Solvable Galois, Frobenius map and more

Tuesday, March 20, 2018 4:37 PM

Assume characteristic of K is zero.

Let $f(x) \in K[x]$. Let L be a splitting field of $f(x)$ over K. $\Rightarrow$ L is normal over K

$\text{char}(K) = 0 \Rightarrow$ L is separable over K

(Notice I don't mention if f is irreducible)

$\Rightarrow$ L is Galois over K

Def: $\text{Gal}_K(f(x)) = \text{Gal}(L/K)$, named Galois group of $f(x)$ over K.

Lemma: Let $a \in K^\times$ and $n \in \mathbb{N}$, $n \geq 2$, and $f(x) = x^n - a \in K[x]$. Then $\text{Gal}_K(f(x))$ is a solvable groups.

pf: Case 1: $x^n - 1$ splits over K (i.e. K contains a primitive n^{th} root of 1.)

Let L be a splitting field of $f(x)$ over K.

Let $\alpha \in L$ be a root of $f(x) = x^n - a$ splits over L, $\beta \in L$ be another root.

$\Rightarrow \beta^n = \alpha^n = a$

(It is possible that $\beta \in K$, i.e. $x^n - 1$, $\beta \in L \setminus K$ but $1 \in K$ reason is $x^n - 1$ is reducible)

$\frac{\beta^n}{\alpha^n} = \frac{a}{a} = 1 \Rightarrow \left(\frac{\beta}{\alpha}\right)^n = 1$

$\Rightarrow \left(\frac{\beta}{\alpha}\right)$ is root of $x^n - 1$

Let $\zeta \in K$ be a primitive n^{th} root of 1.

$\frac{\beta}{\alpha} = \zeta^i$ for some i, $\Rightarrow \beta = \alpha\zeta^i$

On the other hand, $\forall\, l \in \mathbb{N}$, $(\zeta^l\alpha)^n = \zeta^{nl}\alpha^n = a$

$\Rightarrow \zeta^l\alpha$ is a root of $x^n - a$

Claim: $\{\alpha, \zeta\alpha, \zeta^2\alpha, \cdots, \zeta^{n-1}\alpha\}$ roots of $f(x)$

$\zeta^i\alpha = \zeta^j\alpha \Rightarrow \zeta^{i-j} = 1$ Contradict with ζ is a n^{th} primitive of 1 if $i \neq j$

Now, let $L = K(\alpha, \zeta\alpha, \cdots, \zeta^{n-1}\alpha) = K(\alpha, \zeta) = K(\alpha)$

By $\zeta \in K$

Let $\sigma, \tau \in G = \text{Gal}(L/K) = \text{Gal}(K(\alpha)/K)$, Now, we want to show $\text{Gal}(K(\alpha)/K)$ is an abelian group.

$\sigma(\alpha)$ root of $f(x) \Rightarrow \sigma(\alpha) = \zeta^i\alpha$

$\tau(\alpha)$ root of $f(x) \Rightarrow \tau(\alpha) = \zeta^k\alpha$

$\sigma\tau(\alpha) = \sigma(\zeta^k\alpha) = \sigma(\zeta^k)\sigma(\alpha) = \zeta^k\zeta^i\alpha = \zeta^{k+i}\alpha$

$\tau\sigma(\alpha) = \tau(\zeta^i\alpha) = \tau(\zeta^i)\tau(\alpha) = \zeta^i\zeta^k\alpha = \zeta^{k+i}\alpha$

So $L = K(\alpha) \Rightarrow \beta \in L \Rightarrow \beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_l\alpha^l$ s.t. $a_i \in K$. $l \leq n$

Then $\sigma\tau(\beta) = \tau\sigma(\beta)$ By τ, σ preserves K and $\tau\sigma(\alpha) = \sigma\tau(\alpha)$ $\forall\, \sigma, \tau \in G$.

$\Rightarrow \text{Gal}(K(\alpha)/K)$ is an abelian group and abelian group is solvable

$1 \trianglelefteq \text{Gal}(K(\alpha)/K)$

And $\text{Gal}(K(\alpha)/K)/\{1\}$ is abelian.

Case 2: $x^n - 1$ doesn't split over K. Then $\forall$ pair of roots α, β of $f(x)$, $\left(\frac{\beta}{\alpha}\right)^n = 1$

$\deg(f(x)) = n$, $f(x)$ separable over K, must have n distinct roots in L.

L contains a primitive n^{th} root ζ of 1.

