CS681	**Computational Number Theory**

Lecture 9: Uniqueness of $\mathbb{F}_{p^m}$

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

Last lecture we closed with two questions of existence and uniqueness of fields of order p^m. This lecture, we shall the question of uniqueness and also understand some other properties of extensions.

1 Some More Properties of Field Extensions

Firsly, we need to understand what quotienting means. Suppose we have a field K and we look at the polynomial ring over this field - $K[X]$. Let us take some irreducible polynomial f and look at $K[X]/(f(X))$. What does this mean?

Quotienting means that you consider all occurences of the ideal $(f(X))$ as zero. So in particular, if you look at $f(X)$ in this ring, it would be zero. Hence the variable X can now be thought of as a root of f.

Infact, this is exactly what we do to adjoin roots. Suppose we have a field K and we need to adjoin some element α. We take the minimum polynomial f of α and we look at $K[X]/(f(X))$. Here, essentially, X is α.

This is how we built $\mathbb{C}$. We looked at $\mathbb{R}[X]$ and quotiented it with the ideal generated by $X^2 + 1$. And now note that there is no real distinction between $-i$ or i. Algebraically, $\mathbb{R}(i) \cong \mathbb{R}(-i) = \mathbb{C}$. So the general point to note is that if α and β are both roots of the same irreducible polynomial f, then $K(\alpha) \cong K(\beta) \cong K[X]/(f(X))$.

1.1 Splitting Fields

Until we knew that an object called $\mathbb{C}$ existed, we had no idea if there was an element i such that $i^2 = -1$. So as such, it doesn't make sense to adjoin some element until you know where it is from. When you look at $K[X]/(f(X))$, we said that X can be identified with a root of f, but what root? Where is this root? I know it's not in K (for if it were, $X - \alpha$ is a factor of f and hence can't be irreducible), but where else is it?

This is where splitting fields come in.

Definition 1. *A splitting field of a polynomial f over K is the smallest field extension E/K that contains all the roots of f.*

Or equivalently, it's the smallest field E where the polynomial f factorizes into linear factors.

The first thing to note is that this is not equivalent to adjoining a root. To illustrate the difference, take the field $\mathbb{Q}$ and let us look at the polynomial $X^3 - 2$. This polynomial is irreducible and hence we can talk of the field $\mathbb{Q}[X]/(X^3 - 2)$ and identify the element X with a root of the polynomial say $\sqrt[3]{2}$.

But note that this is *not* the splitting field. The polynomial has other roots, namely $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ where ω is a primitive cube root of unity. And it is clear that $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of the reals and obviously cannot contain the complex number $\sqrt[3]{2}\omega$ and hence cannot be the splitting field of the polynomial.

The splitting field of this polynomial is $\mathbb{Q}(\sqrt[3]{2}, \omega)$ and is a degree 6 extension over $\mathbb{Q}$ whereas the extension by adjoining roots are degree 3 extensions over $\mathbb{Q}$.

An important theorem is the following:

Theorem 1. *If E and E' are two splitting fields of a polynomial $f(X)$ over K, then $E \cong E'$.*

We omit the proof, but nevertheless the theorem is important and will be used. Interested readers can refer any abstract algebra books for the proof of this fact.

1.2 The Frobenius Map

The binomial theorem takes a very simple form over $\mathbb{F}_p$. We know that

$$(X + Y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$$

Lemma 2. *For $i \neq 0, p$, the coefficient $\binom{p}{i}$ is divisible by p.*

Proof. The proof is quite obvious. The coeffient is

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdots (p-i+1)}{1 \cdot 2 \cdots i}$$

and the numerator has a factor of p and the denominator does not. And since this si an integer, the factor of p will remain uncancelled and hence will be divisible by p. □

This then tells us that in the field $\mathbb{F}_p$,

$$(X+Y)^p = X^p + Y^p$$

If you look at it as a automorphism (an isomorphism of $\mathbb{F}_p$ into itself), this shows the map $x \mapsto x^p$ is an automorphism of $\mathbb{F}_p$.

This map $\phi(x) = x^p$ is called the Frobenius map. It is a very important automorphism of finite fields and appears almost everywhere.

1.3 The Multiplicative Group of a Finite Field is Cyclic

Let K be a finite field of p^m elements. We shall show now that the multiplicative group $K \setminus \{0\}$ is a cyclic group.

Infact, we shall show a much stronger theorem.

Theorem 3. *Let K be any field (not necessarily finite) and let A be any finite subgroup of $K^\star = K \setminus \{0\}$. Then the subgroup A is cyclic. (That is, there exists an element $a \in A$ such that every other element in A is a power of a)*

Proof. Let $|A| = M$. We need to show that there exists an element in A of order M. Suppose not, let a be the element of highest order in A. Let the order of a be $m < M$.

