
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>Jayalal Sarma M.N.</i>	1
Lecture 2	<i>Jayalal Sarma M.N.</i>	7
Lecture 3	<i>Jayalal Sarma M.N.</i>	9
Lecture 4	<i>Jayalal Sarma M.N.</i>	14
Lecture 5	<i>Jayalal Sarma M.N.</i>	18
Lecture 6	<i>Jayalal Sarma M.N.</i>	19
Lecture 7	<i>Jayalal Sarma M.N.</i>	20
Lecture 8	<i>Jayalal Sarma M.N.</i>	21
Lecture 9	<i>Jayalal Sarma M.N.</i>	22
Lecture 10	<i>Jayalal Sarma M.N.</i>	23
Lecture 11	<i>Jayalal Sarma M.N.</i>	24
Lecture 12	<i>Jayalal Sarma M.N.</i>	25
Lecture 13	<i>Jayalal Sarma M.N.</i>	26
Lecture 14	<i>Jayalal Sarma M.N.</i>	28
Lecture 15	<i>Jayalal Sarma M.N.</i>	29
Lecture 16	<i>Jayalal Sarma M.N.</i>	30
Lecture 17	<i>Jayalal Sarma M.N.</i>	35
Lecture 18	<i>Jayalal Sarma M.N.</i>	36
Lecture 19	<i>Jayalal Sarma M.N.</i>	37
Lecture 20	<i>Jayalal Sarma M.N.</i>	38

List of Instructors

Table of Contents

Lecture 1 Introduction, Motivation and the Language	1
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
Lecture 2 Informal View and the Basic Algebraic Structures	7
2.1 Another Example Application - Geometric Theorem Proving	7
2.2 An Informal View	8
2.3 Algebraic Preliminaries	8
Lecture 3 Polynomial Rings in one variable	9
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
Lecture 4 Graphs, Groups and Generators	14
4.1 Graph Isomorphism	14
Lecture 5 Multivariate Multipolynomial Division and Applications	18
5.1 Another Example Application - Geometric Theorem Proving	18
5.2 An Informal View	18
5.3 Algebraic Preliminaries	18
Lecture 6 From Dickson's Lemma to Hilbert Basis Theorem	19
6.1 From Multivariate Polynomial Division Algorithm to Ideal Membership Problem	19

6.2	Proof of Hilbert Basis Theorem	19
6.3	Grobner Conditions for Basis	19
6.4	Ideal Membership Problem with Grobner basis as Input	19
Lecture 7	Buchberger's Algorithm	20
7.1	Constructing Counter-Examples to Grobner condition	20
7.2	S -polynomials and Buchberger's Criterion	20
7.3	Buchberger's Algorithm - Correctness & Termination	20
7.3.1	Ascending Chain Condition for Ideals	20
7.4	Proof of Buchberger's criterion.	20
7.4.1	A structure Lemma for counter examples for Grobner condition	20
Lecture 8	Proof of Buchberger's criterion.	21
8.1	A Structure Lemma	21
8.2	A Proof by Contradiction	21
Lecture 9	Minimality, Elimination Theory	22
9.1	Minimal and Reduced Grobner Basis	22
9.2	Uniqueness of Reduced Grobner basis	22
9.3	Elimination Theory and Elimination Ideals	22
9.4	Grobner Basis for the Elimination Ideals	22
Lecture 10	An application of Monomial ordering	23
10.1	Applications of Grobner Basis	23
10.1.1	3-coloring via Grobner Basis	23
10.2	Integer Programming	23
10.2.1	Formulation as polynomials	23
10.2.2	\mathbb{F} -algebra homomorphism	23
10.2.3	Kernel	23
10.2.4	Testing membership in the image	23
10.2.5	Bringing in optimisation	23
Lecture 11	Integer Programming using Grobner Basis	24
11.1	Characterizing the Image	24
11.2	Observations on the Grobner Basis	24
11.3	Bringing in Optimality	24
11.4	Remarks about generalizations	24
Lecture 12	From Root Finding to Factorization	25
12.1	Number of Roots	25
12.2	A Linear Algebraic Method - The companion Matrix	25

