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. It should be noted that these notes should not be used to learn about groups, etc. for the first time.

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

Definition 1 (Monoid) *For a set G and an operator $\cdot : G \times G \to G$, a pair $(G, \cdot)$ is a monoid 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 $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

Definition 2 (Group) *A monoid $(G, \cdot)$ is a group iff 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 $a, b \in G$, $a \cdot b = b \cdot a$.*

Definition 3 (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) $(R, +)$ is an Abelian group with identity element 0.*
2. *(Multiplication) $(R, \cdot)$ 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 $a, b \in R$, $a \cdot b = b \cdot a$. A ring is an integral domain if it has no zero divisors.

Definition 4 (Field) *A tuple $(F, +, \cdot)$ is a field iff the following properties are satisfied:*

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

Definition 5 (Vector space) *A set V (whose elements are called* vectors*), along with a vector addition operation $+ : V \times V \to V$ and a scalar multiplication operation $\cdot : \mathbb{F} \times V \to V$, is a vector space over the field $\mathbb{F}$ iff the following properties are satisfied:*

1. *(Closure under addition) $(V, +)$ is an Abelian group.*
2. *(Scalar distributivity with respect to vector addition) For all $\alpha \in \mathbb{F}$, $u, v \in V$, $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$.*
3. *(Scalar distributivity with respect to field addition) For all $\alpha, \beta \in \mathbb{F}$, $u \in V$,$(\alpha + \beta)u = \alpha u + \beta u$.*
4. *(Field, vector space associativity): For all $\alpha, \beta \in \mathbb{F}$, $u \in V$,$\alpha(\beta u) = (\alpha\beta)u$.*
5. *(Identity field element): For all $u \in V$, $1 \cdot u = u$, where 1 is the multiplicative unit of $\mathbb{F}$.*

Proposition 6 *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. Symbols in the blackboard font will denote fields, e.g. $\mathbb{F}$. A subscript to a field symbol indicates the order of the field, e.g. $\mathbb{F}_p$ is a finite field of prime order.

2.2 Prime fields

Definition 7 *A field $\mathbb{F}$ is prime if $|\mathbb{F}| = p$ for some prime p.*

Theorem 8 *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 $1_{\mathbb{L}}$; since $\mathbb{K}^*$ and $\mathbb{L}^*$ (the multiplicative groups of $\mathbb{K}$ and $\mathbb{L}$ respectively) are cyclic groups, this mapping extends naturally and uniquely to an isomorphism between $\mathbb{K}$ and $\mathbb{L}$. ■

Definition 9 *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 10 (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 11 *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 12 *Let $\mathbb{F}$ be a finite field. Then it has prime characteristic.*

Proof Suppose $\mathbb{F}$ had characteristic $r = ab > 1$, where $a, b \neq 1$. That means the sum $0_{\mathbb{F}} = \overbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}^{r}$ can be divided up into a groups of $\beta = \overbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}^{b}$. By assumption, $\beta \neq 0_{\mathbb{F}}$. Then, $0_{\mathbb{F}} = \beta^{-1} \cdot 0_{\mathbb{F}} = \beta^{-1}(\overbrace{\beta + \cdots + \beta}^{a}) = \overbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}^{a}$, contradicting the minimality of r. ■

Fact 13 *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 14 *Let $\mathbb{F}$ be a finite field, with characteristic p. Then $\mathbb{F}$ is an $\mathbb{F}_p$-vector space.*

Proof This follows from the uniqueness of prime fields; we can think of $\mathbb{F}_q$ as being $\mathbb{Z}/p\mathbb{Z}$. Vector addition is the same as addition in $\mathbb{F}$, and scalar-vector multiplication is repeated addition in the obvious manner. ■

Corollary 15 *Let $\mathbb{F}$ be a finite field. Then $|\mathbb{F}| = p^t$ for some prime p and some positive integer t.*

Proof This follows from the earlier fact that all finite vector spaces over $\mathbb{F}$ are isomorphic to $\mathbb{F}^n$ for some n. ■

Lemma 16 (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 $f = q \cdot g + r$.*

Proof Existence of a pair (q, r) follows from the standard polynomial division algorithm. We now argue uniqueness: suppose there were two such pairs $(q, r) \neq (\tilde{q}, \tilde{r})$. Then $(q - \tilde{q}) \cdot g + (r - \tilde{r}) = 0$, but this is impossible, because if $q \neq \tilde{q}$, then $(q - \tilde{q}) \cdot g$ is a nonzero polynomial of degree greater than $r - \tilde{r}$, and if $q = \tilde{q}$ but $r \neq \tilde{r}$, then $r - \tilde{r}$ is also a nonzero polynomial, a contradiction. ■

