6.S897 Algebra and Computation Feb 17, 2015

Lecture 4

Lecturer: Madhu Sudan *Scribe: Akshay Degwekar*

In this lecture, we will review some of the basics of algebra for this course. Primarily we will cover three things - Factoring - When is it reasonable to think about Factorization? Then we will cover Finite fields and finally look at the Trace function.

This course assumes that you know concepts like Groups, Rings, Fields and Vector spaces over fields. We briefly review the definitions, but do not treat the topic in detail. We will mostly deal with enumerable objects and not fields like $\mathbb{R}$ - which require us to deal with imprecise calculation.

1 Basic Definitions

Definition 1 (Group) *A set G with an operator $\cdot : G \times G \to G$, is a* Group *iff it satisfies the following properties:*

1. *(Closure) For all $a, b \in G$, $a \cdot b \in G$.*[1]
2. *(Associativity) For all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*
3. *(Identity) There exists $e \in G$ such that for all $a \in G$, $e \cdot a = a \cdot e = a$.*
4. *(Inverse) For all $a \in G$ there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

A group is *Abelian* if $a \cdot b = b \cdot a$ for all $a, b \in G$. For the sake of brevity we now drop the $\cdot$.

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) $(R, +)$ is an Abelian group with identity element 0.*
2. *(Multiplication) $\cdot$ is closed and associative.*[2]
3. *(Distributivity) For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$.*

A ring $(R, +, \cdot)$ is a commutative *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 3 (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 4 (Vector space) *A set V (whose elements are called* vectors*), along with a addition $+ : V \times V \to V$ and a scalar multiplication $\cdot : \mathbb{F} \times V \to V$, is a vector space over the field $\mathbb{F}$ when the properties hold:*

1. *(Closure) $(V, +)$ is an Abelian group.*
2. *(Distributivity) For all $\alpha \in \mathbb{F}$, $u, v \in V$, $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$. and*
   For all $\alpha, \beta \in \mathbb{F}$, $u \in V$,$(\alpha + \beta)u = \alpha u + \beta u$.
3. *(Associativity): For all $\alpha, \beta \in \mathbb{F}$, $u \in V$,$\alpha(\beta u) = (\alpha\beta)u$.*
4. *(Identity): For all $u \in V$, $1 \cdot u = u$, where 1 is the multiplicative unit of $\mathbb{F}$.*

[1] This is redundant but we still state it

[2] Also called a semi-group

2 Factoring and Unique Factorization Domains

In this section we will only consider Unique Factorization Domains (UFDs) - they are subclasses of rings which admit unique factorizations. Here we assume that ring has an identity.

An element of a ring is a *unit* if it has an inverse. Also an element a is *reducible* if there exist non-unit elements b, c such that $a = bc$. An element is *irreducible* if it is not reducible.

Definition 5 (Unique Factorization Domain) *A UFD is an integral domain R in which every non zero element x of R can be written as a product of irreducible elements $x = p_1 p_2 \dots p_t$. This representation is unique upto permutation or multiplication by units.*

We now look at the first construction of a field from a ring. If R is an integral domain, then we can construct the ring of fractions denoted by $\tilde{R}$ as follows -

Definition 6 (Ring of Fractions) *The field $\tilde{R}$ is the set $R \times R/\{0\}$ where we represent elements as tuples (a, b) where $a \in R$ and $b \in R/\{0\}$ with the operations defined as -*

1. *(Equality) $(a, b) = (c, d)$ if and only if $ad = bc$.*

2. *(Addition) $(a, b) + (c, d) \stackrel{\text{def}}{=} (ad + bc, bd)$*

3. *(Multiplication) $(a, b) \cdot (c, d) \stackrel{\text{def}}{=} (ac, bd)$.*

We can do this for every ring. It is an easy exercise to show that if R is a UFD then $\tilde{R}$ is a Field.

3 Getting bigger fields from fields

We have seen one way of constructing Fields from rings, now we will see how to construct rings and fields via polynomials.

If we are given a field $\mathbb{F}$ we consider $\mathbb{F}[x]$ the ring of polynomials over $\mathbb{F}$. Also from the previous section, we know that the ring of fractions of $\mathbb{F}[x]$ that is the ring of rational functions over $\mathbb{F}$ will be a field if $\mathbb{F}[x]$ is a UFD. We claim that this is true.

