

(25)

THEOREM: Fix a prime power  $q = p^d$  with  $d \in \{1, 2, \dots\}$ .  
 (15.7.3, 15.7.4')

- (a)  $\exists$  an irreducible polynomial  $f(x) \in \mathbb{F}_p[x]$  of degree  $d$ , and hence a finite field  $\mathbb{F} := \mathbb{F}_p[x]/(f(x))$  with  $|\mathbb{F}| = q = p^d$
- (b) They are all isomorphic (as rings/fields), so we can call any of them  $\mathbb{F}_q$ .
- (c) Any such  $\mathbb{F}_q$  has the Frobenius map  $\mathbb{F}_q \xrightarrow{F} \mathbb{F}_q$   
 $\alpha \longmapsto \alpha^p$   
 giving an  $\mathbb{F}_p$ -automorphism of  $\mathbb{F}_q$
- (d)  $\mathbb{F}_q$  is the set of all the (distinct!) roots of  $x^q - x$  inside any extension  $K \supset \mathbb{F}_p$  where it splits, i.e.  $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$ .

Equivalently,  $\mathbb{F}_q = \{ \alpha \in K : \alpha^q = \alpha \} = \{ \alpha \in K : (F \circ F \circ \dots \circ F)(\alpha) = \alpha \}$   
 $\quad \quad \quad \parallel \quad \quad \quad \parallel \quad \quad \quad \parallel$   
 $\quad \quad \quad ((\alpha^p)^p)^{\dots}$   $F^d(\alpha)$

(e) Inside  $\mathbb{F}_p[x]$ , the irreducible factorization of  $x^d - x$  is

$$x^d - x = \prod_{\substack{\text{all irreducibles} \\ g(x) \in \mathbb{F}_p[x] \\ \text{with } \deg(g) \text{ dividing } d}} g(x)$$

(f)  $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^d} \iff e \text{ divides } d$

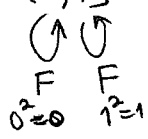
3/29/2019

EXAMPLES: Let's examine  $\mathbb{F}_2 \subset \mathbb{F}_{2^2} \subset \mathbb{F}_{2^4}$ , by first cataloguing irreducibles in  $\mathbb{F}_2[x]$  up to degree 4:  
 $\quad \quad \quad \cap \quad \quad \quad \parallel \quad \quad \quad \parallel$   
 $\quad \quad \quad \mathbb{F}_8 = \mathbb{F}_{2^3} \quad \quad \quad \mathbb{F}_4 \quad \quad \quad \mathbb{F}_{16}$

degree:	1	2	3	4
	$x$	<del><math>x^2 = (x+1)^2</math></del>	<del><math>x^3 = (x+1)(x^2+x+1)</math></del>	<del><math>x^4 + x + 1</math></del>
	$x+1$	$x^2+x+1$	$x^3+x+1$	<del><math>x^4+x^2+1 = (x^2+x+1)^2</math></del>
			$x^3+x^2+1$	$x^4+x^3+1$
			<del><math>x^3+x^2+x+1 = (x+1)^3</math></del>	$x^4+x^3+x^2+x+1$

(76)

$$\mathbb{F}_2 = \{0, 1\} = \text{roots of } x(x-1) = x^2 - x$$



$$\mathbb{F}_4 = \mathbb{F}_{2^2} = \mathbb{F}_2[\alpha] / (\alpha^2 + \alpha + 1) = \{0, 1, \alpha, \alpha^2\}$$

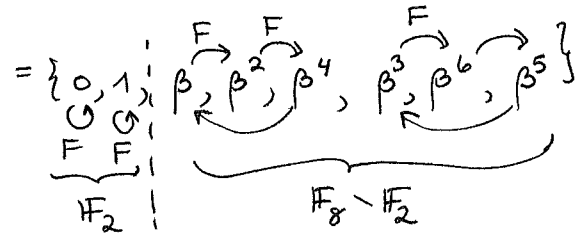
$$\begin{aligned} x^4 - x &= x^4 - x = x(x^3 - 1) \\ &= x(x-1)(x^2 + x + 1) \text{ in } \mathbb{F}_2[x] \\ &= x(x-1)(x-\alpha)(x-\alpha^2) \text{ in } \mathbb{F}_4[x] \end{aligned}$$

deg 1 irreducibles      deg 2 irreducible

$$\mathbb{F}_8 = \mathbb{F}_{2^3} = \mathbb{F}_2[\beta] / (\beta^3 + \beta + 1)$$

$$= \{0, 1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\}$$

$\beta^4 = \beta + 1$   
 $\beta^5 = \beta^2 + \beta$   
 $\beta^6 = \beta^2 + \beta + 1$

