Notes on Galois Theory

BY WENCHAO ZHANG
SUSTC

June 10, 2020

Abstract

This note is a rearrangement of the lecture notes for the Galois theory at South University of Science and Technology of China, 2012. This supplementary course is taught by Prof. Jie-Tai Yu. The original scanned version by Camscanner is archived on Nutstore (older account) and Onedrive (SUSTC).

Table of contents

1 Introduction

There are four main theorems in the Galois theory.

Theorem 1.1. *For any polynomial* $f \in k[x]$ *with* $\deg(f) = 0$*, we can uniquely determine* $\mathrm{Gal}(f)$*.*

Note. $\mathrm{Gal}(f)$ is the symmetric group of roots and it keeps the coefficients of f unchanged.

Theorem 1.2. $f(x) = 0$ *is solvable if and only if* $\mathrm{Gal}(f)$ *is solvable.*

Theorem 1.3. *The Galois group of the general polynomial equation* $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ *is* $\mathrm{Gal}(f) = S_n$*.*

The coefficients $a_0, \ldots, a_{n-1}$ are independent symbols.

Theorem 1.4. S_n $(n \geqslant 5)$ *is unsolvable.*

Here is the relations for those theorems between algebra equations and Galois groups.

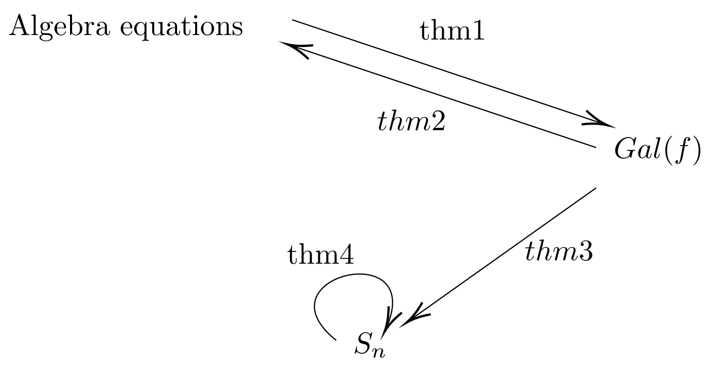

Figure 1.1. Relations for main theorems

2 Field extension

F, K, E, L, A are always represent fields.

Definition 2.1. (extension) $F \subseteq K \Leftrightarrow K \supseteq F \Leftrightarrow K/F \Leftrightarrow \begin{array}{c} K \\ | \\ F \end{array}$.

Remark 2.2. K/F implies that K is a F-vector space.

Definition 2.3. (finite extension) $\dim(K/F) := [K\colon F]$, *if* $\dim(K/F)$ *is finite, then we call* K/F *a finite extension.*

Example 2.4. $[\mathbb{C}\colon \mathbb{R}] = 2$, and $\{1, \sqrt{-1}\}$ is a $\mathbb{R}$-basis of $\mathbb{C}$.

Theorem 2.5. (tower of extensions) *If there are two finite extensions,* K/E, E/F *with* $[K\colon E] = m$, $[E\colon F] = m$ *respectively, then* K/F *is also a finite extension such that* $[K\colon F] = mn$.

Proof. Consider an E-basis $\{\alpha_i\}_1^n$ of K and a F-basis $\{\beta_j\}_1^m$ of E, then $\{\alpha_i\beta_j\}_{1,1}^{n,m}$ is a F-basis of K, whose dimension is mn. □

Definition 2.6. (algebraic extension) α *is algebraic over* F*, if there exists* $f(x) \in F[x]$ *with* $\operatorname{def}(f) \geqslant 1$ *s.t.* $f(\alpha) = 0$. α *is called an algebraic element over* F.

If $\forall \alpha \in K$*, s.t.* α *is always algebraic over* F*, then* K/F *is called an* ***algebraic extension****.*

Theorem 2.7. *A finite extension is always an algebraic extension.*

Proof. Let $[K\colon F] = n$, then we have $\forall \alpha \in K$, $\{1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^n\} \subseteq K$ are linear dependent (since there are $n+1$ elements). Thus there exist $b_0, b_1, \ldots, b_n \in F$ with at least one nonzero element, s.t.

$$b_0 \cdot 1 + b_1\alpha + \cdots + b_n\alpha^n \equiv 0$$

Define $f(x) = b_0 + b_1 x + \cdots + b_n x^n \in F[x]$, then $f(\alpha) = 0$. Hence α is algebraic over F. □

Remark 2.8. The converse result is not true. There are infinite algebraic extensions, for example, let $\mathbb{A}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, then $[\mathbb{A}:\mathbb{Q}]=\infty$. However, α is algebraic over F, if and only if $[F[\alpha]:F]<\infty$.

代数扩张本身并不一定是有限扩张, 但可表作有限子扩张的归纳极限。

Definition 2.9. (fractional field) *$F(u)$ is the smallest field containing F and u, i.e.*

$$F(u):=\left\{\frac{f(u)}{g(u)}\middle| f(x),g(x)\in F[x], g(u)\neq 0\right\}.$$

Theorem 2.10. *u is algebraic over F if and only if $F(u)=F[u]=\{f(u)|f(x)\in F[x]\}$.*

Proof. "$\Rightarrow$" We only need to proof $\frac{1}{g(u)}$ $(g(u)\neq 0)$ can be written as a polynomial of u. Let $p(x)\in F[x]$ be the minimal polynomial of u in $F[x]$, s.t. $p(u)=0$.

Then $p(x)$ is irreducible over F. We claim that for any $f(x)\in F[x]$ with $f(u)=0$, we have $p(x)|\,f(x)$. Actually, $f(x)=q(x)p(x)+r(x)$ with $\deg(r(x))<\deg(p(x))$, so $r(u)=0$ thus $r(x)=0$ (because of the minimality of $p(x)$.).

