6.S897 Algebra and Computation	February 15, 2012

Lecture 3

Lecturer: Madhu Sudan *Scribe: Henry Yuen*

Of central importance to Algebra and Computation are structures such as groups, rings, and especially finite fields. Here, we review basic definitions and cover the construction of finite fields.

1 Basic definitions: Groups, rings, fields, vector spaces

Definition 1 (Group) *For a set G and an operator $\cdot : G \times G \to G$, a pair $(G, \cdot)$ is a group iff the following properties are satisfied:*

1. *(Identity) There exists $e \in G$ such that for all $a \in G$, $a \cdot e = a$.*
2. *(Associativity) For all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*
3. *(Inverses) For all $a \in G$, there exists an element $b \in G$ such that $a \cdot b = e$.*

We say a group $(G, \cdot)$ is commutative or Abelian iff for all $a, b \in G$, $a \cdot b = b \cdot a$. If $(G, \cdot)$ has an identity and satisfies associativity but not all elements have inverses is called a monoid.

Definition 2 (Ring) *For a set R and binary operators $\cdot$ and $+$ over R, the triple $(R, +, \cdot)$ is a ring iff the following properties are satisfied:*

1. *(Commutative addition with additive identity) $(R, +)$ is an Abelian group with identity element 0.*
2. *(Multiplication with multiplicative identity) $(R, \cdot)$ is a monoid with identity element 1.*
3. *(Distributivity) For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$.*

We say that a ring $(R, +, \cdot)$ is a commutative ring iff for all $a, b \in R$, $a \cdot b = b \cdot a$.

Definition 3 (Field) *A tuple $(F, +, \cdot)$ is a field iff the following properties are satisfied:*

1. *$(F, +, \cdot)$ is a ring.*
2. *$(F - \{0\}, \cdot)$ is an Abelian group.*

Definition 4 (Vector space) *V is a vector space over the field $\mathbb{F}$ if there is an addition operation $+ : V \times V \to V$ and an scalar multiplication operation $\cdot : \mathbb{F} \times V \to V$ such that:*

1. *(Closure under addition) $(V, +)$ is an Abelian group.*
2. *(Scalar distributivity) For all $a \in \mathbb{F}$, $u, v \in V$, $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$.*

Proposition 5 *All finite vector spaces V over a field $\mathbb{F}$ is isomorphic to $\mathbb{F}^n$ for some n.*

2 Finite Fields

Much of the course will be concerned with computation over finite fields. Here, we'll cover the basics of finite fields: existence, uniqueness, and construction.

2.1 Notation

All the fields discussed below will be finite. p and q will almost always denote a prime and a prime power (p^t for some prime p and positive integer t), respectively.

2.2 Prime fields

Definition 6 *A field $\mathbb{F}$ is prime if $|\mathbb{F}| = p$ for some prime p.*

Theorem 7 *For every prime p, a finite field of size p exists, and moreover, it is unique up to isomorphism.*

Proof Consider the quotient ring $\mathbb{Z}/p\mathbb{Z}$. It is a field, and a field of size p. Let $\mathbb{K}, \mathbb{L}$ be two fields of order p. For isomorphism, map $0_{\mathbb{K}}$ to $0_{\mathbb{L}}$, $1_{\mathbb{K}}$ to $1_{\mathbb{L}}$; it is clear that this mapping extends naturally and uniquely to an isomorphism. ■

Definition 8 *The characteristic of a finite field char($\mathbb{F}$) is the smallest integer n such that the multiplicative identity 1 added to itself n times is equal to the additive identity 0.*

2.3 Constructing Fields from Fields

Constructing non-prime fields is more interesting; we will actually construct them starting with prime fields. But before we get into that, let's look at how we can construct larger fields from smaller ones.

Definition 9 (Field of fractions) *Let R be an integral domain. The field of fractions $F(R) = R \times R/\sim$ where $\sim$ is an equivalence relation such that $a, b, c, d \in R$, $(a, b) \sim (c, d)$ if and only if $ad = bc$.*

Proposition 10 *The field of fractions $F(R)$ for an integral domain R is a field.*

Here are two primary ways of constructing fields from fields. Let $\mathbb{F}$ be a field, and let $\mathbb{F}[X]$ be the ring of polynomials with coefficients in $\mathbb{F}$.