(By L is a splitting field of $x^n - a$, and $\geq$ root of $x^n - a$ $\exists \subseteq L$, and those roots are distinct. Then suppose α, β are distinct roots of $x^n - a$, then $\alpha^n = \beta^n = a$

And $\alpha \neq \beta \Rightarrow \alpha\beta^{-1} \neq 1$, $\left(\frac{\alpha}{\beta}\right) \neq 1$. Then $\left(\frac{\alpha^n}{\beta^n}\right) = \left(\frac{\alpha}{\beta}\right)^n \neq 1$

Also, consider $\beta_1 \neq \beta_2$, then $\beta_1^{-1} \neq \beta_2^{-1} \Rightarrow \alpha\beta_1^{-1} \neq \alpha\beta_2^{-1}$

$\Rightarrow \left(\frac{\alpha}{\beta_1}\right) \neq \left(\frac{\alpha}{\beta_2}\right)$, $\left(\frac{\alpha}{\beta_1}\right)^n = \left(\frac{\alpha}{\beta_2}\right)^n = 1$

Then we will have: $\left(\frac{\alpha}{\beta_i}\right)$ are distinct n^{th} roots of 1. (β_i includes α)

Thus L contains a primitive n^{th} root ζ of 1)

$\Rightarrow L = K(\alpha, \zeta) \geq K(\alpha)$

(By Case 1, we know that $K(\alpha, \zeta)$ is a splitting field of $x^n - a$ over K (or $K(\zeta)$)) ↑ $x^n - 1$ splits here

From Case 1, $K(\alpha, \zeta)$ is Galois over $K(\zeta)$

$\text{Gal}(K(\alpha, \zeta)/K(\zeta))$ is abelian

Also, from tutorial, we know that $K(\zeta)$ is an abelian extension of K.

$\Rightarrow \text{Gal}(K(\zeta)/K)$ is abelian

Then $K(\zeta)$ is Galois over K, by F.T.G.T.

We have $\text{Gal}(K(\alpha, \zeta)/K(\zeta)) \trianglelefteq \text{Gal}(K(\alpha, \zeta)/K)$

$\Rightarrow G/H \cong \text{Gal}(K(\zeta)/K)$

$\Rightarrow G/H$ is abelian

$\Rightarrow G/H \cong Gal(K(\mathfrak{A})/K)$

$\Rightarrow G/H$ is abelian

Thm $1 \trianglelefteq H \trianglelefteq G$

H is abelian

G/H is abelian

$\Rightarrow G$ is solvable.

(Or, H and G/H are solvable groups $\Rightarrow G$ is solvable)

Definition:

A (finite) extension M of K is a radical extension of K if there exists $a_1, \dots, a_r \in M$ such that $M = K(a_1, \dots, a_r)$ and $n_1, \dots, n_r \in \mathbb{N}$, such that

$a_1^{n_1} \in K$, and for $2 \le j \le r$, $a_j^{n_j} \in K(a_1, \dots, a_{j-1})$

Definition: $f(x) \in K[x]$ is solvable by radicals if there exists a radical M of K such that $f(x)$ splits over M. ($M \supseteq$ splitting field of $f(x)$ over K)

Example: $2^{\frac{1}{3}}$, $x^3 - 2$, $M = \mathbb{Q}(2^{\frac{1}{3}}, \frac{\sqrt{3}}{2} i)$. Then M is Galois over K.

Theorem: $\mathrm{char}(K) = 0$. If $f(x) \in K[x]$ and $f(x)$ is solvable by radicals over K

Then $Gal_K(f(x))$ is a solvable group.

Example: Find a generic $f(x) \in \mathbb{Q}[x]$ such that $Gal_{\mathbb{Q}}(f(x)) \cong S_5$ (Check the Textbook Material)

Proposition: $\mathrm{char}(K) = 0$. Let M be a radical extension of K. $\exists a_1, \dots, a_r \in M$ and $n_1, \dots, n_r \in \mathbb{N}$ such that $M = K(a_1, \dots, a_r)$, $a_1^{n_1} \in K$, and $a_j^{n_j} \in K(a_1, \dots, a_{j-1})$ for $2 \le j \le r$

Then there exists $K \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r$ such that

(1) F_j is Galois over K

(2) $Gal(F_j/K)$ is solvable

(3) $K(a_1, \dots, a_j) \subseteq F_j$ $1 \le j \le r$

pf: Case $r = 1$, Let F_1 = splitting field of $x_1^{n_1} - a_1^{n_1} \in K[x]$ over K.

Learn from Monday, $Gal(F_1/K)$ is solvable and $K(a_1) \subseteq F_1$ (Bc $a_1 \in F_1$, $K \subseteq F \Rightarrow K(a_1) \subseteq F$)

↑ (Splitting field of $x^n - a$ is over a field K with $\mathrm{char}(K) = 0$ is always Galois over K,

And $Gal(L/K)$ is always solvable)

($Gal_K(x^n - a)$)

Now, consider the case that $r \ge 2$. We prove this theorem by induction.

Suppose for $1 \le m < r$, the proposition holds for $M' = K(a_1, \dots, a_m)$

$\exists K \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m$ satisfying (i), (ii), (iii) for $j \le m$.