Theorem 7 *If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ the ring of polynomials is a UFD.*

The proof proceeds from the "Division Algorithm" which says that for all $f, g \in \mathbb{F}[x]$ then $\exists! q, r$ such that $\deg(r) < \deg(g)$ such that $f = qg + r$

As an aside, this also gives us the notion of modular arithmetic in this ring and the idea of evaluation $f(\alpha)$ can be defined as the remainder when f is divided by $(x - \alpha)$. Furthermore from here we can argue that every degree d polynomial over a field has at most d roots.

A more general version of Theorem 7 stated below is due to Gauss.

Theorem 8 *If R is a UFD then $R[x]$ is a UFD*

Sketch of Proof To prove the theorem, we first observe that $\tilde{R}[x]$ is a UFD. This follows from the fact that $\tilde{R}$ is a field and then we apply Thm 7.

The meat of the proof is the so called *Gauss's Lemma* which we just state.

Lemma 9 (Gauss's Lemma) *For a polynomial $p \in R[x]$. If p has a non trivial factorization in $\tilde{R}[x]$ then it has a non trivial factorization in $R[x]$.*

Using Gauss's Lemma, we see that $R[x]$ has to be a UFD because $\tilde{R}[x]$ is a UFD. Since $\tilde{R}[x]$ is a UFD, there cannot be multiple factorizations for a polynomial in $R[x]$ because these would imply non-unique factorizations in $\tilde{R}[x]$ and that the existence of a factorization is guaranteed by the Gauss's lemma.
■

As an interesting fact, we note that this procedure not only gives us larger UFD's but also the Hensel's Lifting which we will encounter later in the course, allows a near black box translation of algorithms for factoring on R to give algorithms for factoring on $R[x]$. We have seen one way to construct bigger fields from fields - $\mathbb{F}(x)$ - the field of fractions. Now we see another way of constructing fields.

Consider a field $\mathbb{F}$ and an irreducible polynomial $g \in \mathbb{F}[x]$ and consider $\mathbb{F}[x]/g$ to be the polynomials modulo g. We claim that this is a field. This gives us a way to construct bigger Finite fields from smaller finite fields.

4 Finite Fields

For most of this course, we will deal with finite fields. We cover some of the basics here.

Let p be a prime and $q = p^t$ be a prime power. We denote fields like $\mathbb{F}$.

4.1 Prime fields

Prime fields are fields of a prime size. We show that for every prime p, there is a field of size p which is simply given by $\mathbb{Z}/p\mathbb{Z}$ that is the set of residues modulo p.

Theorem 10 *For every prime p, a finite field of size p exists, and moreover, it is unique up to isomorphism. We denote this field by $\mathbb{F}_p$.*

Definition 11 (Characteristic) *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*.*

Fields are said to be characteristic 0, if they do not have finite characteristic. All finite fields have a finite characteristic which is in fact a prime.

4.2 Representing Finite Fields

To perform computation efficiently, we want to succinctly represent the elements in a form amenable to algebraic manipulation. We will see three representations.

Vector Representation We can show that if $\mathbb{K}$ and $\mathbb{F}$ are finite fields such that $\mathbb{F} \subseteq \mathbb{K}$ then $\mathbb{K}$ is in fact a vector space over $\mathbb{F}$.

Also if we start with a finite field $\mathbb{K}$ such that $|K| = p^t$ then $\mathbb{F}_p \subseteq \mathbb{K}$ and hence the finite field has to have a size $|\mathbb{F}_p|^t$ for some t. We can now represent it as a vector over $\mathbb{F}_p$. This representation is succinct and can be used to efficiently perform addition but is inadequate for multiplication.

Matrix Representation Let $\alpha \in \mathbb{F}$. Now α defines a linear map from $\mathbb{F} to \mathbb{F}$ $\beta \to \alpha\beta$. So we can represent it as a matrix M_α.

This representation is good for both addition and multiplication because for $\alpha, \gamma \in \mathbb{F}$, $M_{\alpha+\gamma} = M_\alpha + M_\gamma$ and $M_{\alpha\gamma} = M_\alpha M_\gamma$. The representation is fairly compact - it takes $\log(|F|)^2$ bits.

4.3 Existence of Finite Fields

Constructing non-prime fields is more interesting; we will actually construct them starting with prime fields.

We will now prove the theorem that a finite field of size r exists if and only if $r = p^t$ for some prime p and natural number t.

The first attempt One way of showing this is to start with the observation that for a field $\mathbb{F}_p$ consider an irreducible polynomial of degree d and construct the field $\mathbb{F}[x]/g$. The size of this field will be p^d.

This approach works, but we need to show the existence of an irreducible polynomial for every degree. There is a sophisticated non constructive argument that does this.

But instead we here take a different approach. This requires us to introduce some machinery.

4.3.1 The right approach

First we start off with an observation.