So for $g(u)\neq 0$, $p(x)\nmid g(x)$. By Bezout's identity, there exist $a(x),b(x)\in F[x]$ such that $a(x)p(x)+b(x)g(x)=1$. Then $b(u)g(u)=1$ which implies $\frac{1}{g(u)}=b(u)$.

"$\Leftarrow$" Because $F(u)=F[u]$ then $1/u\in F[u]$, thus there exists $f(u)=1/u$, i.e. $uf(u)-1=0$. Let $g(x)=xf(x)-1\in F[x]$, then $g(u)=0$, i.e. u is algebraic over F. $\square$

Example 2.11. $\mathbb{R}[i]=\mathbb{R}(i)\Rightarrow 1/i=f(i)=-i$, i.e. $g(x)=-x^2-1$ is the characteristic polynomial of i. On the other hand, i is algebraic over $\mathbb{R}$. For example, consider $g(i)=2i+1$, $\frac{1}{2i+1}=\frac{2i-1}{-5}=\frac{1-2i}{5}$.

This can be obtained by Bezout's identity as well: the minimal polynomial of i is $p(x)=x^2+1$. Then there exists $a(x)p(x)+b(x)g(x)=a(x)(x^2+1)+b(x)(2x+1)=1$. We can use the Euclidean algorithm.

$$\begin{aligned}(x^2+1) &= (2x+1)\left(\frac{1}{2}x+1\right)-\frac{5}{2}x\\ 2x+1 &= \left(-\frac{5}{2}x\right)\left(-\frac{4}{5}\right)+1\\ -\frac{5}{2}x &= 1\times\left(-\frac{5}{2}x\right)\end{aligned}$$

By the penultimate(倒数第二个) identity,

$$\begin{aligned}1 &= (2x+1)+\frac{4}{5}\left(-\frac{5}{2}x\right)\\ &= (2x+1)+\frac{4}{5}\left[(x^2+1)-(2x+1)\left(\frac{1}{2}x+1\right)\right]\\ &= (2x+1)\left[1-\frac{4}{5}\left(\frac{1}{2}x+1\right)\right]+\frac{4}{5}(x^2+1)\\ &= (2x+1)\left(\frac{1-2x}{5}\right)+\frac{4}{5}(x^2+1)\end{aligned}$$

i.e. $a(x)=\frac{4}{5}$, and $b(x)=\frac{1-2x}{5}$.

Remark 2.12. The monic and irreducible polynomial which vanishes u for an algebraic extension $F(u)/F$ is called the minimal polynomial in $F[x]$ of u, and is denoted by $\mathrm{MinPoly}_F(u)$.

Theorem 2.13. *Let u be algebraic over F, then $[F(u)\colon F]=\deg(\mathrm{MinPoly}_F(u))$.*

Proof. For $F(u)=F[u]$, we want to prove that $\{1,u,\ldots,u^{n-1}\}$ is a F-basis of $F[u]$.

1) Suppose

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

is the minimal polynomial of u, then $p(u)=0$. Thus

$$u^n=-(a_{n-1}u^{n-1}+\cdots+a_0)$$

i.e. any $f(u)$ can be represent by the basis.

2) All the elements inside the basis are linear independent, if not then there exists a smaller degree polynomial vanishes u, which contradicts to the minimality of $p(x)$.

In summary, we have $[F(u)\colon F]=\deg(\mathrm{MinPoly}_F(u))$. □

Theorem 2.14. *If α, β are algebraic over F, so are $\alpha\pm\beta$, $\alpha\beta$ and α/β $(\beta\neq 0)$.*

Theorem 2.15. *Let K/F be a field extension, and $E:=\{\alpha\in K|\alpha \text{ is algebraic over } F\}$. Then $K/E/F$ and E/F is algebraic.*

Such E is called *algebraic closure* of F in K.

Theorem 2.16. (tower of algebraic extensions) *If K/E, E/F are algebraic extensions, then K/F is algebraic as well.*

Proof. $\forall a\in K$, let $\mathrm{MinPoly}_E(\alpha)=x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$, thus $F(b_0,\ldots,b_{n-1},a)/F(b_0,\ldots,b_{n-1})$ is algebraic (finite). Note that $F(b_0,\ldots,b_{n-1})/F$ is algebraic and finite. Thus by Theorem tower of finite extensions, $F(b_0,\ldots,b_{n-1},a)/F$ is finite, hence algebraic. □

Definition 2.17. (composition) *Suppose E,F contained in some larger field, the smallest field containing F and E is called composition field, which denoted by $FE=EF=F(E)=E(F)$.*

Definition 2.18. (lifting) *If we have K/F and E/F, then we called KE/E a lifting of K/F, and KE/K a lifting of E/F.*

$$\begin{tikzcd}[arrows=dash]
 & KE \arrow[dl] \arrow[dr] & \\
K \arrow[dr] & & E \arrow[dl] \\
 & F &
\end{tikzcd}$$

Theorem 2.19. *If K/F is algebraic, then the lifting KE/E is also algebraic.*

Proof. We consider an arbitrary elements α in K, then α is algebraic over F. Since E/F, we have α is also algebraic over E (coefficients are in F must be in E). By Theorem 2.14, for any $\beta \in E$, we have $\alpha\beta, \alpha \pm \beta, \alpha/\beta$ (for $\beta \neq 0$) is algebraic over E. Hence, we have all elements of KE is algebraic over E, i.e. KE/E is algebraic. □