Corollary 17 *Let $f \in \mathbb{F}[X]$. For all $a \in \mathbb{F}$, $f(x) \equiv f(a) \mod (x - a)$.*

Corollary 18 *Let $f \in \mathbb{F}[X]$ have degree r. Then f has at most r roots in $\mathbb{F}$.*

Proof This follows from the Division Lemma and the previous corollary: repeated division of f by $(x - r)$ for a root $r \in \mathbb{F}$ will eventually whittle f to either a constant or an irreducible polynomial. ■

Lemma 19 (Multiplicative group of finite fields are cyclic) *Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}^*$, the multiplicative group of $\mathbb{F}$, is cyclic.*

Proof Let $\mathbb{F}$ have order p^r for some prime p and positive integer r. The multiplicative group $\mathbb{F}^*$ has order $p^r - 1$. Let $\hat{p}$ be some prime that divides $p^r - 1$, and let $U_{\hat{p}}$ be the subgroup of elements of $\mathbb{F}^*$ whose orders are a power of $\hat{p}$. Clearly, by Lagrange's theorem, $U_{\hat{p}}$ has order q^s for some s. Suppose $U_{\hat{p}}$ were not cyclic. Then all elements of $U_{\hat{p}}$ must be roots of the polynomial $x^{q^{s-1}} - 1$ (by Lagrange's theorem), which contradicts the corollary above. Thus all subgroups of $\mathbb{F}^*$ of prime power order are cyclic. By the Fundamental Theorem of Abelian groups, we can write $\mathbb{F}^*$ as the direct sum $\mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_k}$, where each q_i are prime powers. The foregoing argument shows that any pair q_i and q_j $(i \neq j)$ must be coprime, and it is easy to see that the entire direct sum must be cyclic. ■

Corollary 20 *Let $\mathbb{F}$ be a field of order q. Then $x^q - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha)$.*

Proof $x^q - x$ 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 $\mathbb{F}^*$, which has order $q - 1$. By Lagrange's theorem $\alpha^q = \alpha$, and we are done. ■

We now are ready to construct our field of order $q = p^r$. To do so, we will construct a polynomial in $\mathbb{F}_p[X]$ whose roots all lie in an *extension field* of $\mathbb{F}_p$, and the extension field will have order q.

Definition 21 (Extension field) *Let $\mathbb{K}, \mathbb{L}$ be finite fields. $\mathbb{L}$ is an extension field of $\mathbb{K}$ iff $\mathbb{K} \subseteq \mathbb{L}$ and $\mathbb{L}$ is an $\mathbb{K}$-vector space. We denote the field extension as $\mathbb{L}/\mathbb{K}$.*

Frequently, however, we will also say that $\mathbb{L}/\mathbb{K}$ is a field extension even if $\mathbb{K}$ isn't technically a subset of $\mathbb{L}$, but rather, naturally embeds into $\mathbb{L}$. For example, an important method of constructing extension fields for us will be to take a field $\mathbb{F}$, and consider the quotient field $\mathbb{L} = \mathbb{F}[X]/(f)$ for some polynomial $f \in \mathbb{F}[X]$. Since $\mathbb{F}$ naturally embeds into $\mathbb{F}[X]$ which naturally embeds into $\mathbb{F}[X]/(f)$, we also say that $\mathbb{L}/\mathbb{F}$ is a field extension.

Lemma 22 *Let $\mathbb{F}$ be a field of order q. Let $f \in \mathbb{F}[X]$ be an irreducible, monic polynomial of degree r. Then the quotient ring $\mathbb{F}[X]/(f)$ is a field and has order q^r.*

Proof We provide a proof sketch. $\mathbb{F}[X]/(f)$ must be a field: there are both additive and multiplicative inverses, and since f is irreducible, the underlying ring of $\mathbb{F}[X]/(f)$ is an integral domain. Furthermore, it is a vector space over $\mathbb{F}$. Observe that $1, X, X^2, \ldots, X^{r-1}$ forms a basis for $\mathbb{F}[X]/(f)$, so $\mathbb{F}[X]/(f)$ must have dimension r and thus cardinality q^r. ■

