

LECTURE

5

## Multivariate Multipolynomial Division and Applications

Preamble

**5.1 Another Example Application - Geometric Theorem Proving**

**5.2 An Informal View**

**5.3 Algebraic Preliminaries**

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Aug 20, 2013

LECTURE

6

## From Dickson's Lemma to Hilbert Basis Theorem

Preamble

- 6.1 From Multivariate Polynomial Division Algorithm to Ideal Membership Problem
- 6.2 Proof of Hilbert Basis Theorem
- 6.3 Grobner Conditions for Basis
- 6.4 Ideal Membership Problem with Grobner basis as Input

## Buchberger's Algorithm

Preamble

**7.1 Constructing Counter-Examples to Grobner condition**

**7.2  $S$ -polynomials and Buchberger's Criterion**

**7.3 Buchberger's Algorithm - Correctness & Termination**

**7.3.1 Ascending Chain Condition for Ideals**

**7.4 Proof of Buchberger's criterion.**

**7.4.1 A structure Lemma for counter examples for Grobner condition**

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Feb 6, 2013

LECTURE

8

## **Proof of Buchberger's criterion.**

Preamble

**8.1 A Structure Lemma**

**8.2 A Proof by Contradiction**



## Minimality, Elimination Theory

### Preamble

Minimal and Reduced Grobner Basis. Ideal Equality Problem. Uniqueness of Reduced Grobner basis. Elimination Theory and Elimination Ideals. Grobner Basis for the Elimination Ideals. Relating to the Robotics Arms problem.

### 9.1 Minimal and Reduced Grobner Basis

### 9.2 Uniqueness of Reduced Grobner basis

### 9.3 Elimination Theory and Elimination Ideals

### 9.4 Grobner Basis for the Elimination Ideals

## An application of Monomial ordering

### Preamble

Applications of Grobner Basis. 3-coloring via Grobner basis. Testing membership in Kernel and Image of Ring Homomorphisms. Applications to Integer Programming.

### 10.1 Applications of Grobner Basis

#### 10.1.1 3-coloring via Grobner Basis

### 10.2 Integer Programming

#### 10.2.1 Formulation as polynomials

#### 10.2.2 $\mathbb{F}$ -algebra homomorphism

#### 10.2.3 Kernel

#### 10.2.4 Testing membership in the image

#### 10.2.5 Bringing in optimisation

## Integer Programming using Grobner Basis

Proof of the characterization of the Image of the  $k$ -algebra homomorphism. Observation about the Grobner basis in the special case of integer programming. Defining the monomial ordering to bring in optimization. Proof of optimality of the solution.

### 11.1 Characterizing the Image

### 11.2 Observations on the Grobner Basis

### 11.3 Bringing in Optimality

### 11.4 Remarks about generalizations

## From Root Finding to Factorization

*Shorter Lecture:* From Root finding to factorization of polynomials. Why or when is a polynomial completely factorizable over the underlying ring/field? Why should they be unique factorizable? Informal answers, and directions to explore.

### 12.1 Number of Roots

### 12.2 A Linear Algebraic Method - The companion Matrix

### 12.3 From Roots to Factorization

### 12.4 Informal Answers and the road ahead

## Unique Factorization Domains

Irreducible and Prime Elements in an Integral Domain. Primes are irreducible. When is it that all irreducibles are primes? A proof that this is exactly when the domain is a UFD. A field is a UFD. Every principal Ideal Domain (example:  $F[x]$  and  $\mathbb{Z}$ ) is a UFD. What about rings like  $F[x_1, x_2]$ , and  $\mathbb{Z}[x]$ ? Gauss's theorem : If  $R$  is a UFD, then so is  $R[x]$ . Proof of the theorem using the characterization about irreducibles in  $R[x]$ . The case when the irreducibles are from  $R$  itself (Gauss's Lemma).

### 13.1 Irreducible vs Prime Elements of an Integral Domain

### 13.2 A characterization of Unique Factorizability

### 13.3 A Non-trivial Application - All Principal Ideal Domains are Unique Factorization Domains

### 13.4 Gauss's Theorem

#### 13.4.1 All constant primes in $R$ are primes in $R[x]$

#### 13.4.2 All non-constant irreducibles in $\mathbb{Z}[x]$ are irreducibles in $\mathbb{Q}[x]$

All primes in  $\mathbb{Q}[x]$  are primes in  $\mathbb{Z}[x]$

## Irreducibility

Continuing the proof of Gauss's theorem : The case when the irreducibles are from the  $\mathbb{R}[x]$ . Moving the argument to the Field of Fractions. Conclusion : Two tasks are well-framed.