Theorem 2.20. *If K/F is finite, then the lifting KE/E is also finite.*

Proof. Assume $[K:F]=n$, such that $K=F(\alpha_1,\ldots,\alpha_n)$, thus $KE=EF(\alpha_1,\ldots,\alpha_n)=E(\alpha_1,\ldots,\alpha_n)$. Consider two towers of finite extensions:

$$\begin{array}{c} F(\alpha_1,\ldots,\alpha_n) \\ | \\ F(\alpha_1,\ldots,\alpha_{n-1}) \\ | \\ F(\alpha_1) \\ | \\ F \end{array}, \quad \begin{array}{c} E(\alpha_1,\ldots,\alpha_n) \\ | \\ E(\alpha_1,\ldots,\alpha_{n-1}) \\ | \\ E(\alpha_1) \\ | \\ E \end{array}$$

Since $\deg(\mathrm{MiniPoly}_F(\alpha_i)) \geqslant \deg(\mathrm{MiniPoly}_E(\alpha_i))$, thus by induction $[KE:E] \leqslant [K:F]=n$. □

Definition 2.21. (Composition of field extensions) *KE/F is the composition of K/F and E/F.*

$$\begin{tikzcd} & KE \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\ K \arrow[dr, dash] & & E \arrow[dl, dash] \\ & F & \end{tikzcd}$$

Theorem 2.22.

1. *If K/F, E/F are finite, then KE/F is finite.*
2. *If K/F, E/F are algebraic, then KE/F is algebraic.*

Proof. K/F is finite(resp. algebraic) $\Rightarrow$ KE/E is finite (resp. algebraic) because of lifting. E/F is finite, hence by the tower properties, KE/F is finite (resp. algebraic). □

Definition 2.23. (embedding) *An embedding $F \overset{\varphi}{\hookrightarrow} L$ is a field injective homomorphism from F into L.*

$$F \overset{\sigma}{\to} \sigma(F) \overset{\mathrm{id}}{\hookrightarrow} L.$$

Definition 2.24. (τ acts on function) *Let $g(\alpha) \in F[\alpha]$ and $F[\alpha] \overset{\tau}{\hookrightarrow} L$. Then*

$$\tau(g)(x) = \tau(b_n)x^n + \cdots + \tau(b_0) \in \tau(F)[x].$$

$g(x)$ is irreducible over $F \Longleftrightarrow \tau(g)(x)$ is irreducible over $\tau(F)$.

α is a root of $g(x) \Longleftrightarrow \beta := \tau(\alpha)$ is a root of $\tau(g)(x)$.

Definition 2.25. (restriction of embedding) *Let $K\,/\,F$ be a field extension, $K \overset{\tau}{\hookrightarrow} L$ is an embedding, then we call $\tau|_F = \sigma$ the restriction of embedding from F into L. i.e. $\forall a \in F$, $\tau(a) = \sigma(a)$.*

On the contrary, τ is an extension embedding of σ on K.

Note. There is a unique restriction for fixed embedding, while there are several extension for a certain embedding.

Theorem 2.26. *The number of extension τ over σ for the field extension $F(\alpha)\,/\,F$ equals to the number of distinct roots of $\sigma(p)(x)$ in L, where $p(x)$ is the minimal polynomial of α over F. In particular, this number is $\leqslant [F(\alpha){:}\, F]$.*

$$\begin{tikzcd}
\tau \arrow[d, no head] & F(\alpha) \arrow[d, no head] \arrow[dr] & \\
\sigma & F \arrow[r] & L
\end{tikzcd}$$

Proof. Let β be a root of $\sigma(g)(x)$ in L,

$$\forall g(\alpha) = b_n\alpha^n + \cdots + b_1\alpha + b_0,\ \ b_i \in F \text{ are not all zero}$$

we may define $\tau(g(\alpha)) = \sigma(g)(\beta) = \sigma(b_n)\beta^n + \cdots + \sigma(b_0) \in L$. We prove that τ is a homomorphism and extension, since $\tau(g(\alpha) + h(\alpha)) = \tau(g(\alpha)) + \tau(h(\alpha))$, $\tau(g(\alpha)h(\alpha)) = \tau(g(\alpha))\tau(h(\alpha))$ and $\tau|_F = \sigma$, $\tau(\alpha) = \sigma(\alpha)$.

Then $F[\alpha] \cong F[X]\,/\,\langle p(x)\rangle \cong \frac{\sigma(F)[X]}{\langle \sigma(p)(x)\rangle} \cong \sigma(F)[\beta]$. □

Definition 2.27. (separable element) *An algebraic element α over F is called separable over F iff $\mathrm{MinPoly}_F(\alpha)$ has no multiple roots in any extension field of F.*

Note 2.28. For separable element α, $[\tau{:}\,\sigma] = [F(\alpha){:}\, F] = \deg(\mathrm{MinPoly}_F(\alpha))$.

If F is characteristic 0, then any algebraic element α is naturally separable.

Theorem 2.29. *Let F be a field $f(x) \in F[x]$ ($\deg f \geqslant 1$) has no multiple roots in any extension field of F iff $\gcd(f(x), f'(x)) = 1$.*

Proof. (sketch) Consider $f(x) = (x - a)^m g(x)$. □

Corollary 2.30. *If $\mathrm{char}(F) = 0$, $p(x) \in F[x]$ is irreducible over F, then $p(x)$ has no multiple roots.*

Proof. Let $\deg(p(x)) = n$, then $\deg(p'(x)) = n - 1$, since $p'(x) \not\equiv 0$, hence $\gcd(p(x), p'(x)) = 1$. By Theorem 2.29, there is no multiple roots. □

Theorem 2.31. *Let F be a finite field, then every algebraic elements α over F is separable.*

Proof. Let $|K{:}\,\mathbb{F}_q| = n$, choose $\{u_1, u_2, \ldots, u_n\}$ as an $\mathbb{F}_q$ basis of K. Then any element of K can be written as

$$a = b_1u_1 + \cdots + b_nu_n, b_i \in \mathbb{F}_q$$

For each b_i, we have q choices, then we have q^n distinct elements. $\square$

Corollary 2.32. *Let F be a finite field,* $\mathrm{char}(F) = p$, *then* $F = \mathbb{F}_{p^m}$ $(m \geqslant 1)$.

