Math 491, Thursday, April 9 Chapter 22 Finite Fields

Thu
Fri
Mon
Tue

Chapter 22

Thu Problem session

Fri Chapter 23

Sage 22

Basics of Finite Fields

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

ring

② $\{\underset{\uparrow 0}{1}, 1+1, 1+1+1, \ldots, \underbrace{1+1+\cdots+1}_{p-1\ 1\text{'s}}\}$ $\quad (\underbrace{1+1+\cdots+1}_{p\ 1\text{'s}} = 0)$

$=$ subfield $\cong \mathbb{Z}_p$

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

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

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

$\mathbb{Z}_p$ = scalars $\qquad$ Scalar multiplication:

$$\underset{\uparrow\ \text{define}}{\alpha f} = \underset{\uparrow\ \text{field}}{\alpha f} \qquad \alpha \in \mathbb{Z}_p,\ f \in F$$

So F is a finite extension of $\mathbb{Z}_p$, so finite degree

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

So basis $B = \{f_1, f_2, \ldots, f_n\}$. Every element of F

" looks like "

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_n f_n \qquad \alpha_i \in \mathbb{Z}_p$$

p choices

Theorem VRTB $\Rightarrow$ expressions are unique

<u>all</u> different

Total of $p \cdot p \cdots p = p^n$ such elements.

<u>Fact</u> Every finite field has order p^n.

Also for every choice of a p & a n, there is a finite field of order p^n.

Seperable Extensions

Ex A seperable extension

$x^2+x+1 \in \mathbb{Q}[x]$ no rational roots

$\Rightarrow a^2+a+1=0$

$a^2+a=-1$

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

$(x-a)(x-(-a-1)) = (x-a)(x+a+1) = x^2+ax+x-ax-a^2-a$

$= x^2+x-(a^2+a) = x^2+x-(-1) = x^2+x+1$

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

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

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

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

$t=0$

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

Check: $(s+ta)^2+(t-2s)(s+ta)+(s^2-st+t^2)$

$= s^2 + 2sta + \boxed{t^2a^2} + st + t^2a - 2s^2 - 2sta + s^2 - st + t^2$

$= t^2 + (2st + t^2 - 2st)a + t^2a^2$

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

Is this polynomial seperable?

Factors as $(X - (s+ta))(X - ((s-t) - ta))$

$\leftarrow t = 0$

$(X-s)(X-s) = (X-s)^2$

repeated roots

$X^2 - (s+ta+(s-t)-ta)X + (s+ta)((s-t)-ta)$

$X^2 - (2s-t) + (s^2 - st - sta + sta - t^2a - t^2a^2)$

$-t^2(a+a^2) = -t^2(-1) = t^2$

$t=0$ then $s+ta = s$ is a root of the seperable polynomial $X - s \in \mathbb{Q}[X]$

distinct roots

Are the two roots in the $t \neq 0$ case different?

In other words $s+ta = (s-t) - ta$???

Note: $\{1, a\}$ is a basis for $\mathbb{Q}(a)/\mathbb{Q}$.

linear independence (VRRB) $\Rightarrow$ $s = s-t$ coeff. $1 = a^0$
$t = -t$ coeff. a^1

$\Rightarrow$ $t=0$ $\Rightarrow\Leftarrow$ $t=0$

v_1, v_2 basis V

$2v_1+v_2,\ v_1+v_2$ basis??

$(2a_1+a_2)v_1 + (a_1+a_2)v_2 = 0$

$$\begin{cases} 2a_1+a_2=0 \\ a_1+a_2=0 \end{cases}$$

Minimal poly (above)???

$(s+ta)^0 = 1$
$(s+ta)^1 = s+ta$
$(s+ta)^2 =$

linearly dependent in $\mathbb{Q}(a)/\mathbb{Q}$
$3 > 2$

So there exists $\alpha_1, \alpha_2, \alpha_3$ so that

$\alpha_1(1) + \alpha_2(s+ta) + \alpha_3(s+ta^2) = 0 = 0$

Two equations (coeffs of $1, a$) in three vars $(\alpha_1, \alpha_2, \alpha_3)$
homogeneous HMVEI $\Rightarrow$ infinitely many solutions
Choose a solution w/ $\alpha_3 = 1$.