Lemma 23 (Splitting Field Lemma) *For all $g \in \mathbb{F}[X]$, there exists a field extension $\mathbb{L}$ of $\mathbb{F}$ such that g splits completely into linear factors in $\mathbb{L}[X]$.*

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 $\mathbb{L} = \mathbb{F}[X]/(g)$; it is of size q^r where $r = \deg(g)$. Then by the above corollary, g splits completely into linear factors in $\mathbb{L}[X]$. 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 24 *Let $\mathbb{F} \subseteq \mathbb{L}$ be fields, and g a polynomial in $\mathbb{F}[X]$. Then $\mathbb{L}$ is called the splitting field of g over $\mathbb{F}$ if and only if g factors completely into linear polynomials in $\mathbb{L}[X]$.*

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

Proposition 25 *Let $\mathbb{L}$ be a splitting field of $x^{q^r} - x$ over $\mathbb{F}_q$. Then $S = \{\alpha \in \mathbb{L} \mid \alpha^{q^r} = \alpha\}$ forms a field of order q^r.*

Proof Since $\mathbb{L}$ is the splitting field of $g(x) = x^{q^r} - x$ over $\mathbb{F}_q$, we know that all of g's completely factors into linear polynomials over $\mathbb{L}[X]$. We now show that all the roots of g have multiplicity 1, establishing that there are q^r distinct roots of g in $\mathbb{L}$, and thus S has cardinality q^r. S is clearly a field. Suppose $\alpha \neq 0 \in \mathbb{L}$ is a root of g, and that for contradiction $(x-\alpha)^2$ divided g. Since 0 cannot be a double root of g (by inspection x^2 does not divide $x^{q^r} - x$), $(x-\alpha)^2$ must divide $g'(x) = x^{q^r-1} - 1$. However, $g'(x) \equiv r(x) \mod (x-\alpha)$, where $r(x) = \sum_{i=0}^{q^r-2} \alpha^{q-1-i} x^i$, but $r(\alpha) = (q^r - 1)\alpha^{q^r-2}$, which is not 0. ■

Lemma 26 (Unique containment) *Let $\mathbb{F}, \mathbb{G}$ be subfields of $\mathbb{K}$. If $|\mathbb{F}| = |\mathbb{G}|$, then $\mathbb{F} = \mathbb{G}$.*

Proof Let $\mathbb{K}$ have order p^r for some prime p. All subfields of $\mathbb{K}$ must have order p^k for $k \leq r$. Suppose $|\mathbb{F}| = |\mathbb{G}| = p^k$. Consider the polynomial $f(x) = x^{p^k} - x \in \mathbb{K}[X]$. All elements of $\mathbb{F}$ and $\mathbb{G}$ must be roots of f, but since f can have at most p^k roots in $\mathbb{K}$, $\mathbb{F} = \mathbb{G}$. ■

Lemma 27 (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 over $\mathbb{F}_p$ where each element of the vector space is an ordered tuple of $\mathbb{F}_p$, it is clear that ϕ extends to an isomorphism $\tilde{\phi}$ between $\mathbb{K}$ and $\mathbb{L}$. ■

We've shown a way to construct the unique field of order q for any prime power q. We now show a more direct method of creating $\mathbb{F}_q$.

2.5 Constructing finite fields via minimal polynomials

Definition 28 (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 $g(\alpha) = 0$.*

Definition 29 (Adjoining field elements) *Let $\mathbb{L}/\mathbb{K}$ be a finite field extension. For all $\alpha \in \mathbb{L}$, $\mathbb{K}(\alpha)$ denotes the minimal subfield of $\mathbb{L}$ that contains α. We say that $\mathbb{K}(\alpha)$ is the field formed by* ***adjoining*** *α to $\mathbb{K}$.*

Fact 30 *Let $\mathbb{L}/\mathbb{K}$ be a finite field extension, and $\alpha \in \mathbb{L}$. Then every element $a \in \mathbb{K}(\alpha)$ can be expressed as the sum $a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_k \cdot \alpha^k$ for some k, where $a_i \in \mathbb{K}$.*

Lemma 31 *Let $\mathbb{L}/\mathbb{K}$ be a finite field extension. Let g be the minimal polynomial for some $\alpha \in \mathbb{L}$ over $\mathbb{K}$. Then $\mathbb{K}(\alpha) \cong \mathbb{K}[X]/(g)$.*