Consider $\mathbb{F}_{p^m}(\alpha) / \mathbb{F}_{p^m}$, and $\deg(\mathrm{MinPoly}_{\mathbb{F}_q}(\alpha)) = n$, then $\mathbb{F}_{p^{mn}}^*$ is a group with $p^{mn} - 1$ elements. We then have $\alpha^{p^{mn}-1} = 1 \Longrightarrow \alpha^{p^{mn}} - \alpha = 0$ (no multiple roots.)

Theorem 2.33. (separable extension) *Let K/F be finite. K/F is called separable if $[K{:}\,F]$ equals the number of distinct τ.*

Proposition 2.34. *K/F is separable $\Longleftrightarrow$ $\forall \alpha \in K$, α is separable over F.*

Proof. "$\Leftarrow$" Consider algebraic extension $K = F(\alpha_1, \alpha_1, \ldots, \alpha_n) / F(\alpha_1, \ldots, \alpha_{n-1}) / \cdots / F$ and the extension of embedding $\tau / \sigma_{n-1} / \cdots / \sigma$.

"$\Rightarrow$" Suppose on the contrary K/F is separable but $\exists \alpha \in K$ is in separable over F. Consider the extension $\bar{\sigma}{:}\, F(\alpha) \to L$ of embedding $\sigma{:}\, F \to L$. Then the distinct τ over $\bar{\sigma}$ is $\leqslant [K{:}\, F(\alpha)]$ and distinct $\bar{\sigma}$ over σ is $< [F(\alpha){:}\, F]$. Thus the distinct τ over σ is $< [K{:}\, F(\alpha)][F(\alpha){:}\, F] = [K{:}\, F]$. $\square$

Note 2.35. The infinite extension of $\mathbb{F}_p$ is an example of non-separable extension. In fact, consider $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, $F = \mathbb{F}_2(u^2)$ and $K = \mathbb{F}_2(u)$. Then $\mathrm{Minpoly}_F(u) = (x - u)^2 = x^2 - u^2$. But there is only 1 embedding (identity) over F.

Definition 2.36. (primitive element) *Suppose $K = F(u)$, then u is called a primitive element of K over F.*

Lemma 2.37. *Suppose $K/\mathbb{F}_q$ is finite, then $\exists \alpha \in K$ such that $K = \mathbb{F}_q(\alpha)$.*

Proof. $[K{:}\, \mathbb{F}_q] = n$, then $K = \mathbb{F}_{q^n}$, hence $K - \{0\}$ is a cyclic group,

$$K - \{0\} = \{1, \alpha, \alpha^2, \ldots, \alpha^{q^n - 2}\},$$

Thus $K = \mathbb{F}_q(\alpha)$. $\square$

Theorem 2.38. *Let K/F be **finite separable** extension, then $\exists \alpha \in K$, such that $K = F(\alpha)$.*

Proof. We only prove F is infinite case. WLOG, we may assume $K = F(\beta, \gamma)$. Since $K = F(\alpha_1, \ldots, \alpha_r) = F(\alpha_3, \ldots, \alpha_r)(\alpha_1, \alpha_2) = E(\alpha_1, \alpha_2)$.

$$\begin{tikzcd}
\sigma \arrow[d, dash] & K = F(\beta, \gamma) \arrow[d, dash] \arrow[ddr] & \\
\bar{\sigma} \arrow[d, dash] & F(\alpha) \arrow[d, dash] \arrow[dr] & \\
\mathrm{Id} & F \arrow[r] & A
\end{tikzcd}$$

Figure 2.1. extension of fields and embeddings

Suppose $[K{:}\, F] = n$, $\#\sigma = n$ and $\#\bar{\sigma} \leq [F(\alpha){:}\, F]$. On the other hand,

$$[F(\beta, \gamma){:}\, F(\alpha)][F(\alpha){:}\, F] = [K{:}\, F] = n$$

Since $[F(\beta,\gamma):F(\alpha)] \geqslant \#\sigma/\bar{\sigma}$, $[F(\alpha):F] \leqslant \#\bar{\sigma}$. Hence $[F(\alpha):F] = \#\bar{\sigma}$.

So we define

$$f(x) = \prod_{1\leqslant i\leqslant j\leqslant n} [\sigma_i(\beta + x\gamma) - \sigma_j(\beta + x\gamma)] = \prod_{1\leqslant i\leqslant j\leqslant n} [(\sigma_i(\beta) - \sigma_j(\beta)) + (\sigma_i(\gamma) - \sigma_j(\gamma))x]$$

Note that $\deg(f) \leqslant \binom{n}{2}$, $f \in A[X]$. For F is infinite, $\exists c \in F$, s.t. $f(c) \neq 0$. Then we have

$$\sigma_i(\beta) \neq \sigma_j(\beta), \sigma_i(\gamma) \neq \sigma_j(\gamma)$$

Thus $\#\bar{\sigma} = \#\sigma = n$, $F(\beta,\gamma) = F(\alpha)$. □

Definition 2.39. *We call τ is over F, if the following holds (i.e. fixed F)*

$$\begin{array}{ccc} \sigma & K & \searrow \\ | & | & \\ \mathrm{id} & F & \longrightarrow A \end{array}$$

Theorem 2.40. *Let K/F be algebraic, σ is an embedding from K into K over F, $\sigma(K) \subseteq K$. Then $\sigma(K) = K$ i.e. $\sigma \in \mathrm{Aut}(K/F)$.*

Proof. K/F is algebraic, for each $\alpha \in K$, α is algebraic over F. Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be all distinct roots of $\mathrm{MinPoly}_F(\alpha)$. Since σ is injective, σ is a permutation of $\{\alpha_1,\ldots,\alpha_r\}$. So $\exists \alpha_i$, s.t. $\sigma(\alpha_i) = \alpha$. Therefore, σ is surjective. □

For non algebraic extension, we won't get an automorphism.

