Math 491, Thursday, April 9  Chapter 22  Finite Fields

Thu
Fri
Mon
Tue
Thu  Problem session
Fri  Chapter 23

Sage 22
Basics of Finite Fields

1. Field, assume finite $\Rightarrow$ characteristic is prime, $p$

2. \[ \{ 1, 1+1, 1+1+1, \ldots, \underbrace{1+1+\ldots+1}_{p \text{ 1's}} \} \quad (\underbrace{1+1+\ldots+1}_{p \text{ 1's}} = 0) \]

   $= \text{sub field } \cong \mathbb{Z}_p$

3. $F$ is an extension field of $\mathbb{Z}_p$

   So $F$ is a vector space w/ scalars from $\mathbb{Z}_p$

   $F = \text{vectors}$ $\\text{vector addition: } f_1 + f_2 \uparrow \text{define field } f_1, f_2 \in F$

   $\mathbb{Z}_p = \text{scalars}$ $\\text{scalar multiplication: } \alpha f \uparrow \text{define field } \alpha \in \mathbb{Z}_p, f \in F$
So $F$ is a finite extension of $\mathbb{Z}_p$, of finite degree $n$.

Say $[F: \mathbb{Z}_p] = n$ (where $n = \dim(F)$).

So basis $B = \{ f_1, f_2, \ldots, f_n \}$. Every element of $F$ "looks like" $\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_n f_n$ where $\alpha_i \in \mathbb{Z}_p$.

$p$ choices for each $\alpha_i$, so $\mathbb{Z}_p^n$ gives $p^n$ such elements, all different.

Fact: Every finite field has order $p^n$.

Also for every choice of a $p$ and a $n$, there is a finite field of order $p^n$. 
A separable extension $x^2 + x + 1 \in \mathbb{Q}[x]$ has no real roots.

Let $a$ be one root. Then $-a-1$ is the other root.

\[
(x-a)(x-(-a-1)) = (x-a)(x+a+1) = x^2 + ax + x - ax - a - a = x^2 + x - (a^2 + a) = x^2 + x - (-1) = x^2 + x + 1
\]

Extension $\mathbb{Q}(a)$ basis $\{a^0, a^1\} = \mathbb{Q}a^1$

$[\mathbb{Q}(a) : \mathbb{Q}] = 2$

$\mathbb{Q}(a) = \{s(1) + ta \mid s, t \in \mathbb{Q}\} = \langle 3s, a^1 \rangle$

Is $s + ta$ a root of a separable polynomial?

Minimal polynomial of $s + ta$ is $x^2 + (t - 2s)x + (s^2 - st + t^2)$

Check: $(s + ta)^2 + (t - 2s)(s + ta) + (s^2 - st + t^2)$
\[= \frac{S^2 + 2sta + t^2a^2}{s} + \frac{st + t^2a - 2s^2 - 2sta + s^2}{s} - st + t^2 \]

\[= t^2 + (2st + t^2 - 2st)a + t^2a^2 \]

\[= t^2 + t^2a + t^2a^2 = t^2(1+a+a^2) = t^2 \cdot 0 = 0 \]

Is this polynomial separable?

Factors as \((x - (s+ta))(x - ((s-t)-ta))\)

\[x^2 - (s+ta + (s-t)-ta) x + (s+ta)((s-t)-ta)\]

\[x^2 - (2s-t) + (s^2 - st - sta + sta - t^2a - t^2a^2)\]

\[-t^2(a+a^2) = -t^2(1) = t^2 \]

\[t = 0 \quad \text{then} \quad s+ta = s\]

is a root of the separable polynomial \(x-s \in \mathbb{Q}[x]\) and other roots
Are the two roots in the \( t \neq 0 \) case different?

In other words

\[ s + t a = (s-t) - t a \] ??

Note: \( s, t \) is a basis for \( \mathbb{Q}(a) / \mathbb{Q} \).

Linear independence (VRRR)

\[ \Rightarrow s = s-t \quad \text{coeff. } 1 = a \]
\[ t = -t \quad \text{coeff. } a^1 \]

\[ \Rightarrow t = 0 \quad t = 0 \]

Minimal poly (above) ???

\[ (s + t a)^0 = 1 \]
\[ (s + t a)^1 = s + t a \]
\[ (s + t a)^2 = \]

\[ \text{so there exists } \alpha_1, \alpha_2, \alpha_3 \text{ s.t.} \]

\[ \alpha_1(1) + \alpha_2(s + t a) + \alpha_3(s + t a^2) = 0 = 0 \]

Two equations (coeffs of \( 1, a \)) in three vars \((\alpha_1, \alpha_2, \alpha_3)\)

Homogeneous HME with \( a \neq 0 \)

\[ \Rightarrow \text{infinite many solutions} \]

Choose a solution with \( \alpha_3 = 1 \).