12.3 From Roots to Factorization	25
12.4 Informal Answers and the road ahead	25
Lecture 13 Unique Factorization Domains	26
13.1 Irreducible vs Prime Elements of an Integral Domain	27
13.2 A characterization of Unique Factorizability	27
13.3 A Non-trivial Application - All Principal Ideal Domains are Unique Factorization Domains	27
13.4 Gauss's Theorem	27
13.4.1 All constant primes in R are primes in $R[x]$	27
13.4.2 All non-constant irreducibles in $\mathbb{Z}[x]$ are irreducibles in $\mathbb{Q}[x]$.	27
Lecture 14 Irreducibility	28
14.1 Completing Gauss's Theorem	28
14.2 A Remark about Field of Fractions	28
14.3 Eisenstein criterion for irreducibility	28
Lecture 15 Quotient Rings and First Isomorphism Theorem	29
15.1 Quotient Rings and Irreducibility	29
15.2 Quotient Rings and First Isomorphism Theorem	29
15.3 Application 1 : Chinese Remaindering Theorem	29
15.4 Application 2 : From Irreducibility to Field Extensions	29
Lecture 16 More on Fields	30
16.1 Field Extensions as Vector Spaces	30
16.1.1 Linear Independence, Basis, and Dimension	31
16.1.2 Minimal Polynomials - viewing adjoining as a vector space . .	31
16.2 Characteristic of Rings & Fields	31
16.3 Sizes of Finite Fields	32
16.4 Constructing Field Extensions	33
16.5 Uniqueness of Fields up to isomorphism	33
Lecture 17 Warming up to Berlekamp's Factorization Algorithm	35
Lecture 18 Berlekamp's Lemma	36
Lecture 19 Berlekamp's Factorization Algorithm	37
Lecture 20 Berlekamp's Factorization Algorithm	38
20.1 The Berlekamp Subalgebra \mathbb{W}	38
20.2 From Number of Irreducible Factors to Dimension	38

20.3 Using \mathbb{W} for factorization	38
20.4 Constructing a basis for \mathbb{W} - a linear algebraic approach	38

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

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

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

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.

Graphs, Groups and Generators

Preamble

4.1 Graph Isomorphism

DEFINITION 1. (Graph Isomorphism.) Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be graphs. We say $G_1 \cong G_2$ (read as G_1 is *isomorphic* to G_2) if there exists a bijection $\sigma : V_1 \rightarrow V_2$ such that $\forall (u, v) \in V_1 \times V_2$ we have

$$(u, v) \in E_1 \iff (\sigma(u), \sigma(v)) \in E_2$$

In other words, we say a graph G_1 is isomorphic to G_2 if there exists a relabeling of the vertices in G_1 such that the adjacency and non-adjacency relationships in G_2 is preserved.

OBSERVATION 1. If $|V_1| \neq |V_2|$ we have that G_1 is not isomorphic to G_2 .

The graph isomorphism problem is stated as follows.

PROBLEM : GRAPH ISOMORPHISM

Input : $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

Output : Decide if $G_1 \cong G_2$ or not.

A natural question to ask in this setting is that if there is an isomorphism from a graph G to itself.

Let $[n] = \{1, 2, \dots, n\}$. Let S_n denote the set of all permutations from the set $[n]$ to $[n]$.

DEFINITION 2. (Graph Automorphism.) Let $G = (V, E)$ be a graph. An automorphism of G is a bijection $\sigma : V \rightarrow V$ such that $\sigma(G) = G$. Let

$$Aut(G) = \{\sigma \mid \sigma \in S_n \text{ and } \sigma(G) = G\}$$

be the set of all automorphisms of G .

The graph automorphism problem is stated as follows.

PROBLEM : GRAPH AUTOMORPHISM

Input : A graph $G = (V, E)$

Output : Construct $Aut(G)$.

OBSERVATION 2. Let $\tau : [n] \rightarrow [n]$ be the identity permutation. That is, for all $i \in [n]$, $\tau(i) = i$. Then by definition $\tau \in Aut(G)$ for any graph $G = (V, E)$. This identity permutation τ is in $Aut(G)$.

Are there other permutations from $[n]$ to $[n]$ that are in the set $Aut(G)$? How large can the set $Aut(G)$ be ?

Formally, the graph rigidity problem is stated as follows.

PROBLEM : GRAPH RIGIDITY

Input : A graph $G = (V, E)$

Output : Decide if $Aut(G)$ is trivial or not.