Example 2.41. (counter example) Consider $K = F(u)$, $\varphi(F(u)) = F(u^2) \subsetneq F(u)$, where u is non-algebraic over F.

Definition 2.42. (normal extension) *K/F is finite. If $\sigma(K) = K$, i.e. σ induce an automorphism of K. Then K/F is called a normal extension.*

Example 2.43. (counter example) Consider the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, and the embedding to $\mathbb{C}$, i.e. $\sigma: \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ are extension of id. Then $\sigma_1 = \mathrm{Id}$, $\sigma_2: \sqrt[3]{2} \to \sqrt[3]{2}\omega$, $\sigma_3: \sqrt[3]{2} \to \sqrt[3]{2}\,\omega^2$. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

Definition 2.44. (split field) *$K = F(\alpha_1, \ldots, \alpha_n)$ is called split field of $f(x)$ over F for α_i are all roots of $f(x)$, and denoted by $K = \mathrm{Split}_F(f)$.*

Theorem 2.45. *K/F is normal $\Longleftrightarrow$ $K = \mathrm{Split}_F(f)$ for some $f(x) \in F[x]$.*

Proof. "$\Longleftarrow$" Suppose K is split field $K = F(\alpha_1, \ldots, \alpha_n)$. $f(x) = (x - \alpha_1)\cdots(x - \alpha_n) \in F[x]$. We only need to prove $\sigma(K) \subseteq K$ and $\sigma(\alpha_i) = \alpha_j \in K$.

"$\Longrightarrow$" $K = F(\alpha_1, \ldots, \alpha_r)$ is finite. $\mathrm{MinPoly}_F(\alpha_i) = p_i(x) \in F[x]$. Let $p(x) = \prod_{i=1}^r p_i(x) \in F[x]$. K is split field of $p(x)$. □

3 Galois Extension

Definition 3.1. **(embedding set)** *K/F is finite, define* $\mathrm{Emb}(K/F) := \{\sigma | \sigma: K \to A, \mathrm{Id}: F \to A, \sigma/\mathrm{Id}\}$

Note 3.2. We don't need condition $\sigma(K) \subseteq K$ for the definition.

Definition 3.3. **(fixed subfield)** *Let K/F be finite, $\varnothing \neq S \subseteq \mathrm{Emb}(K/F)$. Define*

$$K^S = \{\alpha \in K | \sigma(\alpha) = \alpha \,\text{for all}\, \sigma \in S\} \supseteq F$$

K^S, $K^{\mathrm{Emb}(K/F)}$ is a field and is a subfield of K.

Theorem 3.4. *Let K/F be separable. Then $K^{\mathrm{Emb}(K/F)} = F$.*

Proof. We have $K^S \supset F$, suppose on the contrary $K^{\mathrm{Emb}(K/F)} \supsetneqq F$. Then there exists $\alpha \in K^{\mathrm{Emb}(K/F)}$ but $\alpha \notin F$, such that $\mathrm{MinPoly}_F(\alpha) = p(\alpha)$, $\deg(p(x)) \geqslant 2$. Then we have another root $\beta \neq \alpha$. Hence there is additional embedding $\sigma(\alpha) = \beta$. $\sigma \in \mathrm{Emb}(K/F)$. But by the definition of K^S, $\sigma(\alpha) = \alpha$, which is a contradiction. $\square$

Example 3.5. **(counter example)** $\mathbb{F}_2(u) = K/F = \mathbb{F}_2(u^2)$, then $\mathrm{Emb}(K/F) = \{\mathrm{Id}\}$. However, $K^{\mathrm{Emb}(K/F)} = K^{\{\mathrm{Id}\}} = K \neq F$.

Since all embeddings of a normal extension is an automorphism of K, hence we have

Theorem 3.6. *If K/F is normal, then* $\mathrm{Emb}(K/F) = \mathrm{Aut}(K/F)$.

Definition 3.7. **(Galois extension)** *A finite extension K/F is called Galois iff K/F is normal and separable. In this case, we denote the Galois group*

$$\mathrm{Gal}(K/F) := \mathrm{Aut}(K/F).$$

Note 3.8. normal means all embeddings are automorphisms, separable means all embeddings are distinct.

Lemma 3.9. *If we have field extensions $K/E/F$, K/F is normal, then K/E is also normal.*

Theorem 3.10. *For field extension $K/E/F$, if K/F is Galois, then K/E is also Galois.*

$$K^{\mathrm{Gal}(K/E)} = K^{\mathrm{Emb}(K/E)} = E.$$

Theorem 3.11. *K/F is Galois, then* $\mathrm{Gal}(K/K^H) = H$.

