(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:

$\cap$ $\quad\quad \| \; \mathbb{F}_4 \quad \| \; \mathbb{F}_{16}$

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

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 F

$0^2 = 0$ $1^2 = 1$

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

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

$x^{2^2} - x = x^4 - x = x(x^3-1)$

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

deg 1 irreducibles; deg 2 irreducible

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

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

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

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

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

$= x(x-1)(x^3+x+1)(x^3+x^2+1)$ 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 $\gamma \neq 1$, $\gamma^3 \neq 1$, $\gamma^5 = \gamma\cdot\gamma^4 = \gamma(\gamma+1) = \gamma^2+\gamma \neq 1$

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

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

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

$x^{2^4} - x = x^{16} - x = x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)$ 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 $qx^{q-1} - 1 = -1$ ($q = p^d = 0$ in $\mathbb{K}$), 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 $\underbrace{F^d(\alpha)}_{F(F^{d-1}(\alpha))} = \alpha$, 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 $F(1) = 1 \Rightarrow F(1+1+\cdots+1) = 1+1+\cdots+1$

Now that we have a finite field $\mathbb{F}$ with $|\mathbb{F}| = q = p^d$,
we know $\mathbb{F}^\times = \mathbb{F} - \{0\}$ is cyclic, say $\mathbb{F}^\times = \langle \gamma \rangle = \{1, \gamma, \gamma^2, \ldots, \gamma^{q-2}\}$ ($1 = \gamma^{q-1}$)

and then $\mathbb{F} = \mathbb{F}_p(\gamma)$, so $[\mathbb{F}_p(\gamma) : \mathbb{F}_p] = d$ (with $\mathbb{F}_p(\gamma) = \mathbb{F}$) implies

that $f(x) := m_{\mathbb{F}_p,\gamma}(x) \in \mathbb{F}_p[x]$ is irreducible of degree d.

Thus far we have proven (a), (c), (d).

To prove (b), given two fields $\mathbb{F}, \mathbb{F}'$ with $|\mathbb{F}| = |\mathbb{F}'| = q = p^d$,
want to show they are isomorphic. As above, pick $\gamma \in \mathbb{F}$
with minimal polynomial $f(x) = m_{\mathbb{F}_p,\gamma}(x)$ of degree d in $\mathbb{F}_p[x]$.
Since $\gamma^{q-1} = 1$, so $\gamma^q = \gamma$, and γ is a root of $x^q - x$,
one must have $f(x)$ dividing $x^q - x$ in $\mathbb{F}_p[x]$, say $x^q - x = f(x)g(x)$.
But then since $\mathbb{F}'$ also splits $x^q - x$ completely as $x^q - x = \prod_{\alpha' \in \mathbb{F}'} (x - \alpha')$
$= f(x)g(x)$,

there exists some root $\gamma' \in \mathbb{F}'$ for $f(x)$.
But then $\mathbb{F}' = \mathbb{F}_p(\gamma') \cong \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p(\gamma) = \mathbb{F}$

To prove (f), note $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^d} \Rightarrow \underbrace{[\mathbb{F}_{p^d} : \mathbb{F}_p]}_{d} = [\mathbb{F}_{p^d} : \mathbb{F}_{p^e}] \underbrace{[\mathbb{F}_{p^e} : \mathbb{F}_p]}_{e} \Rightarrow e$ divides d

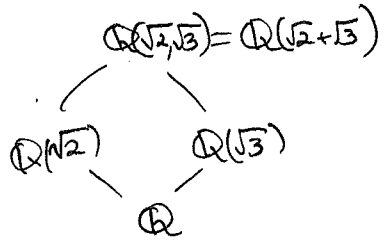
and conversely, if e divides d (say $d = ef$) then $\alpha^{p^e} = \alpha \Rightarrow \alpha^{p^d} = F^d(\alpha) = F^{ef}(\alpha) = \overbrace{F^e(F^e(\cdots(F^e(\alpha))\cdots))}^{f \text{ times}} = \alpha$ (where $\alpha^{p^e} = F^e(\alpha)$)

so $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^d}$ ($\mathbb{F}_{p^e} = \{\text{roots of } x^{p^e} - x\}$, $\mathbb{F}_{p^d} = \{\text{roots of } x^{p^d} - x\}$)

