Office Hour: 11:00 – noon.
Starting from this Thursday.

Classification of Finite Fields (fields with finitely many elements)

Claim 0:  
If a field $F$ contains finitely many elements, then  
\[ \text{char}(F) < \infty. \]  
(Recall $\text{char}(F)$ is the smallest positive integer $m > 0$ s.t.  
\[ 1 + 1 + \cdots + 1 = 0 \in F \]

pf: Consider the set \( S = \{ 1, 2, 3, \ldots, m, \ldots \} \subseteq F \)
which only contains finitely many elements.
If $\text{char}(F) = 0$ (meaning $m \cdot 1 \neq 0$ for any $m \in \mathbb{Z}$),
then $S$ will contains infinitely many elements. Contradiction.

Recall we showed before $\text{char}(F)$ must be a prime number.
\[ n = \prod p_i^{y_i} \quad n \cdot 1 = 0 \quad \Rightarrow \quad \exists p \mid n \quad p \cdot 1 = 0 \]
since there is no zero-divisors in $F$. 

Claim 1: If char\( (F) = p \), \( |F| < \infty \), then \( |F| = p^n \) for some \( n \in \mathbb{Z}_+ \).

pf: If char\( (F) = p \), then \( \exists \, 0, 1, \ldots, p-1 \in F \) is a subfield \( \mathbb{F}_p (\mathbb{Z}_p) \), so \( F \) is a field extension of \( \mathbb{F}_p \). So it is a vector space \( /F_p\), say with dim = \( n \). We know \( n < \infty \) because \( |F| < \infty \).

Therefore \( F \) contains \( p^n \) elements since any dimension \( n \) \( \mathbb{F}_p \) -vs contains \( p^n \) elements.

Q: Any example of fields \( F \) s.t.
1) char\( (F) < \infty \)
2) \( |F| = \infty \).

e.g. \( F = \mathbb{F}_p (t) = \{ \frac{f(t)}{g(t)} \mid f(t), g(t) \in \mathbb{F}_p [t] \} \)

\( t, -, \times, \div \) is a field.

\( F \) is still a field extension of \( \mathbb{F}_p \), therefore char\( (F) = p \), \( t, t^2, t^3, \ldots \) are all different elements in \( F \). So \( |F| = \infty \).
Our main goal is to show the following theorem.

**Thm.** There exists a unique finite field \( F \) s.t. 

\[ |F| = p^n = q \quad \text{for every } p \text{ and every } n. \]

**Pf:** Existence : (It is clear \( \text{char}(F) = p \). so \( F \) must 
a field extension of \( \mathbb{F}_p \).)

Let \( f(x) = x^9 - x \in \mathbb{F}_p[x] \). Let \( K \) be the 
splitting field of \( f(x) \) over \( \mathbb{F}_p \).

(Recall splitting field of \( f(x) \in F[x] \) is the smallest field extension \( F \subseteq K \) s.t. \( f(x) = \prod_{i} (x - x_i) \in K[x], \)
or equivalently, the smallest field extension containing all roots of \( f(x) \).)

\[ K = \overline{\mathbb{F}_p}(f) \]

meaning splitting field of \( f(x) \).

\[ \overline{\mathbb{F}_p} \]

**Claim 2:** \( S = \{ x \in K | f(x) = 0 \} \)

Then \( \overline{\mathbb{F}_p} \leq S \leq K \) is a subfield of \( K \).

**Pf:** If \( x_1^2 = x_1, \quad x_1^2 = x_2 \), then

1) \( (x_1 + x_2)^2 = x_1 + x_2 \) \( \leftarrow \) use \( p \mid \text{combinatoric number} \)

2) \( \left( \frac{1}{x_1} \right)^2 = \frac{1}{x_1} \)

3) \( x_1 \cdot x_2 \)

\[ \overline{\mathbb{F}_p} \leq S \quad \text{since } x \in \overline{\mathbb{F}_p} \text{ satisfy } \]

\[ x^{p - 1} = 1 \]
Lemma: Given a finite group \( G \) with \( |G| = n \). Then \( g^n = e \) for all \( g \in G \). (We will prove this in next class.)

Notice \( \mathbb{F}_p \setminus \{0\} = \mathbb{F}_p^\times \) is an abelian group with \( |\mathbb{F}_p^\times| = p-1 \). So by the lemma, \( \alpha^{p-1} = 1 \) \( \forall \alpha \in \mathbb{F}_p^\times \)

so \( \alpha^p = \alpha \), thus \( \alpha^q = (\alpha^p)^{\frac{p}{q}} = \alpha \). \( \square \)

So \( S \) contains all roots of \( f(x) \). Then \( S = K \) by definition of splitting fields.

To show \( |S| = p^n \) it suffices to show that all roots are different.

Claim 3: \( f(x) \) has distinct roots. 
pf: Suppose \( f(x) \) has repeated roots. \( f(x) = \prod (x-\alpha_i) \)

\[ f(x) = (x-\alpha)^2 \cdot g(x) \quad \text{where} \quad g(x) = \prod \frac{1}{x-\alpha_i} \]

then \( f'(x) = 2(x-\alpha) \cdot g(x) + (x-\alpha)^2 \cdot g(x) \).

where \( f'(x) \) is defined to be \( \sum a_n \cdot n x^{n-1} \) for \( \sum a_n x^n \).

Then \( f'(\alpha) = 0 \) but \( f'(x) = q \cdot x^{2-1} - 1 = -1 \) since \( p \div q \). \( \square \) (Remark: product rule also holds with this new definition of \( f'(x) \))

Then we know \( |S| = p^n \). So we finish the existence.
Uniqueness: If $F$ contains $p^n$ elements. Consider its multiplicative group $F^* = F \setminus \{0\}$. \[|F^*| = p^n - 1\] elements. So, by the Lemma before, $\alpha^{p^n - 1} = 1$ for all $\alpha \in F$. So $\alpha^{p^n} = \alpha$. So all elements of $F$ are roots of $f(x) = x^{p^n} - x$, so $F \subseteq K$ the splitting field of $f(x)$, we know $|K| = p^n$ because in last part $K = S$ has size $p^n$ and $F$ has size $p^n$, so $F = K$.

Q: Do we always get the splitting field for $f(x)$ by $F_p[x]/\langle f(x) \rangle$ for irreducible $f(x) \in F_p[x]$.
Ans. Yes. Requires a proof. (Left as an exercise).

Corollary. Finite fields with $q = p^n$ elements, denoted by $\mathbb{F}_q$, is the splitting field of $f(x) = x^2 - x$. Actually every element in $\mathbb{F}_q$ is a root of $f(x)$.
Q: How to find a set of basis for $\mathbb{F}_q$ as a
\[\dim_{\mathbb{F}_p} v.s.\] over $\mathbb{F}_p$?