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash] & \{\mathrm{Id}\} \arrow[d, dash] \\
K^H \arrow[r, dash] \arrow[d, dash] & H \arrow[d, dash] \\
F \arrow[r, dash] & \mathrm{Gal}(K/F)
\end{tikzcd}$$

Proof. Suppose $H = \{\sigma_1, \ldots, \sigma_r\}$. K / F is (finite) separable, $\exists \alpha \in K$ st. $K = F(\alpha) = K^H(\alpha)$. Define $f(x) = (x - \sigma_1\alpha) \cdots (x - \sigma_r\alpha)$. $\forall \sigma \in H$, we have

$$\sigma(f)(x) = (x - \sigma\sigma_1 x) \cdots (x - \sigma\sigma_r x)$$

$H = \{\sigma_1, \ldots, \sigma_r\} = \{\sigma\sigma_1, \ldots, \sigma\sigma_r\}$. It follows $f(x) = \sigma(f)(x)$. So the coefficients of $f(x)$ doesn't change through σ, thus $f(x) \in K^H[x]$.

On the other hand $f(\alpha) = 0$, $\mathrm{id} \in H$,

$$\mathrm{MinPoly}_{K^H}(\alpha) | f(x) \Longrightarrow [K : K^H] = [K^H(\alpha) : K^H] \leq \#H$$

While $[K^H(\alpha) : K^H] = \#\text{distinct embedding } K \text{ over } K^H = \#H$, hence

$$[K : K^H] = |H|$$

Every embedding of K / K^H is automorphism and K / K^H is normal and separable. Then K / K^H is Galois, and $\mathrm{Gal}(K / K^H) = H$. □

Theorem 3.12. (first fundamental theorem of Galois theory) *Let K / F be Galois and $K \geqslant E \geqslant F$, then K / E is Galois and $K^{\mathrm{Gal}(K / E)} = E$.*

For any subgroup of $\mathrm{Gal}(K / F)$, $H \subseteq \mathrm{Gal}(K, F)$. K / K^H is Galois and $\mathrm{Gal}(K / K^H) = H$. Define $A = \{E | K \geqslant E \geqslant F\}$, $B = \{H | H \subseteq \mathrm{Gal}(K / F)\}$.

$$\begin{array}{ll} \varphi : A \to B & \psi : B \to A \\ E \mapsto \varphi(E) = \mathrm{Gal}(K / E) & H \mapsto \psi(H) = K^H \end{array}$$

Then φ and ψ are bijective, counter-inclusion: $E_1 \leqslant E_2 \Rightarrow \mathrm{Gal}(K / E_1) \geqslant \mathrm{Gal}(K / E_2)$ and $H_1 \leqslant H_2 \Rightarrow K^{H_1} > K^{H_2}$. Moreover, $\varphi \circ \psi = \mathrm{Id}_B$, $\psi \circ \varphi = \mathrm{Id}_A$.

Note 3.13. φ, ψ are map between field and group, not homomorphism.

Lemma 3.14. *Let λ be any embedding from E into A over F, if K / E is Galois then $\lambda(K) / \lambda(E)$ is also Galois and*

$$\mathrm{Gal}(\lambda(K), \lambda(E)) = \lambda \mathrm{Gal}(K / E) \lambda^{-1}.$$

Proof. *Suppose $\sigma \in \mathrm{Gal}(K / E)$ only $\lambda\sigma\lambda^{-1}(\lambda(K)) = \lambda\sigma(K) = \lambda(K)$. For any $\lambda(\alpha) \in \lambda(E)$,$\alpha \in E$, $\lambda\sigma\lambda^{-1}(\lambda(\alpha)) = \lambda\sigma(\alpha) = \lambda(\alpha)$.* □

Theorem 3.15. (second fundamental theorem of Galois theory) *Let K / F be Galois, $K \geqslant E \geqslant F$, then E / F is Galois if and only if* $\mathrm{Gal}(K / E) \lhd \mathrm{Gal}(K / F)$.

In particular, if E / F is Galois, $\mathrm{Gal}(E / F) = \frac{\mathrm{Gal}(K / F)}{\mathrm{Gal}(K / E)}$.

Proof. "$\Longleftarrow$" Let λ be any embedding from E into A over F. λ can be extended to embedding of K into A over F. For K/F is Galois, so we have $\lambda(K)=K$. We only need to prove $\lambda(E)=E$.

$$\mathrm{Gal}(K/\lambda(E))=\mathrm{Gal}\,(\lambda(K)/\lambda(E))=\lambda\mathrm{Gal}(K/E)\lambda^{-1}=\mathrm{Gal}(K/E),$$

The last equality holds because that $\mathrm{Gal}(K/E)\lhd\mathrm{Gal}(K/F)$. Hence,

$$\lambda(E)=K^{\mathrm{Gal}(K/\lambda(E))}=K^{\mathrm{Gal}(K/E)}=E.$$

$$\begin{tikzcd}
\lambda\colon \arrow[d, no head] & K \arrow[r] \arrow[d, no head] & \lambda(K)=K \arrow[d, no head] \arrow[ddr] & \\
\lambda\colon \arrow[d, no head] & E \arrow[r] \arrow[d, no head] & \lambda(E) \arrow[dr] & \\
\mathrm{id}\colon & F \arrow[rr] & & A
\end{tikzcd}$$

Figure 3.1. Galois normal subgroup embedding field

"$\Rightarrow$" E/F is Galois. We define $\varphi(\mathrm{Gal}(K/F))\to\mathrm{Gal}(E/F)$ by $\sigma\mapsto\varphi(\sigma)=\sigma|_E$. This is a surjective group homomorphism, and

$$\ker\varphi=\{\sigma\in\mathrm{Aut}(K/F)\colon\sigma|_e=\mathrm{id}_E\}=\mathrm{Gal}(K/E)$$

