CSCI-B609: A Theorist's Toolkit, Fall 2016 Sept 29

Lecture 12: Fields and Polynomials

Lecturer: Yuan Zhou *Scribe: Adithya Vadapalli*

1 Introduction

In this lecture, we will talk about Fields and Polynomials. A quick recap - Field is a number system that includes the operations $\{+, -, \times, \div\}$. Ring is a number system that includes the operations $\{+, -, \times\}$. A group is a number system with one operation which satisfies the properties

1. Closure
2. Associativity
3. Identity Element
4. Inverse Element

In fact, every **Ring** is **Group** and every **Field** is a **Ring**. Fields can be both finite and infinite. However, in this lecture we will restrict ourselves to finite fields.

Remark 1. *Throughout this lecture p is a prime number.*

2 Fields

In this section we will introduce the concept of Fields.

Definition 1. *Fields are commutative groups with addition ('+') and multiplication ('×') with the properties.*

1. *Addition should have an identity element.*
2. *Multiplication (excluding 0) with identity $1 \neq 0$.*

By the properties of group both '+' and '×' have associativity and commutativity and are closed under these operations.

Few examples of fields are $\mathbb{Q}$ (Rational Numbers), $\mathbb{Z}$ (Integers), $\mathbb{R}$ (Real Numbers) etc. These are examples of infinite fields. As stated earlier, we will be restricting ourselves only to finite fields. With the help of the following Fact and Corollary, we will show the existence of finite fields.

Fact 1. *$gcd(p, q) = 1 \iff \exists a, b \in \mathbb{Z}$, such that $ap + bq = 1$*

Proof. The backward direction of the proof is easy to see. We will show the forward direction. Without loss of generality, we assume that $p \geq q$.

1. Case 1: $p = 1$, then $gcd(p, q) = 1$, we have $1.p + 0.q = 1$.
2. Case 2: $p > 1$, then $gcd(p, q) = gcd(q, p \bmod q) = 1$. By induction assume that $\exists u, v$ such that, $uq+vp = 1$. This implies, $uq+v(p-kq) = 1$. This results in $vp+(u-v)q = 1$.

□

The above proof is the so-called Extended Euclidean Algorithm.

Remark 2. *It will take* $\log(pq)$ *steps to reach the boundary condition,* $p = 1$.

Corollary 2. *For each $a \in \{1, 2, \cdots, p-1\}$, $\exists b \in \{1, 2, \cdots, p-1\}$, $k \in \mathbb{Z}$ such that, $ab + kp = 1$.*

We are now ready to define our first finite field.

Definition 3. $\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$ *under addition modulo p and multiplication is denoted as* $\mathbb{F}_p$.

We are now ready to show that $\mathbb{F}_p$ is a field.

Claim 1. *$\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ is a field where '+' is addition under modulo p, '×' is multiplication under modulo p.*

Proof. Closeness, associativity, commutativity, distributivity are straightforward. Additive Inverse of $a \in \mathbb{F}_p$ is $(p - a) \bmod p$. We only need to verify the existence of multiplicative inverse. From Corollary 2 we know that, $\exists b \in \{1, 2, \cdots, p-1\}$ and $k \in \mathbb{Z}$ such that, $ab + kp = 1$. Now since, $p \bmod p = 0$ we can get, $ab + k.0 = 1 \bmod p$. Which results in $ab = 1 \bmod p$. This implies b is the multiplicative inverse of a. □

3 Polynomials

Let $\mathbb{F}[x_1, x_2, \cdots, x_n]$ be the set of polynomials of $x_1, x_2, \cdots, x_n$ taken from $\mathbb{F}$. This means that all the coefficients of the polynomial are from the field $\mathbb{F}$.

Definition 4. *(Degree of the Polynomial). Total degree of the polynomial is the maximum degree of any monomial. Individual degree of x_i is the maximum degree of x_i in the polynomial.*

Example. Consider the polynomial $f(x_1, x_2, x_3, x_4) = c_1 x_1^3 x_2^4 + c_2 x_1^2 x_3 x_4^2$. Here the total degree of the polynomial is 7 and the degree of x_1 is 3.

Fact 2. *Given $A(x), B(x)$, There is unique $Q(x)$ and $R(x)$ such that,* $\deg(R) < \deg(A)$ *and* $B(x) = A(x)Q(x) + R(x)$.

The above fact corresponds to dividing $B(x)$ by $A(x)$.

Corollary 5. *There is an analog to the Euclidean Algorithm for two univariate polynomials $A(x)$ and $B(x)$. The output is the highest degree polynomial which divides both $A(x)$ and $B(x)$.*

We will now introduce the notion of irreducible polynomials.

Definition 6. *A polynomial $P(x)$ with* $\deg(P) > 1$ *is irreducible if and only if for any $Q(x)$ with* $0 < \deg(Q) < \deg(P)$*, $Q(x)$ does not evenly divide $P(x)$.*

Another way to view the above definition is with help of the above corollary. A polynomial $P(x)$ is irreducible if and only if, $gcd(P(x), Q(x)) = e \in \mathbb{F}$, e is the identity element, for any $Q(x)$ whose degree is less than $P(x)$.

Examples.

1. $P(x) = x^2 + x + 1$ is irreducible in $\mathbb{F}_2$ because $P(x) = x(x+1) + 1$.
2. $Q(x) = x^2 + 1$ is not irreducible in $\mathbb{F}_2$ because $Q(x) = (x+1)^2$.

4 Fields with Polynomials

Claim 2. *$\mathbb{F}$ is a finite field, then $\{\mathbb{F}[x]$ mod $P(x)\}$ is a field of size $|\mathbb{F}|^{\deg(P)}$*

Proof. (Sketch). Again as in Claim 1, the only non-straightforward thing to verify is the existence of a multiplicative inverse. One can extend the Extended Euclidean Algorithm

to polynomial $P(x), Q(x)$ and find $A(x), B(x)$ such that $A(x)P(x) + B(x)Q(x) = 1$ as long as the gcd of $A(x)$ and $B(x)$ is $e \in \mathbb{F}$ (Note that e is the identity element). Since $P(x)$ is irreducible, $gcd(P(x), Q(x))$ must be e for all $Q(x)$ with $\deg(Q) < \deg(P)$. □

Example. Let $\mathbb{F} = \mathbb{F}_2$, $P(x) = x^2 + x + 1$. The field $\{\mathbb{F}[x] \bmod P(x)\}$ is $\{0, 1, x, x + 1\}$. The multiplicative inverse of 1 is 1. x is $(x + 1)$ and $(x + 1)$ is x.

Fact 3. *Checking if $P(x)$ of degree l is irreducible is in deterministic* $\text{poly}(\log(p))$ *time.*

The following Fact gives us a way to pick random polynomials which are irreducible with a bounded probability.

Fact 4. *If we pick $P(x) = x^l + c_{l-1}x^{l-1} + \cdots + c_1x + c_0$ randomly, (note that $c_i \in \mathbb{F}$).* $\frac{1}{2l} \leq \Pr[P(x)$ *is irreducible*$] \leq \frac{1}{l}$

And in fact, asymptotically is $\sim \frac{1}{l}$.

The following theorem about irreducible polynomials generalizes the first example we showed for irreducible polynomials.

Theorem 7. *For $\mathbb{F} = \mathbb{F}_2$, $x^{2.(3k)} + x^{3k} + 1$ is irreducible for all $k \geq 0$.*

Now we will conclude the lecture about finite fields. In the next lecture we will talk about the roots of polynomials and the Schwartz-Zippel Lemma.