Now, let $f_{m+1}(x) = \prod_{\sigma \in Gal(F_m/K)} (x^{n_{m+1}} - \sigma(a_{m+1}^{n+1})) \in K(a_1, \dots, a_m)[x]$

By assumption, $\underbrace{a_{m+1}^{n+1} \in K(a_1, \dots, a_m)}_{\text{Since this is radical}} \subseteq F_m$

$\sigma : F_m \to F_m \Rightarrow \sigma(a_{m+1}^{n_{m+1}}) \in M' \subseteq F_m$

So $x^{n_{m+1}} - \sigma(a_{m+1}^{n_{m+1}}) \in F_m[x]$ $\forall \sigma \in Gal(F_m/K)$

Say $g(x) \in F_m[x]$

Learn: $h(x) = \prod_{\sigma \in Gal(F_m/K)} \sigma(g)(x)$, then $h(x) \in K[x]$

pf: Let $\tau \in Gal(F_m/K)$. Then $\tau(h(x)) = h(x)$?

Bg $\{\sigma \mid \sigma \in Gal(F_m/K)\}$

$= \{\tau\sigma \mid \sigma \in Gal(F_m/K)\}$

$\tau\sigma_1 = \tau\sigma_2 \Rightarrow \sigma_1 = \sigma_2 \Rightarrow$ injective

And $\sigma = \tau(\tau^{-1}\sigma) \Rightarrow$ Surjective

$\Rightarrow \tau(h(x)) = h(x)$ $\forall \tau \in Gal(F_m/K)$

$\Rightarrow$ Every coefficient of $h(x)$ belongs to $F_m^{Gal(F_m/K)} = K$

$\Rightarrow h(x) \in K[x]$

Then using above lemma we can get $f_{m+1}(x) \in K[x]$, Now, let F_m be the splitting field of $h(x) \in K[x]$ over K

Let F_{m+1} = Splitting field of $f_{m+1}(x)h(x)$ over K. $\Rightarrow F_m \in F_{m+1}$

And we can also see that a_{m+1} is also a root of $x^{n_{m+1}} - a_{m+1}^{n_{m+1}}$ which is a divisor of $f_{m+1}(x)$

$\Rightarrow K(a_1, \dots, a_{m+1}) \subseteq F_{m+1}$ (Bg Splitting field should contain all the root, and $K(a_1, \dots, a_m) \subseteq F_m$

Let f_{m+1}

And we can also see that α_{m+1} is also a root of $x^{n_{m+1}} - \alpha_{m+1}^{n_{m+1}}$ which is a divisor of $f_{m+1}(x)$

$\Rightarrow K(\alpha_1, \cdots, \alpha_{m+1}) \subseteq F_{m+1}$ (By Splitting field should contain all the root, and $K(\alpha_1, \cdots, \alpha_m) \subseteq F_m$

Also, no doubt that F_{m+1} is Galois over K. (Normal + separable)

To show that $Gal(F_{m+1}/K)$ is solvable. We have the lemma, then just use the lemma

with some induction we can show that

$Gal(F_m/K)$ is solvable.

$$Gal(F_{m+1}/K)/Gal(F_{m+1}/F_m) \cong Gal(F_m/K)$$

(By Fundamental Theorem of Galois Theory,

F_m is Galois over K (By previous prop)

So $Gal(F_{m+1}/F_m) \trianglelefteq Gal(F_{m+1}/K)$

And we also have $G/H \cong Gal(F_m/K)$ which is solvable

$Gal(F_{m+1}/F_m)$ is solvable

By F_{m+1} is the splitting field of $x^{n_{m+1}} - \alpha_{m+1}^{n_{m+1}}$ over F_m

$\Rightarrow Gal(F_{m+1}/F_m)$ is solvable by Lemma

$\Rightarrow$ G/H and H is solvable

$\Rightarrow G$ is solvable $\Rightarrow Gal(F_{m+1}/K)$ is solvable.

Thm: $char(K) = 0$. Let $f(x) \in K[x]$. If $f(x)$ is solvable by radicals over K. Then $Gal_K(f(x))$ is a solvable group.

pf: Have splitting field L of $f(x)$ over $K \subseteq M$.

$Gal_K(f(x)) = Gal(L/K)$

$K \subseteq L \subseteq M \subseteq F_r$ (Apply above proposition)

We have F_r is Galois over K and $Gal(F_r/K)$ is solvable

Let $G = Gal(F_r/K)$

Let $H = Gal(F_r/L) \leq H \Rightarrow H$ is solvable

Since L is Galois over K (Normal + Separable)

$\Rightarrow$ $L = F_r^H \Rightarrow H \trianglelefteq G$.

$Gal(L/K) \cong G/H$ Solvable. (Quotient of Solvable group is solvable)

Conversely, Suppose $Gal(L/K)$ is solvable, want to show $L \subseteq$ radical extension of K.

