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

$char(F) < \infty$. (Recall $char(F)$ is the smallest positive integer $m > 0$ s.t. $\underbrace{1+1+\cdots+1}_{m} = 0 \in F$)

Pf: Consider the set $S = \{1, 2\cdot 1, 3\cdot 1, \ldots, m\cdot 1, \ldots\} \subseteq F$

which only contains finitely many elements.

If $char(F) = 0$ (meaning $m \cdot 1 \neq 0$ for any $m \in \mathbb{Z}$).

then S will contains infinitely many elements. Contradiction $\square$.

Recall we showed before $char(F)$ must be a prime number.

$n = \prod p_i^{r_i}$ $\quad n \cdot 1 = 0 \Rightarrow \exists\, p \mid n \quad p \cdot 1 = 0$

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 $\{0, 1, \cdots p-1\} \subseteq F$ 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 $/\mathbb{F}_p$, say with $\dim = n$. We know $n < \infty$ because $|F| < \infty$. Therefore F contains p^n elements since any dimension n $\mathbb{F}_p$-v.s contains p^n elements. $\square$.

Q: Any example of fields. F s.t.

1) $char(F) < \infty$

2) $|F|$ "=" ∞.

eg. $F = \mathbb{F}_p(t) = \left\{ \frac{f(t)}{g(t)} \;\middle|\; f(t), g(t) \in \mathbb{F}_p[t] \right\}$

$+, -, \times, \div$ is a field.

F is still a field extension of $\mathbb{F}_p$, therefore $char(F) = p$.

$t, t^2, t^3, \cdots$, are all different elements in F. So $|F|$ "=" ∞.

Our main goal is to show the following theorem.

Thm. There exists a unique finite field F s.t.

$|F| = p^n = q$ for every p and every n.

pf: Existence: (It is clear $\mathrm{char}(F) = p$. so F must a field extension of $\mathbb{F}_p$.)

Let $f(x) = x^q - x \in \mathbb{F}_p[x]$. 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. $f(x) = \prod_i (x - \alpha_i) \in K[x]$, or equivalently, the smallest field extension containing all roots of $f(x)$).

$$K = \mathbb{F}_p(f)$$
$$|$$
$$\mathbb{F}_p$$

meaning splitting field of $f(x)$.

Claim 2: $S = \{\alpha \in K \mid f(\alpha) = 0\}$

Then $\mathbb{F}_p \subseteq S \subseteq K$ is a subfield of K.

pf: If $\alpha_1^q = \alpha_1$, $\alpha_2^q = \alpha_2$, then

1) $(\alpha_1 + \alpha_2)^q = \alpha_1 + \alpha_2$ ← use $p \mid$ combinatoric number

2) $\left(\frac{1}{\alpha_1}\right)^q = \frac{1}{\alpha_1}$

3) $(\alpha_1 \cdot \alpha_2)^q = \alpha_1 \cdot \alpha_2$

$\mathbb{F}_p \subseteq S$ since $\alpha \in \mathbb{F}_p$ satisfy

$\alpha^{p-1} = 1$

[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 .

multiplicative grp of a field

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. $\alpha^{p-1} = 1 \quad \forall \alpha \in \mathbb{F}_p^\times$.

so $\alpha^p = \alpha$, thus $\alpha^q = \underbrace{((\alpha^p)^{p\cdots})^p}_{q \text{ times}} = \alpha$. $\square$.

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.

<u>Claim 3</u> : $f(x)$ has distincts roots.

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

$$f(x) = (x-\alpha)^2 \cdot g(x). \quad \text{where } g(x) = \prod_{i \in I} (x - \alpha_i)$$

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

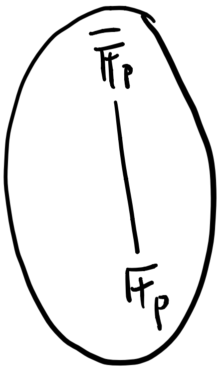
where $f'(x)$ is defined to be $\sum_n a_n \cdot n \cdot x^{n-1}$ for $\sum a_n x^n$.

Then $f'(\alpha) = 0$ But $f'(x) = q \cdot x^{q-1} - 1 = -1$ since $p \mid q$.

Contradiction. $\square$. (Remark: product rule also holds with this new definition of $f'(x)$).

Then we know $|S| = p^n$. So we finish the existence.

<u>Uniqueness:</u> If F contains p^n elements. Consider its multiplicative group $F^\times = F \setminus \{0\}$. $|F^\times| = p^n - 1$ elements. So. by the Lemma before. $\alpha^{q-1} = 1$ for all $\alpha \in F$. So $\alpha^q = \alpha$. So all elements of F are roots of $f(x) = x^q - x$, 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 $F = K$.

$\square$.

Q: Do we always get the splitting field for $f(x)$ by $\mathbb{F}_p[x]/f(x)$ for irreducible $f(x) \in \mathbb{F}_p[x]$.

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 $f(x) = x^q - x$. 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$=n$ v.s over $\mathbb{F}_p$?