Thus we have $\mathrm{Gal}(E/F)=\frac{\mathrm{Gal}(K/F)}{\mathrm{Gal}(K/E)}$. ☐

Example 3.16. Let $f(x)=x^3-2=(x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\omega^2)$, $\omega=\frac{-1+\sqrt{3}i}{2}$. Consider $K=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)=\mathrm{split}_{\mathbb{Q}}(x^3-2)$. Then we have

$$\begin{tikzcd}
 & & K=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) \arrow[dll, no head] \arrow[dl, no head] \arrow[dr, no head] \arrow[drr, no head] & & \\
\mathbb{Q}(\alpha_1) \arrow[drr] & \mathbb{Q}(\alpha_2) \arrow[dr] & & \mathbb{Q}(\alpha_3) \arrow[dl] & \mathbb{Q}(\omega) \arrow[dll] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & \mathrm{Gal}(K/K)=\{\mathrm{id}\} \arrow[dll, no head] \arrow[dl, no head] \arrow[dr, no head] \arrow[drr, no head] & & \\
\underset{\{\mathrm{id},(2,3)\}}{\mathrm{Gal}(K/\mathbb{Q}(\alpha_1))} \arrow[drr] & \underset{\{\mathrm{id},(1,3)\}}{\mathrm{Gal}(K/\mathbb{Q}(\alpha_2))} \arrow[dr] & & \underset{\{\mathrm{id},(1,2)\}}{\mathrm{Gal}(K/\mathbb{Q}(\alpha_3))} \arrow[dl] & \underset{\{\mathrm{id},(1,2,3),(1,3,2)\}}{\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3}))} \arrow[dll] \\
 & & \mathrm{Gal}(K/\mathbb{Q})=S_3 & &
\end{tikzcd}$$

Figure 3.2. Field extensions and group extensions

Note that Only $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3}))$ is a normal subgroup. Hence, only $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois.

Example 3.17. If K/E, E/F are Galois, then K/F is not always Galois. Here is an example, $K=\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$, $E=\mathbb{Q}(\sqrt{2})$ and $F=\mathbb{Q}$.

4 Solvable Groups

Definition 4.1. $\phi_n = \phi_n^{A/F} := \{\theta \in A | \theta^n = 1_F\} = \langle \varepsilon \rangle := \{\varepsilon^0 = 1, \varepsilon, \varepsilon^2, \dots\}$, *$\varepsilon$ is called primitive n-root of* 1.

Definition 4.2. *K/F is Galois, then we call K/F is Abelian if* $\mathrm{Gal}(K/F)$ *is abelian, K/F is cyclic if* $\mathrm{Gal}(K/F)$ *is cyclic.*

Theorem 4.3. *Let ε be a primitive n-root of 1 in $A \supset F$, then $F(\varepsilon)/F$ is abelian. (Suppose* $\mathrm{char}(F) \nmid n$*)*

Proof. $[\sigma(\varepsilon)]^n = \sigma(\varepsilon^n) = \sigma(1) = 1$, then $\sigma(\varepsilon) = \varepsilon^{n_\sigma} \in F(\varepsilon)$. $\sigma(F(\varepsilon)) = F(\varepsilon)$. $(x^n - 1)' = n x^{n-1} \neq 0$, $\gcd(x^n - 1, n x^{n-1}) = 1$. So it is Galois and $\sigma \circ \tau = \tau \circ \sigma$ since

$$\tau \circ \sigma(\varepsilon) = \tau(\sigma(\varepsilon)) = \tau(\varepsilon^{n_\sigma}) = (\tau(\varepsilon))^{n_\sigma} = \varepsilon^{n_\tau n_\sigma} = \sigma \circ \tau(\varepsilon)$$

□

Theorem 4.4. *Suppose F contains an n-th primitive root of 1, $\varepsilon \in F \subseteq A$,* $\mathrm{char}(F) \nmid n$*, and $\alpha^n = b \in F$, then $F(\alpha)/F$ is cyclic.*

Proof. $\left(\frac{\sigma(\alpha)}{\alpha}\right)^n = \frac{\sigma(\alpha^n)}{\alpha^n} = \frac{\sigma(b)}{b} = \frac{b}{b} = 1$, and $\frac{\sigma(\alpha)}{\alpha} = \varepsilon_\sigma = \varepsilon^{n_\sigma} \in F(\alpha)$. Hence $\sigma(\alpha) = \varepsilon_{\sigma_n} \cdot \alpha \in F(\alpha)$. So $F(\alpha)/F$ is normal. Let $f(x) = x^n - b$, $f'(x) = n x^{n-1}$, $\gcd(f, f') = 1$ no multiple roots.

Hence, $F(\alpha)/F$ is separable and then Galois. Suppose $\sigma, \tau \in \mathrm{Gal}(K/F)$, then

$$\tau\sigma(\alpha) = \tau(\sigma(\alpha)) = \tau(\varepsilon_\sigma \alpha) = \varepsilon_\sigma \tau(\alpha) = \varepsilon_\sigma \varepsilon_\tau \alpha.$$

We make a group homomorphism that

$$\begin{array}{rcl} \varphi(\mathrm{Gal}(F(\alpha)/F)) \cong \mathrm{Gal}(F(\alpha)/F) & \xrightarrow{\varphi} & \phi_n^{A/F} \\ \sigma & \mapsto & \varphi(\sigma) = \varepsilon_\sigma \end{array}$$

Since $\varphi(\tau\sigma) = \varepsilon_{\sigma\tau} = \varphi(\tau)\varphi(\sigma)$, $\sigma(\alpha) = \varepsilon_\sigma \alpha = \alpha$, it is a homomorphism and injective.

By the theorem, a subgroup of a cyclic group is also cyclic.