$G = Gal(L/K)$

$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_L = G$, G_{i+1}/G_i is cyclic.

$L^{G_0} \supseteq L^{G_1} \supseteq L^{G_2} \cdots \supseteq L^{G_L}$

Notice, if E is a cyclic extension of F of degree n, and $x^n - 1$ splits over F,

Then E = splitting field of $x^n - a$ over some $a \in F$.

$n = \pi [L^{G_i} : L^{G_{i+1}}]$

$L = L^{G_0}$ — $L^{G_0}(\zeta)$

L^{G_1} — $L^{G_1}(\zeta)$

$\vdots$ — $\vdots$

$K = L^G$ — $K(\zeta)$

Need to show $L^{G_i}(\zeta)$ is an cyclic extension of $L^{G_{i+1}}(\zeta)$

proof is in book pg 627 ~ 629. I'll write it down as soon as I get time.

Now, consider $F_p = \mathbb{Z}/p\mathbb{Z}$, $char(F_p) = p$. Let K be an algebraic extension of F_p.

Let $\sigma_p : K \to K$ by $\sigma_p(\alpha) = \alpha^p$, $\alpha \in K$. We can show that σ_p is a homomorphism. (Frobenius map)

$\sigma_p(\alpha + \beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = \sigma_p(\alpha) + \sigma_p(\beta)$

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

$\sigma_p(1) = 1$

And so $\sigma_p(j) = \sigma_p(\underbrace{1 + \cdots + 1}_{j}) = \sum_{i=1}^{j} \sigma_p(1) = j \quad \forall j \in F_p$ (or Fermat's little theorem $\Rightarrow j^p = j$)

Claim: σ_p is surjective. Since K is an algebraic extension of F_p.

First, let $K = F_p(\alpha) \cong F_p[x]/(m_{\alpha,F}(x))$

$\dim_{F_p} K$ is finite and σ_p are 1-to-1 by

$\sigma_p(a) = \sigma_p(b)$

$\Rightarrow (a-b)^p = 0 \Rightarrow a-b = 0$

$\Rightarrow a = b$ by K is a field, no zero divisors

Also, σ is homo $\Rightarrow \sigma$ is injective

$\Rightarrow \dim_{F_p} \sigma(K) = \dim_{F_p} K$

$\Rightarrow [\sigma(K) : F_p] = [K : F_p]$ Is to show $\sigma_p(1), \sigma_p(\alpha), \sigma_p(\alpha^2), \cdots, \sigma_p(\alpha^{n-1})$ are linearly independent.

$\Rightarrow \sigma(K) = K$

If $k_0\sigma_p(1) + k_1\sigma_p(\alpha) + \cdots + k_{n-1}\sigma_p(\alpha^{n-1}) = 0$

$\Rightarrow \sigma_p(k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}) = 0$

By injective

$\Rightarrow k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1} = 0$

$\Rightarrow k_i = 0$ By $1, \alpha, \cdots, \alpha^{n-1}$ are linearly independent.

Now, Let $K = F_p(\alpha_1, \alpha_2, \cdots, \alpha_n)$

Then $[\sigma(K) : F_p] = [K : F_p]$ By σ is injective

$\Rightarrow \sigma(K) = K$

Claim 2: $\sigma_p \in Aut(K/F_p)$, $\forall \alpha \in F_p$, $\sigma_p(\alpha) = \alpha^p = \alpha$

K is not finite, consider the simplest case: $K = F_p(\alpha)$, $[K : F_p] = n$

what will happen is that, then $\forall a \in K$, $a = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$, s.t. $a_i \in F_p$

Then $\sigma_p(a) = a^p$

$= a_0 + a_1\alpha^p + \cdots + a_{n-1}\alpha^{p(n-1)}$

Then if $\alpha^p = \alpha$, we have

$\alpha^{p-1} = 1$

$\Rightarrow \alpha$ is a solution of $x^{p-1} - 1$

Hence, $(F_p)^\times$ are the solution of $x^{p-1}-1$ and

$|(F_p)^\times| = p-1 \Rightarrow \alpha \in (F_p)^\times$, contradict (Field is U.F.D, so it has at most $p-1$ solutions)

$\Rightarrow \alpha^p \neq \alpha$

If $\sigma_p(a) = a$

$a_1(\alpha^p - \alpha) + a_2(\alpha^{2p} - \alpha^2) + \cdots + a_n(\alpha^{(n-1)p} - \alpha^{n-1}) = 0$

Fuck this stupid proof!

Now, forget this proof. Consider $x^p - x$ in K, it has at most p solutions

And We know F_p are solutions of this polynomial and $|F_p| = p$

$\Rightarrow$ If $a \notin F_p$, $a \in K$, then $a^p \neq a$

$\Rightarrow \sigma_p \in Aut(K/F_p)$

Let $n \in \mathbb{N}$, Let L be the splitting field of $x^{p^n} - x$ over F_p.