Claim 12 *That if $g(y)$ is an irreducible polynomial in $\mathbb{F}[y]$ and $\mathbb{K} = \mathbb{F}[x]/g(x)$ be the field constructed. Then,*

$$(y - x)|g(y)$$

Proof Substitute $y = x$ to get $g(x) \bmod g(x) = 0$ and hence it is a factor. ■ Now we consider the notion

of a splitting field

Definition 13 (Splitting Field) *The splitting field of $g(x) \in \mathbb{F}[x]$ is the smallest field $\mathbb{K}$ such that $F \subseteq \mathbb{K}$ such that g splits into linear factors over $\mathbb{K}[x]$.*

Now we know from Claim 12 that splitting fields exist. Now for the construction. Suppose we want to construct a field of size $q = p^t$. Consider the polynomial $x^q - x$ over $\mathbb{F}[x]$. Let $\mathbb{K}$ be its splitting field. We consider the set of roots - $S = \alpha \in \mathbb{K} \mid \alpha^q - \alpha = 0$. We first see that $|S| \leq q$ because a polynomial has at most degree many roots. Also, we can observe that $|S| \geq q$ because it is the splitting field. And hence $|S| = q$. It is left as an exercise to show that the set S is a field and hence the exact field we want.

This completes the existence argument.

4.4 Additional properties of Finite fields

Theorem 14 *The multiplicative group over any finite field $\mathbb{F}$ is cyclic.*

Theorem 15 *All finite fields have generators. Let $\mathbb{F}, \mathbb{K}$ be finite fields such that $|\mathbb{K}| = |\mathbb{F}|^t$. Then $\exists \alpha \in \mathbb{K}$ such that the $\mathbb{F}$-span of $\{1, \alpha, \alpha^2, \dots \alpha^{t-1}\}$[3] spans $\mathbb{K}$.*

Theorem 16 *For field $\mathbb{K}$ of characteristic p, the unique embedding of $\mathbb{F}_p$ is given by the set $\{\alpha \in \mathbb{K} \mid \alpha^p = \alpha\}$*

5 Trace

Trace is an important function that maps a large field to its corresponding base field.

Definition 17 (Trace) *The trace $Tr : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is defined as $Tr(x) = x + x^q + \cdots + x^{q^{r-1}}$.*

A priori it is not clear why the trace should be in $\mathbb{F}_q$, to show that it is well defined, we consider $\mathrm{Tr}(\beta)^q = (\beta + \beta^q + \dots \beta^{q^{r-1}})^q = \beta^q + \beta^{q^2} + \dots \beta^{q^{r-1}} + \beta^{q^r} = \mathrm{Tr}(\beta)$.[4] Hence $\mathrm{Tr}(\beta) \in \mathbb{F}_q$.

Lemma 18 *Tr is linear. That is $Tr(x + y) = Tr(x) + Tr(y)$ and $Tr(\alpha x) = \alpha Tr(x)$*

Lemma 19 *Tr is a q^{r-1}-to-1 map.*

[3] $\mathbb{F}$-span is the linear span with scalars from $\mathbb{F}$

[4] We make use of the fact that $(a + b)^{p^t} = a^{p^t} + b^{p^t}$ in fields of characteristic p

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. ■

Trace also has a very nice composition property. If we denote the trace from field $\mathbb{K}$ to $\mathbb{F}$ by $\mathrm{Tr}_{\mathbb{K}\to\mathbb{F}}$ where $\mathbb{F} \subseteq \mathbb{K}$ then if $\mathbb{L}$ further extends $\mathbb{K}$ then we have

$$\mathrm{Tr}_{\mathbb{L}\to\mathbb{F}} = \mathrm{Tr}_{\mathbb{K}\to\mathbb{F}} \circ \mathrm{Tr}_{\mathbb{L}\to\mathbb{K}}.$$

So, trace has these nice properties and also trace is a very sparse polynomial and this has interesting consequences that we will see in the course.

Finally, trace allows us to represent a elements of a $\mathbb{K}$ in terms of $\mathbb{F}$ in the following way. If $\gamma_1, \gamma_2, \ldots \gamma_r$ in $\mathbb{K}$ are $\mathbb{F}$-linearly independent, then the function $\alpha \to (\mathrm{Tr}(\alpha\gamma_1), \mathrm{Tr}(\alpha\gamma_2), \ldots \mathrm{Tr}(\alpha\gamma_r))$ is a bijection. This bijection again is very nice with respect to addition and not so much for multiplication.

Acknowledgments Quite a few things in this scribe have been recycled from the scribed notes of the previous iteration of the course.