1. $F(\mathbb{F}[X])$, the field of fractions, is called the field of *rational functions* over $\mathbb{F}$.
2. Let $g \in \mathbb{F}[X]$ be an irreducible polynomial. Then $\mathbb{F}[X]/(g)$ is a field.

2.4 Constructing Non-prime Fields

Lemma 11 *Let $\mathbb{F}$ be a finite field. Then it has prime characteristic.*

Fact 12 *Let $a, b \in \mathbb{F}$ where $\mathbb{F}$ has characteristic p. Then $(a+b)^{p^r} = a^{p^r} + b^{p^r}$ for any positive integer r.*

Lemma 13 *Let $\mathbb{F}$ be a finite field, with characteristic p. Then $\mathbb{F}$ is an $\mathbb{F}_p$-vector space.*

Corollary 14 *Let $\mathbb{F}$ be a finite field. Then $|\mathbb{F}| = p^t$ for some prime p and some positive integer t.*

Lemma 15 (Division Lemma) *Let f, g polynomials in $\mathbb{F}[X]$ for some finite field $\mathbb{F}$. Then there exists a unique pair $(q, r) \in \mathbb{F}[X]$ such that $\deg(r) < \deg(g)$ and $f = q \cdot g + r$.*

Corollary 16 *Let $f \in \mathbb{F}[X]$ have degree r. Then f has at most r roots in $\mathbb{F}$.*

Corollary 17 *Suppose $\mathbb{F}$ were some field of order q. Then $x^q - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha)$.*

Proof By the division lemma, $x^q - x$ has at most q roots in $\mathbb{F}$. It now suffices to show that for all $\alpha \in \mathbb{F}$, $x - \alpha$ divides $x^q - x$, or equivalently that α is a root. If $\alpha = 0$, then it is clear. Otherwise, note that non-zero α is contained in $\mathbb{F}^*$, the cyclic multiplicative group of $\mathbb{F}$, and by Lagrange's theorem $\alpha^q = \alpha$, and we are done. ■

Lemma 18 (Splitting Field Lemma) *For all $g \in \mathbb{F}[X]$, there exists a field extension $\mathbb{K}$ of $\mathbb{F}$ such that g splits completely into linear factors in $\mathbb{K}[X]$.*

Proof Suppose $\mathbb{F}$ were of order q. There are two cases: $g \in \mathbb{F}[X]$ is irreducible, or not irreducible. Support it were irreducible. Consider the quotient field $\mathbb{K} = \mathbb{F}[X]/(g)$; it is of size q^r where $r = \deg(g)$. Then by the above corollary, g splits completely into linear factors in $\mathbb{K}[X]$. If g were not irreducible, then we can write $g = ab$, where a is an irreducible polynomial and b is a nontrivial polynomial. Since a splits completely over $\mathbb{F}[X]/(a)$, we can then recurse on splitting b over an extension field of $\mathbb{F}[X]/(a)$, until we finally obtain a final extension field where g completely splits. ■

Definition 19 *Let $\mathbb{F} \subseteq \mathbb{K}$ be fields, and g a polynomial in $\mathbb{F}[X]$. Then $\mathbb{K}$ is called the splitting field of g over $\mathbb{F}$ if and only if g factors completely into linear polynomials in $\mathbb{K}[X]$.*

We will use the Splitting Field Lemma to construct our field of order q^r for any r.