OBSERVATION 3. Let G be the complete graph on n vertices. Then $|Aut(G)| = n!$.

Is the set $Aut(G)$ just a set or does it have more algebraic structure ?

DEFINITION 3. (Groups.) A set G together with a binary operation $*$ is said to be a group if the following four conditions are met

- **Closure :** $a, b \in G$, the element $a * b \in G$.
- **Associative :** For any $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.

- **Existence of Identity** : For any $a \in G$ there exists a unique element $e \in G$ such that $a * e = e * a = a$.
- **Existence of Identity** : For any $a \in G$ there exists a unique element $b \in G$ (denoted by a^{-1}) such that $a * b = b * a = e$.

EXAMPLE 1. • S_n forms a group under composition.

- $(\mathbb{Z}_5, +)$ is a group.

From now on, we will use the letter X to denote a graph and G to denote a group.

NOTATION 1. Let $(G, *)$ be a group. Let $H \subseteq G$ such that $(H, *)$ also forms a group. We say H is a *subgroup* of G and denote by $H \leq G$.

EXERCISE 1. For any graph X , the set $Aut(X)$ forms a group under the composition operation. That is, $Aut(G) \leq S_n$.

Let $(G, +)$ be a finite group and $g \in G$ be an element. Let $g^2 = g * g, g^3 = g * g * g$. Similarly $g^k = \underbrace{g * g * \dots * g}_{k \text{ times}}$. Now consider the set $H = \{g, g^2, g^3, \dots\}$. Since $(G, *)$

is a finite group there must exist a k such that $g^k = g$.

LEMMA 4.1. Let $(G, +)$ be a finite group and $g \in G$ be an element. Let $H = \{g, g^2, g^3, \dots\}$ be a set of elements. The unique identity e of G is in H .

Proof. By definition, $g^k = g^{k-1} * g = g$.

As $(G, *)$ is a group, we have the inverse of g^{-1} in G .

Therefore

$$g^{k-1} * g * g^{-1} = g * g^{-1} = e$$

□

NOTATION 2. Let $(G, +)$ be a finite group and $g \in G$ be an element. We say an element $g \in G$ is a generator of the set H if $H = \{g, g^2, g^3, \dots\}$ (denoted by $H = \langle g \rangle$).

OBSERVATION 4. H is a subgroup of G . That is, $H \leq G$.

EXAMPLE 2. • $\langle 1 \rangle = (\mathbb{Z}_5, +)$

DEFINITION 4. An group $(G, *)$ that can be generated by a single element is called a *cyclic group*. Example : $(\mathbb{Z}_5, +)$.

Not every group is cyclic. For instance S_3 is not cyclic.

DEFINITION 5. (Generatin set.)

CS6842 Algorithmic Algebra

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

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

Date: Feb 6, 2013

LECTURE 8

Proof of Buchberger's criterion.

Preamble

8.1 A Structure Lemma

8.2 A Proof by Contradiction

CS6842 Algorithmic Algebra

Date: Aug 28, 2013

LECTURE 9

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

CS6842 Algorithmic Algebra

Date: Sep 4, 2013

LECTURE 13

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 α is a scalar, and v is a vector, then αv is a vector.
- If α is a scalar, and u and v are vectors, then $\alpha(u + v)$ is the same vector as $\alpha u + \alpha v$.
- If α_1, α_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 16.2. 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 Characterestic 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 ℓ be the generator of the ideal. We know that the ideal I is simply $\ell\mathbb{Z}$. This ℓ is called the characterestic of the ring R . In other words, *characterestic 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 characterstic of the ring is 0.

We explore more properties that can be derived from this ℓ . 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}_ℓ . 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 ℓ , then there is an isomorphic copy of \mathbb{Z}_ℓ 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 16.3. *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 ℓ is not prime. $\ell = p.q$ where $p, q < n$. Indeed, ℓ is least integer such that $\ell.n = 0$. Hence $p.1 \neq 0$ and $q.1 \neq 0$. Since ϕ is a homomorphism, associated with the ℓ 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 16.4. *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 $Z \cong R'$, 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 16.5. *The size of any finite field is of 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 $\sum_i \alpha_i a_i = \sum_i \alpha'_i a_i$. 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 16.6. *The splitting field of a polynomial are always isomorphic to each other.*

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

LEMMA 16.7. *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

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

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

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