(25)

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

(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 $\mathbb{K} \supset \mathbb{F}_p$ where it splits, i.e. $x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$.

Equivalently, $\mathbb{F}_q = \{\alpha \in \mathbb{K} : \underbrace{\alpha^q}_{(((\alpha^p)^p)\cdots)^p} = \alpha\} = \{\alpha \in \mathbb{K} : \underbrace{(F \circ F \circ \cdots \circ F)}_{F^d}(\alpha) = \alpha\}$

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

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

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

$\cap$ $\quad$ $=$ $\quad$ $=$

$\mathbb{F}_8 = \mathbb{F}_{2^3}$ $\quad$ $\mathbb{F}_4$ $\quad$ $\mathbb{F}_{16}$

degree:	1	2	3	4
	x	~~$x^2+1 = (x+1)^2$~~	~~$x^3+1 = (x+1)(x^2+x+1)$~~	x^4+x+1
	$x+1$	x^2+x+1	x^3+x+1	~~$x^4+x^2+1 = (x^2+x+1)^2$~~
			x^3+x^2+1	x^4+x^3+1
			~~$x^3+x^2+x+1 = (x+1)^3$~~	$x^4+x^3+x^2+x+1$

(76)

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

F: $0^2 = 0$, F: $1^2 = 1$

$\mathbb{F}_4 = \mathbb{F}_{2^2} = \mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1) = \{0, 1, \alpha, \alpha+1\}$ ($\alpha^3 = 1$, $\alpha^2 = \alpha+1$)

$\{0,1\}$: F, F — $\mathbb{F}_2$; $\{\alpha, \alpha+1\}$: F, F — $\mathbb{F}_4 \setminus \mathbb{F}_2$

$x^{\mathbb{F}_2} - x = x^4 - x = x(x^3-1)$

$= x(x-1)(x^2+x+1)$ in $\mathbb{F}_2[x]$

deg 1 irreducibles; deg 2 irreducible

$= x(x-1)(x-\alpha)(x-\alpha^2)$ in $\mathbb{F}_4[x]$

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

$= \{0, 1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\}$ ($\beta^7 = 1$, $\beta^3 = \beta+1$, $\beta^4 = \beta^2+\beta$, $\beta^5 = \beta^3+\beta^2 = \beta^2+\beta+1$, $\beta^6 = \beta^3+\beta^2+\beta = \beta^2+1$)

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

$\{0,1\}$: F, F — $\mathbb{F}_2$; $\{\beta, \beta^2, \beta^4\}$: F, F; $\{\beta^3, \beta^6, \beta^5\}$: F — $\mathbb{F}_8 \setminus \mathbb{F}_2$

$x^{2^3} - x = x^8 - x = x(x^7-1) = x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$

$= x(x-1)(x^3+x+1)(x^3+x^2+1)$ in $\mathbb{F}_2[x]$

deg 1 irreducibles; deg 3 irreducibles

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

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

$= \{0, 1, \gamma, \gamma^2, \gamma^3, \dots, \gamma^{13}, \gamma^{14}\}$ ($\gamma^{15} = 1$)

$= \{0, 1, \gamma^5, \gamma^{10}, \gamma, \gamma^2, \gamma^4, \gamma^8, \gamma^3, \gamma^6, \gamma^{12}, \gamma^9, \gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}$

$\{0,1\}$: F, F — $\mathbb{F}_2$; $\{\gamma^5, \gamma^{10}\}$: F — $\mathbb{F}_4 \setminus \mathbb{F}_2$; $\mathbb{F}_4$

$\{\gamma, \gamma^2, \gamma^4, \gamma^8\}$: F, F, F; $\{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}$: F, F, F; $\{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}$: F, F, F — $\mathbb{F}_{16} \setminus \mathbb{F}_4$

$x^{2^4} - x = x^{16} - x = x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)$ in $\mathbb{F}_2[x]$

deg 1 irreds; deg 2 irred.; deg 4 irreds

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

proof of THEOREM:

The Frobenius map $\alpha \xrightarrow{F} \alpha^p$ has the key property that it is a ring homomorphism $R \xrightarrow[\alpha \longmapsto \alpha^p]{F} R$ for any ring R of characteristic p:

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

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

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

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

these $\binom{p}{k}$ for $1 \le k \le p-1$ are all divisible by p

since $\binom{p}{k} = \dfrac{(p)(p-1)(p-2)\cdots(p-(k-1))}{k(k-1)(k-2)\cdots(1)}$ — can't be cancelled by the denominator

Now let $\mathbb{K} \supset \mathbb{F}_p$ be any extension where $x^q - x$ splits completely in $\mathbb{K}[x]$, and let $\mathbb{F} := \{\text{all roots of } x^q - x \text{ in } \mathbb{K}\}$

$$= \{\alpha \in \mathbb{K} : \underbrace{\alpha^q}_{F^d(\alpha)} = \alpha\}$$

Since $x^q - x$ has derivative $qx^{q-1} - 1$ ($q = p^d = 0$ in $\mathbb{K}$) $= -1$, these roots $\mathbb{F}$ are all distinct, and hence there are exactly q of them, i.e. $|\mathbb{F}| = q = p^d$.

On the other hand, since F is a ring homomorphism $\mathbb{K} \xrightarrow{F} \mathbb{K}$, F^d is also such a ring homom. $\mathbb{K} \xrightarrow{F^d} \mathbb{K}$

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

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

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

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

This is -1 by applying F^d to $1 + (-1) = 0$: $F^d(1 + (-1)) = F^d(0)$, $F^d(1) + F(-1) = 0$, $1 + F(-1)$

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

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

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