To prove (e), note that an irreducible $f(x) \in \mathbb{F}_p[x]$ divides $x^q - x = x^{p^d} - x$
if and only if its roots lie in $\mathbb{F}_q = \mathbb{F}_{p^d}$, which by (f) means that any of its roots α must
generate a subfield $\mathbb{F}_{p^e} \subset \mathbb{F}_{p^d}$ (with $\mathbb{F}_{p^e} = \mathbb{F}_p(\alpha)$) with e dividing d. But then $\deg(f(x)) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = e$
divides d.
Conversely any such $f(x)$ has roots α that are roots of $x^q - x$, so $f(x)$ divides $x^q - x$ ∎

§15.8 The primitive element theorem

Recall we saw $\mathbb{Q}(\overset{\alpha}{\sqrt{2}}, \overset{\beta}{\sqrt{3}}) = \mathbb{Q}(\overset{\gamma=}{\sqrt{2}+\sqrt{3}})$:



This always happens in characteristic 0 (and for finite fields; see EXER 15.8.1).

THEOREM (15.8.1): When $\mathrm{char}(\mathbb{F}) = 0$, any finite extension $\mathbb{K} \supset \mathbb{F}$ ($[\mathbb{K}:\mathbb{F}] < \infty$) has $\mathbb{K} = \mathbb{F}(\gamma)$ for some $\gamma \in \mathbb{K}$.
(γ called a primitive element for $\mathbb{K}$ over $\mathbb{F}$.)

proof: Since $[\mathbb{K}:\mathbb{F}]$ finite implies $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \dots, \alpha_r)$ for some α_i algebraic over $\mathbb{F}$, using induction on r, it suffices to prove $\mathbb{F}(\alpha,\beta) = \mathbb{F}(\gamma)$ when α, β are algebraic over $\mathbb{F}$: then $\mathbb{K} = \underbrace{\mathbb{F}(\alpha_1,\dots,\alpha_{r-1})}_{=\mathbb{F}(\hat{\gamma})}(\alpha_r) = \mathbb{F}(\hat{\gamma}, \alpha_r) = \mathbb{F}(\gamma)$
(by induction)

So given α, β algebraic over $\mathbb{F}$, pick an extension $\mathbb{K} \supset \mathbb{F}$ so that

$f(x) = m_{\mathbb{F},\alpha}(x) = (x - \overset{\alpha}{\alpha_1})(x-\alpha_2)\cdots(x-\alpha_m)$

$g(x) = m_{\mathbb{F},\beta}(x) = (x - \overset{\beta}{\beta_1})(x-\beta_2)\cdots(x-\beta_n)$

(i.e. $\mathbb{K}$ splits $f(x)g(x)$)

Note $\alpha_1, \dots, \alpha_m$ are distinct, $\beta_1, \dots, \beta_n$ are distinct (why?)

We claim that if we pick $c \in \mathbb{F}$ so that

$$\boxed{\beta_j + c\alpha_i \neq \beta_k + c\alpha_\ell \quad \text{for } (i,j) \neq (k,\ell)}$$

Q: Why can we pick such a $c \in \mathbb{F}$?

A: Can avoid these finitely many bad values

i.e. $c(\alpha_i - \alpha_\ell) \neq \beta_k - \beta_j$ (or $c \neq 0$ if $i = j$)

$$c \neq \frac{\beta_k - \beta_j}{\alpha_i - \alpha_\ell}$$

then $\gamma = \beta_1 + c\alpha_1$ has $\mathbb{F}(\alpha,\beta) = \mathbb{F}(\gamma)$
$= \beta + c\alpha$

(so)
4/3/2019 To see this, its enough to show $\alpha_1 = \alpha \in \mathbb{F}(\gamma)$ since then also $\beta_1 = \gamma - c\alpha_1 \in \mathbb{F}(\gamma)$.

We'll show $x - \alpha_1 = \gcd_{\mathbb{F}(\gamma)[x]}(f(x), g(\gamma - cx)) \; (\in \mathbb{F}(\gamma)[x] \Rightarrow \alpha \in \mathbb{F}(\gamma))$

α_1 is a root of this i.e. $f(\alpha_1) = 0$

$g(\gamma - c\alpha_1) = g(\beta_1) = 0$, so α_1 is also a root of this

$$= \gcd_{\mathbb{K}[x]}(f(x), g(\gamma - cx))$$

$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

$\alpha_2, \ldots, \alpha_n$ are not roots of this, since this would require

$\gamma - c\alpha_i = \beta_j$ for some $i = 2, \ldots, n$

$\beta_1 + c\alpha_1 - c\alpha_i = \beta_j$

$\beta_1 + c\alpha_1 = \beta_j + c\alpha_i$

Contradiction to our choice of c.

∎