Now pick any $x \in A$. We claim that the order of x must divide M. To prove this, let the order of x be n. Let the gcd of m and n be d.

By Euclid's lemma, there exists integers p, q such that $pn+qm = d$. Thus, let us look at the element $g = x^p a^q$. Then $g^m = x^{pm} a^{qm} = a^{qm} = d$ since $qm = d \bmod n$. And similarly $g^n = x^d$. Thus, the order of g is infact equal to $\frac{mn}{d} = lcm(m, n)$. And since we assumed that a was an element of maximum order, the lcm of m and n has to be m and therefore n has to divide m.

Having established this, we see that the order of every element must divide m and therefore $x^m = 1$ for every $x \in A$. And therefore, the polynomial $X^m - 1$ has every element of A as a root. But if we were to assume that $m < M$, then a polynomial of degree m would have $M > m$ roots! And this clearly cannot happen in a field. And therefore, $m = M$ and hence the group A is cyclic. □

2 Uniqueness of $\mathbb{F}_{p^m}$

Now we come to the proof that every field of p^m elements are isomorphic. So essentially, there is only 1 field of size p^m and hence would make sense

to refer to *the* field of size p^m as $\mathbb{F}_{p^m}$.To avoid cluttering of subscripts and superscripts, let $q = p^m$. We need to show that any two fields of size q are isomorphic.

Now let F be any field of order q. Then every element $a \in F$ satisfies the property that $a^q = a$. Hence in particular, every element of the field F is a root of $X^q - X$. And therefore, considering this polynomial over $\mathbb{F}_p$, F is a splitting field of $X^q - X$ over $\mathbb{F}_p$. And by a theorem stated earlier, all splitting fields of a polynomial are isomorphic. And therefore, any two fields of order q are isomorphic.

3 More about $X^q - X$

Here is a very important property of this polynomial $X^q - X$.

Theorem 4. *Let $Irr(K, d)$ be the set of all irreducible polynomials of degree d over K. Then, the following equation holds in $\mathbb{F}_p[X]$:*

$$X^{p^m} - X = \prod_{\substack{f \in Irr(\mathbb{F}_p, d) \\ d|m}} f(X)$$

Proof. We shall show that the LHS is equal to the RHS by comparing the roots on both sides. For the roots to first exist, we shall go to some large field.

Firstly, note the polynomial $X^q - X$ is satisfied by every element of $\mathbb{F}_q$. And by the same degree argument, the roots of the polynomial is precisely all the elements of $\mathbb{F}_q$. We shall first show that every element $\alpha \in \mathbb{F}_q$ is also a root of the RHS.

Since $\alpha \in \mathbb{F}_q$, pick up the minimum polynomial $f(X)$ of α over $\mathbb{F}_p$. We have seen earlier that this polynomial must be irreducible. Hence $\mathbb{F}_p[X]/(f(X))$ corresponds to the field $\mathbb{F}_p(\alpha)$. Let the degree of f be d.

We know that

$$\begin{aligned} [\mathbb{F}_q : \mathbb{F}_p] &= [\mathbb{F}_q : \mathbb{F}_p(\alpha)]\,[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \\ \implies m &= [\mathbb{F}_q : \mathbb{F}_p(\alpha)] \cdot d \\ \implies d \mid m & \end{aligned}$$

And hence, since the degree of this irreducible polynomial divides m, it appears in the product of the RHS as well.

The other way is easy too. Pick up any factor $f(X)$ on the RHS. Let its degree be d. Let α be one of the roots. Then we know that $\mathbb{F}_p(\alpha)$ must be the field $\mathbb{F}_{p^d}$. But since d divides m, this is a subfield of $\mathbb{F}_q$. And therefore every element of $\mathbb{F}_{p^d}$, in particular α, must be in $\mathbb{F}_q$ as well. $\square$

3.1 Extracting Factors

The formula outlined in the previous section is extremely useful in factoring. It helps us pull out factors of the same degree. We shall see a quick sketch here and discuss this in detail next class.

Let us say we have some polynomial f over $\mathbb{F}_p$. How do we extract all linear factors over $\mathbb{F}_p$? The idea is pretty simple. We know that $X^p - X$ splits as linear factors over $\mathbb{F}_p$. And more over, the formal derivative of it is $pX^{p-1} - 1 = -1 \neq 0$ and therefore it has no repeated roots as well.

Then, we have

$$g(X) = gcd(f, X^p - X)$$

Then if $\alpha \in \mathbb{F}_p$ was any root of f, then clearly since α also satisfies $X^p - X$, α will be a root of g as well. And more importantly, since $X^p - X$ is has no repeated roots, g will retain the same property as well. Hence every root of f over $\mathbb{F}_p$ appears exactly once in g.

Having removed all degree 1 factors, we can all extract degree 2 factors by taking the gcd with $X^{p^2} - X$.

We shall discuss this idea of factoring in detail soon.