CS681 **Computational Number Theory**

Lecture 8: More on Finite Fields

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

We will be spending some time on understanding the structure of fields of finitely many elements. In this class we shall some necessary properties that finite fields (or any field in general) should hold.

1 Characteristic of Finite Fields

Looking at the examples of fields that we know of, we clearly see that $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z}$ are different. Apart from just the cardinality properties, $\mathbb{Z}/p\mathbb{Z}$ has this property of k and $p-k$ cancelling off. Using this as a motivation, let us define what a characteristic of a field is. First we shall state it formally and then look at a better interpretation of it.

Definition 1. *For any ring R, there exists the identity element 1. Consider the homomorphism*

$$\begin{array}{rcl} \phi : \mathbb{Z} & \longrightarrow & K \\ n & \mapsto & n \cdot 1 \end{array}$$

where $n \cdot 1$ simple means adding 1, in R, n times. And $\mathbb{Z}$ being a PID, the kernel of this map will be of the form $m\mathbb{Z}$. This number m is called the characteristic of the field.

In other words, the characteristic is the smallest number m such that m times the identity element is zero.

However, it is possible that $m \cdot 1$ will never be zero. For example, take the rings like $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[x]$ etc. The corresponding map will hence have a trivial kernel and that is the ideal $0\mathbb{Z}$. Hence the characteristics of these rings is 0 and not infinity. This is just the language. Infact, we shall refer characteristic 0 rings as rings of infinite characteristic.

Here is a trivial lemma.

Lemma 1. *Let R be a ring (with identity) of characteristic m and S be a ring that contains R. Then characteristic of S is also m.*

Proof. R has characteristic m implies that $\phi : \mathbb{Z} \longrightarrow R$ has the kernel as $m\mathbb{Z}$. The homomorphism works just on the identity element of R and hence would be exactly the same on S (since S has to share its identity element with R). Thus, since the homomorphism is the same, the kernel has to be the same. □

1.1 Characteristic of Fields

Now, suppose m is the characteristic of any ring R. Then by definition the kernel of the map ϕ is $m\mathbb{Z}$. And by the isomorphism theorem, we know that the following map is injective:

$$\hat{\phi} : \mathbb{Z}/m\mathbb{Z} \longrightarrow R$$

And therefore, in a way, a copy of $\mathbb{Z}/m\mathbb{Z}$ is sitting inside R. Thus, $\mathbb{Z}/m\mathbb{Z}$ is a subring of R.

Now let us look at the characteristic of fields instead of rings. Let us take the identity element and just keep adding it. Either, for some m we have $m \cdot 1 = 0$ or it just keeps going on. If it becomes 0, we know that the field has characteristic m. The other case is the characteristic 0 case.

Now, can it be possible that m is composite? Suppose $m = pq$ where both $p, q < m$. Since we know that $m \cdot 1 = 0$, this means that $(p \cdot 1)(q \cdot 1) = pq \cdot 1 = 0$. And by our assumption, we know that neither $p \cdot 1$ nor $q \cdot 1$ is zero; we just showed the existence of zero divisors in a field! That is not possible. Hence summarizing as a theorem:

Theorem 2. *Any field F must either have 0 characteristic or a characteristic that is a prime.*

Let us pick any field F whose characteristic is a prime p. We know that if we let 1 'generate' a subfield of its own by just adding itself, it would get to $\mathbb{Z}/p\mathbb{Z}$. Thus for any field of prime characteristic, it should contain $\mathbb{Z}/p\mathbb{Z}$. We shall refer to $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

For a field of infinite characteristic (characteristic 0, just language), 1 would keep being added on without ever giving a 0. Thus it would generate the entire set of positive integers. And since additive inverses should exist, the negative integers should also belong to the field. And further, because of the multiplicative inverses, all rational numbers should exist. Hence, every field either contains $\mathbb{F}_p$ or $\mathbb{Q}$.

Please keep in mind that finite characteristic does not mean finite cardinality. As a counter example, look at the following set:

$$\mathbb{F}_p(X) = \left\{ \frac{f(X)}{g(X)} \ : \ f, g \in \mathbb{F}_p[X], g \neq 0 \right\}$$

that the set of rational functions over one variable. This field has infinite cardinality and since it contains $\mathbb{F}_p$ has characteristic p.