Since $f'(x) = p^n x^{p^n - 1} - 1 = -1 \Rightarrow$ every root of $f(x)$ has multiplicity one.

$\forall$ root r, $f(r) = 0$, then $(x-r)^2 \mid f(x)$ $\Leftrightarrow f'(r) = 0$ $\Rightarrow$ Every root of $f(x)$ has multiplicity one.

Let $S = \{\alpha \in L \mid f(\alpha) = 0\}$

If $\alpha \in F_p$, then $\alpha^p = \alpha \Rightarrow \alpha^{p^n} = (\alpha^p)^{p^{n-1}} = (\alpha)^{p^{n-1}} = \cdots = \alpha^p = \alpha \Rightarrow f(\alpha) = 0$

$\Rightarrow F_p \subseteq S \subseteq L$

$|S| = p^n$ by $f'(x) = -1 \neq 0$

Let $\alpha, \beta \in S$, $f(\alpha+\beta) = (\alpha+\beta)^{p^n} - (\alpha+\beta)$

$= \alpha^{p^n} + \beta^{p^n} - \alpha - \beta$

$= \alpha^{p^n} - \alpha + \beta^{p^n} - \beta$

$= 0$

One can show this is also closed under multiplication

$f(\alpha\beta) = (\alpha\beta)^{p^n} - \alpha\beta$

$= \alpha^{p^n}\beta^{p^n} - \alpha\beta$

$= \alpha\beta - \alpha\beta$

$= 0$

$f(\alpha^{-1}) = (\alpha^{-1})^p - \alpha^{-1}$

$= (\alpha^p)^{-1} - \alpha^{-1}$

$= \alpha^{-1} - \alpha^{-1}$

$= 0$

$\Rightarrow S$ is a subfield of L. ($F_p \subseteq S \subseteq L$)

Since S contains all roots of $f(x)$, $f(x)$ splits on $L \Rightarrow L = S$

And number of elements in the field is p^n

Lemma: Let M be a degree n extension of F_p, then $\#M = p^n$

$[M : F_p] = n$

α_i be the bases of M over F_p

Lemma: Let M be a degree n extension of F_p, then $\#M = p^n$

$[M : F_p] = n$

Then let $a_1, a_2, \cdots, a_n$ be the bases of M over F_p

Then $M = \{a_0 a_0 + a_1 a_1 + \cdots + a_n a_n \mid a_i \in F_p\}$

$|M| = p \cdot p \cdots p = p^n$, $M^\times = M \setminus \{0\}$ is multiplicative group

$|M^\times| = p^n - 1$

By Lagrange theorem

If $a \in M^\times$, $|a| \mid |M^\times| = p^n - 1$

$\Rightarrow |a| \mid p^n - 1$

$\Rightarrow a^{p^n - 1} = 1$

$a^{p^n} - a = 0$

$\Rightarrow a$ is a root of $x^{p^n} - x$

$\Rightarrow$ Every elem of M is a root of $x^{p^n} - x$ Up to F_p isomorphism

$M \subseteq L$ (We've shown $L = S$)

But $\#M = \#L = p^n$

$\Rightarrow M = L$

Proposition: Let $n \in \mathbb{N}$, up to F_p-isomorphism, there is a unique degree n extension of F_p.

Such an extension is a splitting field of $x^{p^n} - x$ over F_p

Lemma: Let $n \in \mathbb{N}$, $F_{p^n}^\times$ is a cyclic group.

pf: Let $r \in \mathbb{N}$ be the smallest r such that $a^r = 1$ for all $a \in F_{p^n}^\times$

$a^{r+1} = a$, $\Rightarrow a^{r+1} - a = 0$

Then a is the root of $x^{r+1} - x$ $\forall a \in F_{p^n}^\times$

$\Rightarrow r + 1 \geq p^n$

By $\forall a \in F_{p^n}$, a is the root of $x^{r+1} - x$

Then are at least p^n solutions

$\Rightarrow r \geq p^n - 1$

So $r = p^n - 1$

If $a \in F_{p^n}^\times \Rightarrow a^{p^n - 1} = 1$

By the Lagrange theorem $\Rightarrow a^{p^n - 1} = 1 \ \forall a \in F_{p^n}^\times$

$\Rightarrow r \leq p^n - 1$

Since $|F_{p^n}^\times| = p^n - 1$

$\Rightarrow a^{p^n - 1} = 1 \ \forall a \in F_{p^n}^\times$

$\Rightarrow F_{p^n}^\times$ is a cyclic group

Def: If G is a finite group, the exponent of G is the smallest $r \in \mathbb{N}$ such that $g^r = 1$ for all $g \in G$.