- How do we detect irreducibility?
- How do we factorize into irreducible factors?

Eisenstein criterion for irreducibility.

### 14.1 Completing Gauss's Theorem

### 14.2 A Remark about Field of Fractions

### 14.3 Eisenstein criterion for irreducibility

## **Quotient Rings and First Isomorphism Theorem**

Quotient Rings. Irreducibility and Quotient Rings. First Isomorphism Theorem for the Quotient Ring. Application 1 : Chinese remaindering theorem. Application 2 : From Quotient Rings of Irreducible polynomials to Field extensions.

### **15.1 Quotient Rings and Irreducibility**

### **15.2 Quotient Rings and First Isomorphism Theorem**

### **15.3 Application 1 : Chinese Remaindering Theorem**

### **15.4 Application 2 : From Irreducibility to Field Extensions**

## More on Fields

Quick introduction to vector spaces. Viewing field extensions as vector spaces. Characteristic of a field. Sizes of fields. Constructing extensions and uniqueness of fields of a given size (up to isomorphism).

### 16.1 Field Extensions as Vector Spaces

A vector space over a field  $\mathbb{F}$  is a set  $V$  with two kinds of operations - addition and scalar multiplications - satisfying the following properties. Elements of  $V$  are called vectors and elements of  $\mathbb{F}$  are called scalars.

- $(V, +)$  forms an abelian group.
- If  $\alpha$  is a scalar, and  $v$  is a vector, then  $\alpha v$  is a vector.
- If  $\alpha$  is a scalar, and  $u$  and  $v$  are vectors, then  $\alpha(u + v)$  is the same vector as  $\alpha u + \alpha v$ .
- If  $\alpha_1, \alpha_2$  are scalars, and  $v$  is a vector, then  $\alpha_1(\alpha_2 v)$  is the same vector as  $(\alpha_1 \alpha_2)v$  where  $\alpha_1 \alpha_2$  is the multiplication in  $\mathbb{F}$ .

Some easy examples are the set of points in  $\mathbb{R} \times \mathbb{R}$ . Set of polynomials of degree  $d$  over a field  $\mathbb{F}$  forms a vector space with the natural notion of addition and multiplication.

Let  $E$  be a field and  $F$  be a subfield of it. One can view  $E$  as a vector space over  $F$ . To see this, view the elements of  $F$  as scalars and the elements of  $E$  as vectors in the above definition.

#### 16.1.1 Linear Independence, Basis, and Dimension

DEFINITION 16.1. A set of vectors  $v_1, v_2, \dots, v_k$  are said to be *linearly independent*, if:

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k = 0 \implies \alpha_1 = 0 \wedge \alpha_2 = 0 \wedge \dots \wedge \alpha_k = 0$$

For any set  $S$  of vectors, the set of vectors spanned by it, denoted by  $\text{SPAN}(S)$  is the set of vectors that can be expressed as the linear combination of vectors in  $S$ . A set  $S$  is said to be a basis of a vector space, if  $S$  itself is linearly independent and the  $\text{SPAN}(S)$  is the whole space.

We need two observations about the basis of a vector spaces and basis.

All basis of a vector space are of the same size. Suppose there is an  $S$  and an  $S'$  which forms the basis of the same vector space  $V$ , and  $|S| > |S'|$ . Since  $S$  and  $S'$  are subsets of  $V$  itself, the elements of  $S'$  **Jayalal says: This needs to be completed.**

Since all basis of a vector space are of the same size - it must be the case that.



### 16.1.2 Minimal Polynomials - viewing adjoining as a vector space

## 16.2 Characteristic of Rings & Fields

Consider the following Ring homomorphism from  $\mathbb{Z}$  to a ring  $R$ .

$$\phi : \mathbb{Z} \rightarrow R$$

where,  $\forall a \in \mathbb{Z}$ ,  $\phi(a) = |a|.1$  if  $a > 0$ , and  $\phi(a) = |a|.(-1)$  if  $a < 0$ . where  $n.1$  is simply a notation for adding the identity of the ring  $R$ ,  $n$  times to itself.