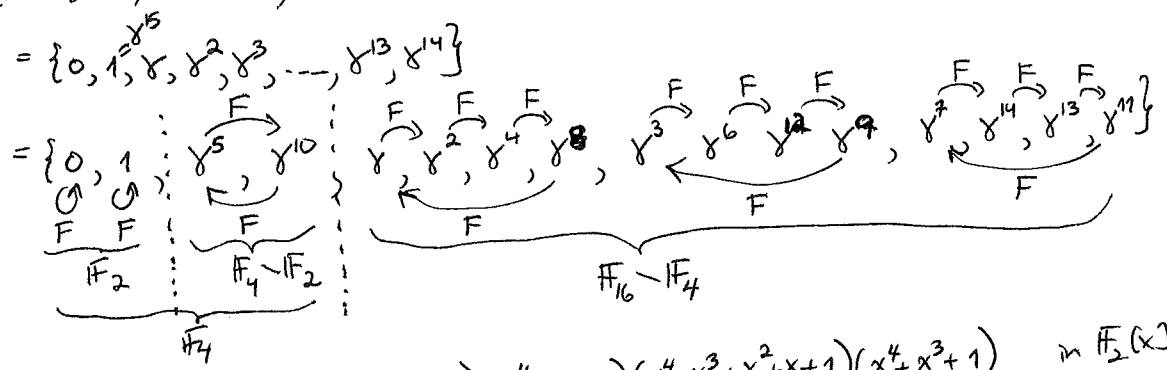


$$\begin{aligned} x^8 - x &= x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \\ &= x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } \mathbb{F}_2[x] \end{aligned}$$

deg 1 irreducibles      deg 3 irreducibles

$$= x(x-1)(x-\beta)(x-\beta^2)(x-\beta^4) \cdot (x-\beta^3)(x-\beta^6)(x-\beta^5) \text{ in } \mathbb{F}_8[x]$$

$$\mathbb{F}_{16} = \mathbb{F}_{2^4} = \mathbb{F}_2[\gamma] / (\gamma^4 + \gamma + 1) \text{ has } \gamma \text{ of multiplicative order 15 since } \gamma \neq 1, \gamma^3 \neq 1, \gamma^5 = \gamma \cdot \gamma^4 = \gamma(\gamma+1) = \gamma^2 + \gamma \neq 1$$



$$\begin{aligned} x^{16} - x &= x^{16} - x = x(x-1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1) \text{ in } \mathbb{F}_2[x] \\ &= x(x-1)(x-\gamma^5)(x-\gamma^{10})(x-\gamma)(x-\gamma^2)(x-\gamma^4)(x-\gamma^8) \cdot (x-\gamma^3)(x-\gamma^6)(x-\gamma^{12})(x-\gamma^9) \cdot (x-\gamma^7)(x-\gamma^{14})(x-\gamma^{13})(x-\gamma^{11}) \text{ in } \mathbb{F}_{16}[x] \end{aligned}$$

deg 1 irreds      deg 2 irred.      deg 4 irreds

(77) proof of THEOREM:

The Frobenius map  $\alpha \mapsto \alpha^p$  has the key property that

it is a ring homomorphism  $R \xrightarrow{F} R$  for any ring  $R$  of characteristic  $p$ :

$$F(1) = 1^p = 1$$

$$F(\alpha\beta) = (\alpha\beta)^p = \alpha^p \beta^p = F(\alpha)F(\beta)$$

$$F(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \binom{p}{2}\alpha^{p-2}\beta^2 + \dots + \binom{p}{p-1}\alpha\beta^{p-1} + \beta^p = \alpha^p + \beta^p$$

The "Freshman dream"  
 $(\alpha+\beta)^p = \alpha^p + \beta^p$   
 when  $\text{char}(R) = p$

these  $\binom{p}{k}$  for  $1 \leq k \leq p-1$  are all divisible by  $p$   
 since  $\binom{p}{k} = \frac{p(p-1)(p-2)\dots(p-k+1)}{k(k-1)(k-2)\dots(1)}$  can't be cancelled by the denominator

Now let  $K \supset \mathbb{F}_p$  be any extension where  $x^p - x$  splits completely in  $K[x]$ ,

and let  $F := \{\text{all roots of } x^p - x \text{ in } K\}$

$$= \{\alpha \in K : \alpha^p = \alpha\}$$

$$\stackrel{\parallel}{=} F^d(\alpha)$$

Since  $x^p - x$  has derivative  $px^{p-1} - 1 \equiv -1$ , these roots  $F$  are all distinct,

and hence there are exactly  $q$  of them, i.e.  $|F| = q = p^d$ .

On the other hand, since  $F$  is a ring homomorphism  $K \xrightarrow{F} K$

$F^d$  is also such a ring homom.  $K \xrightarrow{F^d} K$

and thus  $F$  is actually a subfield of  $K$ : given  $\alpha, \beta \in F$

$$\text{then } F^d(\alpha+\beta) = F^d(\alpha) + F^d(\beta) = \alpha + \beta$$

$$F^d(\alpha\beta) = F^d(\alpha)F^d(\beta) = \alpha\beta$$

$$F^d(-\alpha) = F^d(-1)F^d(\alpha) = -\alpha$$

$$F^d(\alpha^{-1}) = F^d(\alpha)^{-1} = \alpha^{-1}$$

↑  
 apply  $F^d$  to  $\alpha \cdot \alpha^{-1} = 1$

This is  $-1$  by applying  $F^d$  to  
 $1 + (-1) = 0$   
 $F^d(1 + (-1)) = F^d(0)$   
 $F^d(1) + F^d(-1) \stackrel{\parallel}{=} 0$   
 $1 + F^d(-1)$

4/1/2019 > When one restricts  $F$  to  $F \xrightarrow{F} F$ , one finds that  $F^d(\alpha) = \alpha$ , so  $F^{-1} = F^{d-1}$  on  $F$

$$F(F^d(\alpha))$$

and  $F$  becomes a field automorphism of  $F$ , and it fixes  $\mathbb{F}_p$  since  $F(1) = 1 \Rightarrow F(1+1+\dots+1) = 1+1+\dots+1$