S_3 : smallest is 6.

FACT: If G is a finite abelian group, there exists $g \in G$ such that $|g|$ = exponent of G.

$\Rightarrow \exists \beta \in F_{p^n}^\times$ s.t. $|\beta| = p^n - 1$ by $F_{p^n}^\times$ is finite abelian group.

Lemma: $n \in \mathbb{N}$, F_{p^n} is Galois over F_p, $G = Gal(F_{p^n}/F_p)$

$|G| = [F_{p^n} : F_p] = n$

$\sigma_p : F_{p^n} \to F_{p^n}$

$\sigma_p \in Gal(F_{p^n}/F_p)$ By previous proof.

$\langle \sigma_p \rangle \leq G$

$\langle \sigma_p \rangle = G$

pf: F_{p^n} is the splitting field of $f(x) = x^{p^n} - x$ over F_p. And ($f'(x) = -1 \Rightarrow$ each root has multiplicity one)

Then write $f(x) = g_1(x) g_2(x) \cdots g_n(x)$, $g_i(x)$ are irreducibles in $F_p[x]$.

We can see that each $g_i(x)$ extend to one field which is Galois over previous field.

F_{p^n}

$F_p(a_1 \cdots a_k)(\beta_1 \cdots \beta_k)$

$\mid g_2$

$F_p(a_1, \cdots a_k)$

$\mid g_1$

F_p

$\Rightarrow [F_{p^n} : F] = Gal(F_{p^n}/F)$

(Some theorem in previous chapter)

$\Rightarrow F_{p^n}$ is Galois over F_p.

To show $|\sigma_p| = n$

$\sigma_p(a) = a^p$

$\sigma_p^2(a) = \sigma(\sigma(a)) = \sigma(a^p) = a^{p^2}$

$\sigma_p^i(a) = a^{p^i}$

If $\sigma_p^i(a) = a \ \forall a \in F_{p^n}$ (i.e. σ^i is an identity map)

$\Rightarrow a^{p^i} = a \ \forall a \in F_{p^n}$

This is impossible if $i < n$ since there are only p^i roots for $x^{p^i} - x$.

Thus $i \geq n$. $\Rightarrow |\sigma_p| = n$ By $a^{p^n} = a \ \forall a \in F_{p^n}$

This is actually the claim from book, check pg 562.

Proposition: Let E be the splitting field over F of polynomial $f(x) \in F[x]$. Then

$|Aut(E/F)| \leq [E : F]$ with equality if $f(x)$ is seperable over F.

Now, consider $f(x) = g_1(x) g_2(x) \cdots g_n(x)$

Then, By induction, suppose $E = F(a_1)$

Then if $f(x)$ is seperable,

One can show $[Aut(E/F)] = [E : F]$

By carefully mapp a to it's different roots.

$\Rightarrow a^{p^i} = a \quad \forall a \in F_{p^n}$

This is impossible if $i < n$ since there are only p^i roots for $x^{p^i} - x$.

Thus $i \geq n$. $\Rightarrow |\sigma_p| = n$ By $a^{p^n} = a \quad \forall a \in F_{p^n}$

$\Rightarrow |\langle \sigma_p \rangle| \geq |Gal(F_{p^n}/F_p)|$

$\Rightarrow \langle \sigma_p \rangle = Gal(F_{p^n}/F_p)$

Prop: If α is an element of algebraic extension of F_p s.t. $[F_p(\alpha) : F_p] = n$ ($\Rightarrow F_p(\alpha) \cong F_{p^n}$, splitting field of $x^{p^n} - x$ over F_p)

Then (1) the root of $m_{\alpha, F_p}(x)$ are $\{\alpha, \alpha^p, \cdots\cdots, \alpha^{p^{n-1}}\}$

(2) Let φ_p be the Frobenius automorphism on $\overline{F_p}$, $\varphi_p(\beta) = \beta^p$

This actually has infinite degree

$\varphi_p|_{F_p(\alpha)} \in Aut(F_{p(\alpha)}/F_p)$ has order n. This implies $F_p(\alpha)$ is Galois over F_p and $Gal(F_{p(\alpha)}/F_p) = \langle \varphi_p|_{F_p(\alpha)} \rangle$

(1) pf: Let $f(x) = m_{\alpha, F_p(x)} \in F_p[x]$

$\varphi_p(\beta) = \beta^p = \beta \quad \forall \beta \in F_p$

$f(\alpha) = 0 \Rightarrow \varphi_p(f(\alpha)) = 0$

$\varphi_p(f(\alpha)) = f(\varphi_p(\alpha)) = 0$

$\Rightarrow \varphi_p(\alpha)$ is root of $f(x)$

$\Rightarrow \alpha^p$ is a root of $f(x)$

Then $(\alpha^p)^p = \alpha^{p^2}$ is a root of $f(x)$

$\cdots\cdots\cdots$ $\alpha^{p^{n-1}}$ is a root of $f(x)$

Now, let's show $\{\alpha^{p^j} \mid j \in \mathbb{N}\}$ contains n distinct elements $\alpha, \alpha^p, \cdots\cdots, \alpha^{p^{n-1}}$