We will first check that it is a ring homomorphism. **Jayalal says: Yet to be written**

Let  $I$  be the kernel of this map. Since  $\mathbb{Z}$  is a principal ideal domain,  $I$  is singly generated and the generator is simply the least number in absolute value. Let  $\ell$  be the generator of the ideal. We know that the ideal  $I$  is simply  $\ell\mathbb{Z}$ . This  $\ell$  is called the characteristic of the ring  $R$ . In other words, *characteristic of a ring  $R$  with identity is simply the smallest number of times one needs to add 1 to get to 0*. Indeed, it is possible that adding the identity to itself never gets to 0 of the ring. In this case  $I = 0$  and  $\ell = 0$  - we say that the characteristic of the ring is 0.

We explore more properties that can be derived from this  $\ell$ . Let  $R'$  be the image of this homomorphism. We know that  $R'$  is a subring of  $R$ . Consider the quotient ring  $\mathbb{Z}/\ell\mathbb{Z}$  which is same as  $\mathbb{Z}_\ell$ . By the first isomorphism theorem we have the following:  $\mathbb{Z}_\ell \cong R'$ . In other words, if the characteristic of a ring  $R$  is  $\ell$ , then there is an isomorphic copy of  $\mathbb{Z}_\ell$  sitting inside  $R$  as a subring.

Now we turn to characteristic of a field. First of all let us argue that it can only be zero or a prime number.

**LEMMA 16.2.** *The characteristic of a field is either a prime number or zero.*

*Proof.* Let  $F$  be a field. Suppose the characteristic is not a prime and is  $\ell \in \mathbb{Z}$ . Assume for the contradiction that  $\ell$  is not prime.  $\ell = p.q$  where  $p, q < n$ . Indeed,  $\ell$  is least integer such that  $\ell.n = 0$ . Hence  $p.1 \neq 0$  and  $q.1 \neq 0$ . Since  $\phi$  is a homomorphism, associated with the  $\ell$  that we discussed above,  $\phi(pq) = \phi(p)\phi(q)$ . Since the LHS is 0,  $\phi(p)$  and  $\phi(q)$  forms zero divisors in  $\mathbb{F}$ . Thus, we have arrived at a contradiction and hence the lemma.  $\square$

**COROLLARY 16.3.** *Any finite field must have a subfield whose order is a prime number.*

*Proof.* Let  $F$  be a finite field. We first argue that the characteristic cannot be zero. If it is zero, then we know that the ideal  $I$  in the above discussion is the zero ideal and hence the quotient ring is  $\mathbb{Z}$  itself. Hence,  $\exists R' \subseteq F$  such that  $\mathbb{Z} \cong R'$ , which implies that  $\mathbb{F}$  must have infinite cardinality. Thus, characteristic can only be a prime number. Thus, an isomorphic copy of  $\mathbb{Z}_p$  for some prime  $p$  must be present in every field.  $\square$

## 16.3 Sizes of Finite Fields

We combine the ideas developed in the previous two sections to conclude that the sizes of finite fields cannot be arbitrary.

**LEMMA 16.4.** *The size of any finite field is always of the form  $p^d$  for some prime  $p$  and a non-negative integer  $d$ .*

*Proof.*  $\mathbb{Z}_p$  (for some prime  $p$ ) appears a subfield (up to isomorphism) of any finite field. Let  $d$  be the dimension of  $F$  as a vector space over  $\mathbb{Z}_p$ . That is, there is a subset  $S \subseteq F$  with  $|S| = d$ , which forms the basis of  $F$  over  $\mathbb{Z}_p$ . Let us say that  $S = \{a_1, a_2, \dots, a_d\}$ . Indeed, each vector (each element of  $a \in \mathbb{F}$ ) can be viewed as a  $d$ -tuple  $(\alpha_1, \alpha_2, \dots, \alpha_d)$  such that  $a = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_d a_d$ . Can two tuples represent the same  $a$ ? No, because it would mean then that  $\sum_i \alpha_i a_i = \sum_i \alpha' a_i$ . This contradicts the fact that  $S$  is linearly independent (since it forms a basis of  $\mathbb{F}$ ). Hence there are precisely  $p^d$  tuples possible, each of them representing distinct elements of  $\mathbb{F}$  as a vector space over  $\mathbb{Z}_p$ . Hence the size of the field  $\mathbb{F}$  must be exactly  $p^d$ .  $\square$

## 16.4 Constructing Field Extensions

For any  $p$  and  $d$ , is there a field of size  $p^d$ . We will answer this question positively.