2 Order of Finite Fields

Now let us take any finite field K. Then this field must have characteristic that is not zero. Why? Since if it did have characteristic zero, it would contain $\mathbb{Q}$ and hence be infinite.

Since the characteristic of this field is finite, say p, it contains $\mathbb{F}_p$. Recall that if K is a field that contains another field F (in our case $\mathbb{F}_p$), then K is an extension of F.

Thus, this tells us that any field of characteristic p is a vector space over $\mathbb{F}_p$. Since we now have a vector space, we can talk of the dimension of this vector space. The dimension cannot be infinite. Why? For it it was, then the basis, which belongs to K, would be an infinite set. And this is an obvious contradiction since we assumed that K was finite.

Thus, the dimension of K over $\mathbb{F}_p$ is finite, say s. And since every element of K can be written as a s-tuple of elements of $\mathbb{F}_p$, this means that the number of elements of K is p^s.

And, from our earlier theorem, we know that the characteristic of a finite field has to be a prime. Hence the order of any finite field has to be a power of a prime.

Theorem 3. *Any finite field has p^s elements where p is a prime and s a positive integer.*

The moment we make such a statement, we have two questions in mind.

- Existence: For every prime p and positive integer s, do we have a field of p^s elements?
- Uniqueness: Can we have two different fields with p^s elements?

We shall soon see that the answer to the first question is yes and the second is no. There is exactly one field of size p^s.

2.1 Creating Extensions of $\mathbb{F}_p$

The general question is how to obtain extension fields of a given field. As a motivation, let us look at $\mathbb{R}$. How do we get an extension field of $\mathbb{R}$? In a sense, we need to increase our domain. Therefore, we need to find elements that don't belong to $\mathbb{R}$. The way to do that is to look at roots of polynomials. There is no root of the polynomial $X^2 + 1$ in $\mathbb{R}$. Hence, just add the root. This is formally done by quotienting.

But there is a small catch before we do that. We now know that we have the complex number i is a root of $X^2 + 1$ but it is of course the root of $(X^2+1)(X^{213} - 3X^{127} + 897)$ as well. This is where the concept of minimal polynomial comes in.

Definition 2. *Let L be an extension of K. For any $\alpha \in L$, the mimimum polynomial of α over K is the monic polynomial of smallest degree over K that has α as a root.*

Again, the questions of existence and uniqueness comes in. Does every α have a minimum polynomial? The answer is no, and the example is π over $\mathbb{Q}$. It doesn't make sense to talk of a minimum polynomial when the number is transcendental.

But suppose the number is not transcendental, that it is a root of some polynomial. Then do we have a unique minimum polynomial? Yes. Since if f and g are two polynomials of smallest degree that has α as a root, then so does $gcd(f, g)$ and the gcd clearly has smaller degree. This then contradicts that f and g had least degree. Thus the minimum polynomial is unique.

And by the same reason, the minimum polynomial must be irreducible. For if f was the minimum polynomial of α and if $f(X) = g(X)h(X)$ then α must be a root of either g or h and their degree is strictly less than f. Thus the minimum polynomial if indeed irreducible.

Another way is the following. We have some $\alpha \in L$ and we want the minimum polynomial of α. Consider the following homomorphism.

$$\begin{array}{rcl} \text{eval}_\alpha : K[X] & \longrightarrow & L \\ f(X) & \mapsto & f(\alpha) \end{array}$$

The map is called the evaluation map since it just evaluates every polynomial at α. The kernel of this map will be an ideal of $K[X]$, a principle ideal. The generator of this ideal is the minimum polynomial.

Here is a way to create extensions. Look at $\mathbb{F}_p[X]$ and take some irreducible polynomial f of it. Then we know that $\mathbb{F}_p[X]/(f)$ is a field since the ideal (f) is maximal as f is irreducible. If the degree of f is d, then this would give is a field of size p^d.

We shall see this in more detail next time.