Suppose $\alpha^{p^i} = \alpha^{p^j}$ for some $0 \leq j < i \leq n-1$

$(\alpha^{p^i})^{p^{n-i}} = (\alpha^{p^j})^{p^{n-j}} = \alpha^{p^n} = \alpha$ By $F_p(\alpha) \cong F_{p^n}$, so α is a root of $x^{p^n} - x$ over F_p

$\Rightarrow \alpha^{p^{n-j+i}} = (\alpha^{p^n})^{p^{i-j}} = \alpha^{p^{i-j}} = \alpha$

$\alpha \in$ Splitting field of $x^{p^{i-j}} - x$ over F_p $\rightarrow F_{p^{i-j}}$

$\alpha \in F_{p^{i-j}} \Rightarrow F_p(\alpha) \subseteq F_{p^{i-j}}$

$\Rightarrow [F_p(\alpha) : F_p] \leq [F_{p^{i-j}} : F_p] = i - j$

Whereas we have $[F_p(\alpha) : F_p] = n > i - j$

Contradict

$\Rightarrow$ such i and j doesn't exist.

(2) Followed by previous Lemma.

Lemma: Let $n \in \mathbb{N}$,

(1) If $f(x) \in F_p[x]$ is irreducible of degree n, then $f(x)$ divides $x^{p^n} - x$ (Check proposition before)

(2) $x^{p^n} - x$ is the product of all monic irreducible polynomials in $F_p[x]$ of degree $d | n$.

pf: (1) Consider $f(\alpha) = 0$, then let's assume $f(x)$ is monic

Then $f(x) = m_{\alpha, F_p}(x)$

$\Rightarrow [F_p(\alpha) : F_p] = n$

And by proposition before, we know that

α is the solution of $x^{p^n} - x$

$\Rightarrow m_{\alpha, F_p}(x) \mid x^{p^n} - x$

(2) Say $d | n$, $f_d(x) =$ monic irreducible polynomial of degree d, $\in F_p[x]$

Let α be a root of $f_d(x)$ in splitting field of $f_d(x)$

Then $[F_p(\alpha) : F_p] = d \Rightarrow [F_{p^n} : F_p(\alpha)] = \frac{n}{d}$

By $|Gal(F_{p^n}/F_p)| = n \Rightarrow$ a unique H s.t. $|H| = \frac{n}{d}$ and cyclic

Then coppose $\forall K$ s.t. $[F_{p^n} : K] = \frac{n}{d}$

$\Rightarrow$ Then F_{p^n} is Galois over K

and $|Gal(F_{p^n}/K)| = |H|$

$\Rightarrow Gal(F_{p^n}/K) = H$ (By uniqueness of H)

$\Rightarrow K = F_{p^n}^{Gal(F_{p^n}/K)}$

$\Rightarrow F_{p^n}^H = K$

$\Rightarrow F_p(\alpha) = F_{p^n}^H$

Since $[F_p(\alpha) : F_p] = d$

Let's call $F_p(\alpha) = F_{p^d}$

$\Rightarrow \alpha$ is a root of $x^{p^d} - x$

$\alpha^{p^d} = \alpha$

$\alpha^{p^{2d}} = (\alpha^{p^d})^{p^d} = \alpha^{p^d} = \alpha$

$\frac{n}{d} = k \Rightarrow \alpha^{p^{kd}} = \alpha$

$\Rightarrow \alpha^{p^n} = \alpha$

$\Rightarrow \alpha$ is also the root of $x^{p^n} - x$ over F_p

Thus α is the elem of F_{p^n} (i.e. splitting field of

Then if $f(x)$ is separable,

One can show $[Aut(E/F)] = [E:F]$

By carefully mapp α to it's different roots.

Suppose this is true for $n = k$

$E = F(\alpha_1, \cdots\cdots, \alpha_k)$

Then $|Aut(E/F)| = [E:F]$ if $f(x)$ is separable

Now, with $n = k+1$

when $E = F(\alpha_1, \cdots\cdots, \alpha_k, \alpha_{k+1})$

E is a splitting field of $f(x)$ over F

$\Rightarrow E$ is a splitting field of $f(x)$ over $F(\alpha_{k+1})$, and $f(x)$ is separable

$\Rightarrow |Aut(E/F(\alpha_{k+1}))| = [E : F(\alpha_{k+1})]$, and We stuck here, as I mentioned in the "Field Exercise" This method is broken.