Consider a polynomial  $p(x)$  of degree  $d$  that is irreducible over  $\mathbb{Z}_p$ . Let  $a$  be a root of such a polynomial. Clearly  $a \notin \mathbb{Z}_p$ . Consider the field  $\mathbb{Z}_p/\langle p \rangle$ . This is isomorphic to  $\mathbb{Z}_p(a)$  which also is a vector space over  $\mathbb{Z}_p$ .

We argue that the size of this finite field is precisely  $p^d$ . First of all, we argue that any element of the space  $\mathbb{Z}_p(a)$  can be viewed as a linear combination of elements in  $\{1, a, a^2, \dots, a^{d-1}\}$ . We do not need an  $a^d$  in this expression - indeed, it can be written as a combination of the other elements of lesser power since  $p(a) = 0$ . Suppose there is a linear combination of  $(1, a, a^2, \dots, a^{d-1})$  that goes to zero, that is  $a$  is a root of the polynomial of lesser degree than  $p(a)$ . But then there is a polynomial of degree less than  $p(x)$  which has  $a$  as the root.

## 16.5 Uniqueness of Fields up to isomorphism

We will be greedy, for any  $p$  and  $d$ , are there two non-isomorphic fields of size  $p^d$ ? We will answer this question negatively. So, we can always talk about *the* field of size  $p^d$ . **Jayalal says: Define splitting field etc.**

LEMMA 16.5. *The splitting field of a polynomial are always isomorphic to each other.*

*Proof.* **Jayalal says: Yet to be written**  $\square$

LEMMA 16.6. *For any field  $\mathbb{F}$ , there is a polynomial whose splitting field is  $\mathbb{F}$ .*

*Proof.* Let  $|\mathbb{F}| = k$ . Consider the multiplicative group  $\mathbb{F} - \{0\}$ . Let  $g$  be an element in this group. We know by Lagrange's theorem,  $g^{k-1} = 1$  where 1 is the multiplicative identity. Thus for all  $g \in \mathbb{F}$ ,  $g^k = g$ . Thus all of them are roots of the polynomial  $x^k - x$ , as a polynomial in  $\mathbb{F}[x]$ . Since this polynomial can have at most  $k$  roots, the polynomial completely splits in  $\mathbb{F}$  and it does not split in any subfield of  $\mathbb{F}$ . Hence  $\mathbb{F}$  is the splitting field of the polynomial  $x^k - x$ .  $\square$

By combining the above two lemmas, we get the main point of this section. That finite fields of a fixed size must be isomorphic.

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Sep 18, 2013

LECTURE

17

## Warming up to Berlekamp's Factorization Algorithm

Back to Factorization problem. A starting idea to use Fermat's little theorem to extract product of linear factors. Reduction to Squarefree case. Frobenius map ( $x^q = x$ ) and the sub-algebra of the quotient ring  $F[x]/f$ . Dimension of the sub-algebra when  $f$  is irreducible.

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Sep 10, 2013

# LECTURE 18

## Berlekamp's Lemma

Chinese remaindering. Berlekamp algebra  $W$  and its dimension. From an element in  $W$  to factorization - Berlekamp's Lemma.

CS6842 Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Sep 25, 2013

# LECTURE 19

## Berlekamp's Factorization Algorithm

Writing a set of linear equations and the Berlekamp Matrix. The  $O((qn^3)(n^2)(qn^2))$  time algorithm. Reducing the first factor of  $q$  by faster exponentiation. Removing the second factor of  $q$ . Identifying the minimal polynomial for the  $g(x)$ .

## Berlekamp's Factorization Algorithm

Computing the minimal polynomial of  $g(x)$ . Factorizing the minimal polynomial by Rabin's factorization method. Discussions on effect of choosing  $g(x)$  in  $\mathbb{W}$ , at random.

Berlekamp's Algorithm.

**20.1 The Berlekamp Subalgebra  $\mathbb{W}$**

**20.2 From Number of Irreducible Factors to Dimension**

**20.3 Using  $\mathbb{W}$  for factorization**

**20.4 Constructing a basis for  $\mathbb{W}$  - a linear algebraic approach**