Proposition 20 *Let $\mathbb{K}$ be a splitting field of $x^{q^r} - x$ over $\mathbb{F}_q$. Then $S = \{\alpha \in \mathbb{K} \mid \alpha^{q^r} = \alpha\}$ forms a field of order q^r.*

Lemma 21 (Unique containment) *Let $\mathbb{F}, \mathbb{G}$ be subfields of $\mathbb{K}$. If $|\mathbb{F}| = |\mathbb{G}|$, then $\mathbb{F} = \mathbb{G}$.*

Lemma 22 (Uniqueness of finite fields) *Let $\mathbb{F}_{p^r}$ be a finite field of order p^r as constructed above. It is unique up to isomorphism.*

Proof Let $\mathbb{K}, \mathbb{L}$ be finite fields of order p^r. Then both are splitting fields of the polynomial $x^q - x$, where we let $q = p^r$. The finite field $\mathbb{F}_p$ embeds uniquely into both $\mathbb{K}$ and $\mathbb{L}$. Let ϕ be the isomorphism between the copy of $\mathbb{F}_p$ in $\mathbb{K}$ and the copy in $\mathbb{L}$. Treating $\mathbb{K}$ and $\mathbb{L}$ as vector spaces of $\mathbb{F}_p$ where each element of the vector space is an ordered tuple of $\mathbb{F}_q$, it is clear that ϕ extends to an isomorphism $\tilde{\phi}$ between $\mathbb{K}$ and $\mathbb{L}$. ■

We've shown that if we are given an irreducible polynomial $g(x) \in \mathbb{F}_q[X]$ of degree r, then we can construct the unique field of size q^r. Now we show that such an irreducible polynomial of degree r always exists, and hence fields of all prime powers exist.

Lemma 23 *If g is an irreducible polynomial of degree r in $\mathbb{F}_q[X]$, then g divides $x^{q^r} - x \in \mathbb{F}_q[X]$.*

Proof Consider $\mathbb{K} = \mathbb{F}_q[X]/(g)$, which is a field of order q^r. The multiplicative group $\mathbb{K}^*$ is cyclic and has order $q^r - 1$, and by Lagrange's theorem $x^{q^r} \equiv x \mod g(x)$, and thus g divides $x^{q^r} - x$. ■

Lemma 24 *Let q be a prime power and r be some positive integer. Then:*

$$x^{q^r} - x = \prod_{\substack{g \text{ irreducible, monic } \in \mathbb{F}_q[X] \\ \deg(g) | r}} g(x)$$

Corollary 25 *For all prime power q, positive integer r, there exist an irreducible, monic polynomial $g \in \mathbb{F}_q[X]$ of degree r.*

Proof By the above lemma we have that $x^{q^r} - x$ is the product of monic, irreducible polynomials in $\mathbb{F}_q[X]$ with degree that divide r. Via a clever counting argument (which will be filled in the more polished version of these scribe notes later), there must exist a monic, irreducible g with degree exactly equal to r. ■

We have now shown that constructing $\mathbb{F}_q[X]/(g)$ for some irreducible, degree r polynomial g will give the unique finite field of order q^r, up to isomorphism.

Definition 26 (Minimal polynomial) *Let $\mathbb{K}$ be a finite field extension of $\mathbb{F}$. Let $\alpha \in \mathbb{K}$. Then the minimal polynomial of α over $\mathbb{F}$ is a monic, irreducible polynomial g of minimal degree in $\mathbb{F}[X]$ such that $g(\alpha) = 0$.*

3 Functions over finite fields

There is a nice way of looking at functions over finite fields as polynomials. Consider some function $f : \mathbb{F}_q \to \mathbb{F}_q$. f can be, without loss of generality, be represented as some univariate polynomial of degree at most $q - 1$ (this follows from polynomial interpolation).

A function $f : \mathbb{F}_{q^r} \to \mathbb{F}_q$ can be understood in a very nice way by first viewing f as some function $\tilde{f} : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ which just happens to map only into the smaller subfield $\mathbb{F}_q$. Then, as before, we can represent $\tilde{f}$ as a polynomial $\tilde{f}(x) = \sum c_i x^i$. However, since we know the range of $\tilde{f}$ is contained in $\mathbb{F}_q$, we have that

$$\left(\sum c_i x^i\right)^q = \left(\sum c_i x^i\right)$$

in $\mathbb{F}_{q^r}$.

Definition 27 (Trace) *The trace $Tr : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is defined as $Tr(x) = x + x^q + \cdots + x^{q^r - 1}$.*

Lemma 28 (Linearity of Trace) *Tr is linear.*