Proof Write $g = g_0 + g_1X + g_2X^2 + \cdots + g_dX^d$. Then $\mathbb{K}[X]/(g)$ is a degree d field extension of $\mathbb{K}$, thus $|\mathbb{K}[X]/(g)| = q^d$ for $q = |\mathbb{K}|$. We argue that $|\mathbb{K}(a)| = q^d$ as well, and by the uniqueness of finite fields, this shows our lemma. $\mathbb{K}(\alpha)$ is an extension field over $\mathbb{K}$, and hence is a $\mathbb{K}$-vector space. $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ is a basis for $\mathbb{K}(\alpha)$: observe that every element of $\mathbb{K}(\alpha)$ can be written as $a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_k \cdot \alpha^k$ for some k, where $a_i \in \mathbb{K}$. For any $k \geq d$, the set $\{1, \alpha, \alpha_2, \ldots, \alpha^k\}$ is linearly dependent - the polynomial g gives the linear dependency. The set $\{1, \alpha, \alpha_2, \ldots, \alpha^{d-1}\}$ is linearly independent, for otherwise g would not be a minimal polynomial for α. Thus $\mathbb{K}(\alpha)$ is a $\mathbb{K}$-vector space of dimension d, and the conclusion follows. ■

Lemma 32 *Let g is an irreducible polynomial of degree s in $\mathbb{F}_q[X]$. Then g divides $x^{q^t} - x \in \mathbb{F}_q[X]$ if and only if s divides t.*

Lemma 33 *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 34 *For all prime power q, positive integer r, there exist an irreducible, monic polynomial $g \in \mathbb{F}_q[X]$ of degree r.*

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). Let us look at a particular class of functions f that map $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$. We can still write $f(x) = \sum_{i=0}^{q^r-1} c_i x^i$. Since we know the range of f is contained in $\mathbb{F}_q$, we have that

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

Since α is a root of $f^q - f$ for all $\alpha \in \mathbb{F}_{q^r}$, it follows that $x^{q^r} - x$ divides $f^q - f$, or equivalently $f^q = f \mod (x^{q^r} - x)$. We then note that

$$f(x)^q = \left(\sum c_i x^i\right)^q = \sum c_i^q x^{iq}.$$

We then can reduce x^{iq} modulo $x^Q - x$, where $Q = q^r$. This is easy to do because the roots of $x^Q - x$ are precisely $\mathbb{F}_Q$, and thus $x^{iq} = x^{iq \mod (Q-1)}$ modulo $(x^Q - x)$. Observe that the map $i \mapsto iq \mod (Q-1)$ is an invertible map for $i \leq Q-1$, and thus is a permutation. Setting coefficients of the equation $f^q = f \mod (x^Q - x)$ equal, we get that f maps $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ if and only if $c_{iq \mod (Q-1)} = c_i^q$.

We can look for the "simplest" such function by demanding that as many c_i's be zero as possible, without being trivial. This can be accomplished by setting $c_1 = 1$, but that forces (by the equivalent condition above) $c_{q^k} = 1$ for $k \leq r-1$. This leads us to a particularly important function that maps $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$, called the *trace*:

Definition 35 (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 36 (Linearity of Trace) *Tr is linear.*

Lemma 37 *Tr is a* q^{r-1}*-to-*1 *map.*

Proof Let $\alpha \in \mathbb{F}_q$. Then $\mathrm{Tr}(x) - \alpha$ is a polynomial that maps $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ with degree q^{r-1}, and thus it has at most q^{r-1} zeros. But that means every $\alpha \in \mathbb{F}_q$ has a preimage under Tr of size q^{r-1}: otherwise there would be elements of $\mathbb{F}_{q^r}$ that would not map to anything under Tr, which is absurd. ■

Perhaps a more interesting reason for why the trace function is important is because of its "universality" with respect to functions that map $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$, the following sense:

Theorem 38 *Let f be a function that maps $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$. Then there exists a polynomial $g \in \mathbb{F}_{q^r}[X]$ such that $f = Tr(g)$.*

Proof For each $\alpha \in \mathbb{F}_q$, define $t_\alpha \in \mathbb{F}_{q^r}$ to be such that $\mathrm{Tr}(t_\alpha) = \alpha$ (there are q^{r-1} choices to pick from; choose arbitrarily). Then, interpolate a polynomial g of degree $q^r - 1$ such that for each $\chi \in \mathbb{F}_{q^r}$, $g(\chi) = t_{f(\chi)}$. It is clear that $f = \mathrm{Tr}(g)$. ■