Example: $Q(2^{\frac{1}{3}}, 2^{\frac{1}{3}}e^{\frac{2\pi i}{3}}, 2^{\frac{1}{3}}e^{\frac{4\pi i}{3}})$ is Galois over Q

$\Rightarrow Q(2^{\frac{1}{3}}, 2^{\frac{1}{3}}e^{\frac{2\pi i}{3}}, 2^{\frac{1}{3}}e^{\frac{4\pi i}{3}})$ is Galois over $Q(2^{\frac{1}{3}})$

$(x^3 - 2) = (x - 2^{\frac{1}{3}})(x^2 + 2^{\frac{1}{3}}x + 2^{\frac{2}{3}})$

$2^{\frac{1}{3}} \rightarrow 2^{\frac{1}{3}}e^{\frac{2\pi i}{3}}$

$i(2^{\frac{1}{3}}e^{\frac{2\pi i}{3}}) = i(2^{\frac{1}{3}})\, i(e^{\frac{2\pi i}{3}})$

$= 2^{\frac{1}{3}}e^{\frac{2\pi i}{3}} \cdot e^{\frac{4\pi i}{3}}$

$= 2^{\frac{1}{3}}$

$i(2^{\frac{1}{3}}e^{\frac{4\pi i}{3}}) = i(2^{\frac{1}{3}})\, i(e^{\frac{4\pi i}{3}})$

$= 2^{\frac{1}{3}}e^{\frac{2\pi i}{3}}e^{\frac{8\pi i}{3}}$

$= 2^{\frac{1}{3}}e^{\frac{10\pi i}{3}} = 2^{\frac{1}{3}}e^{\frac{4\pi i}{3}}$

One can see that it is not a good idea to use only one α_{k+1}, since it's hard to justify

Thus this is how we do it. Let $f(x) = g_1(x)g_2(x)\cdots\cdots g_m(x)$

s.t. $g_i(x)$ is irreducible.

And let $\alpha_m^1, \alpha_m^2, \cdots\cdots \alpha_m^t$ be the root of $g_m(x)$

Then E is the splitting field over $F(\alpha_m^1, \cdots\cdots \alpha_m^t)$ of $f(x)$

$\Rightarrow |Aut(E/F(\alpha_m^1 \cdots\cdots \alpha_m^t))| = [E : F(\alpha_m^1 \cdots\cdots \alpha_m^t)]$

By inductive assumption, let's just assume all $\deg g_i(x) \geq 2$, so that no roots in F.

And As I mentioned before, it map roots to roots up to minimal polynomial. (Using irreducible and $\sigma \in Aut(E/F)$ can argue this)

And $|Aut(F(\alpha_m^1 \cdots\cdots \alpha_m^t)/F)| = ?$

Same method, $F(\alpha_m^1 \cdots\cdots \alpha_m^t)$ is a splitting field of $g_m(x)$ over F

And $g_m(x)$ is also separable by $f(x)$ is separable and $g_m(x) | f(x)$

$\Rightarrow |Aut(F(\alpha_m^1 \cdots\cdots \alpha_m^t)/F)|$

$= [F(\alpha_m^1 \cdots\cdots \alpha_m^t) : F]$

Therefore, $|Aut(E/F)| = |Aut(\cdots\cdots)|\,|Aut(\cdots\cdots)| = [E:F]$

$\Rightarrow \alpha^{p^n} = \alpha$

$\Rightarrow \alpha$ is also the root of $x^{p^n} - x$ over F_p

Thm α is the elmt of F_{p^n} (i.e. splitting field of $x^{p^n} - x$ over F_p)

$\Rightarrow f_d(x) \mid x^{p^n} - x$

We haven't finish the proof yet. This only shows the $\Pi_{d|n,\deg(g)=d}\, g(x) \mid x^{n^p} - x$, we still need to show the equivalent.
Claim: $\Pi_{d|n,\deg(g)=d}\, g(x) = x^{n^p} - x$
proof: Suppose g(x) is a irreducible polynomial such that degree of g(x) = d such that $g(x) | x^{n^p} - x$, notice I don't claim $d|n$, I am trying to prove $d|n$. Then the roots of $g(x)$ is also the roots of $x^{n^p} - x$, let α be the root of $g(x)$, then since α is also the the root of $x^{n^p} - x$, thus $\alpha \in F_{p^n}$, implies $F_p(\alpha) \leq F_{p^n}$, therefore, it is a subfield of F_{p^n}, then $d|n$.
This completes the proof.

Corollary: Let $n \in \mathbb{N}$, let $f(x), g(x) \in F_p[x]$ be irreducible of degree n. Let $\alpha, \beta \in \overline{F_p}$ be such that $f(\alpha) = g(\beta) = 0$

Then $F_p(\alpha) \cong F_p(\beta)$

$F_p[x]/(f(x))$, $F_p[x]/(g(\beta))$

(Any 2 degree n extensions of F_p are F_p isomorphic)