□

Definition 4.5. (solvable by radical) *Let $f(x) \in F[x]$, $\deg(f) \geqslant 1$, $f(x)$ is called solvable by radical over F if* $\mathrm{Split}_F(f) := L \subseteq K$*, K/F is Galois, s.t. $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = K$ with $F_1 = F(\varepsilon)$* $\mathrm{char}(F) \nmid n$*, $F_{i+1} = F_i(\alpha_{i+1})$, $\alpha_{i+1}^{n_i} = b_i \in F_i$, $n_i | n$, $\forall i = 1, 2, \dots, n-1$.*

In fact, $\mathrm{Gal}(K/F_1) \supseteq \mathrm{Gal}(K/F_2) \supseteq \cdots \supseteq \mathrm{Gal}(K/F_m) = \{\mathrm{id}\}$, $\mathrm{Gal}(F_{i+1}/F_i) \cong \frac{\mathrm{Gal}(K/F_i)}{\mathrm{Gal}(K/F_{i+1})}$, by the first and second fundamental theorems, we have that their are all abelian groups.

Example 4.6. $x^4 + b x^2 + c = 0$ is solvable by radical.

Definition 4.7. (solvable group) *A group G is called sovable if*

$$\exists G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{e\}$$

such that $G_{i+1} \lhd G_i$ with G_i/G_{i+1} is abelian.

Then we have $\mathrm{Gal}_F(f) = \mathrm{Gal}(\mathrm{Split}_F(f)) = \mathrm{Gal}(L/F) = \mathrm{Gal}(K/F)/\mathrm{Gal}(K/L)$. $f(x)$ is solvable by radical over F iff $\mathrm{Gal}(f)$ is solvable.

Lemma 4.8. *Let $N \lhd G$, then G/N is abelian iff $\forall a, b \in G$, $aba^{-1}b^{-1} \in N$.*

Proof. $\forall a, b \in G$, $aba^{-1}b^{-1} \in N \Leftrightarrow aba^{-1}b^{-1}N = N \Leftrightarrow aNbNa^{-1}Nb^{-1}N = N \Leftrightarrow aNbN = bNaN \Leftrightarrow$ G/N is abelian ☐

Lemma 4.9. *Let $n \geqslant 5$, $N \lhd H \subseteq S_n$ if H has all 3-cycle then so is N with H/N abelian.*

Proof. let i, j, k, r, s are distinct integers between 1 and n ($n \geqslant 5$).

$$\sigma = (ijk)(krs)(ijk)^{-1}(krs)^{-1} = (ijk)(krs)(kji)(srk)$$

Consider these integers, $\sigma(i) = r$, $\sigma(r) = k$, $\sigma(k) = i$ thus $\sigma = (irk)$. N must have σ. ☐

Theorem 4.10. *$S_n (n \geqslant 5)$ is not solvable.*

Proof. Suppose on the countrary, S_n is solvable. $S_n = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{\mathrm{id}\}$ s.t. $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian. G_1/G_2, then G_2 has three cycles, hence G_m has three cycles. Contradiction! ☐

5 More on Galois Theory

Definition 5.1. *$x_1, \ldots, x_n$ are independent variables over a field k. $K := k(x_1, \ldots, x_n)$, if $\forall g(x_1, \ldots, x_n) \in K$, $\forall \sigma \in S_n \subseteq \mathrm{Aut}(K)$. Define $\sigma(g)(x_1, \ldots, x_n) = g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in K$. $F = K^{S_n} := \{g \in K | \sigma(g) = g, \forall \alpha \in S_n\}$*

Claim. $\forall \sigma \in S_n, \sigma \in \mathrm{Aut}(K/K^{S_n})$, $[K: K^{S_n}] \geqslant \#\text{distinct embeddings} = n!$

Define $f(t) := (t - x_1) \cdots (t - x_n) = t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n$, $a_i \in K^{S_n}$.

Define $E := k(a_1, a_2, \ldots, a_n)$, $E \subseteq F$. And now we prove that $E = F$, we only need to prove $K/E \leqslant n!$.

In general, we have $E_{i-1} = E_i(x_i)$, and $f_i(t) = \frac{f(t)}{(t - x_{i+1}) \cdots (t - x_n)} = (t - x_1) \cdots (t - x_i)$. $f_i(x_i) = 0$.

$[E_{i-1}: E_i] \leqslant \deg(f_i) = i$. Thus $[K: E] \leqslant n! \Longrightarrow [K: E] = [K: F] = n!$.

Now Claim K/F is Galois and $\mathrm{Gal}(K/F) = S_n$.

- normal ($\leqslant n!$ embeddings but we already have $n!$)
- separable ($< n!$)

Thus $\mathrm{Gal}_F(f) = \mathrm{Gal}(\mathrm{Split}_F(f)) = \mathrm{Gal}(K/F) = S_n$.

Example 5.2. $\mathrm{Gal}_{\mathbb{Q}}((x-1)(x-2)\cdots(x-5)) = \{\mathrm{id}\}$, $\mathrm{Gal}_{\mathbb{Q}}(x^3 - 2) = S_3$, $\mathrm{Gal}_{\mathbb{Q}}(x^5 - 5x - 1) = S_5$.

Question 1. (inverse Galois problem) Given a finite group G, can we find an Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) = G$?

6 Finite Field Extension

Theorem 6.1. *Suppose A is a field with $\operatorname{char} A = p$, then for every $q = p^m, m \geqslant 1$, there exists a unique subfield $\mathbb{F}_q$ of A, where $\mathbb{F}_q$ is a finite field with exact q elements.*

Proof. Define $S = \{\alpha \in A | \alpha^q - \alpha = 0\} \subseteq A$, then if $\alpha, \beta \in S$, $(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta \in S$, and $(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta \in S$. If in addition, $\beta \neq 0$, $(\alpha\beta^{-1})^q = \alpha^q (\beta^q)^{-1} = \alpha\beta^{-1} \in S$. So S is a field.

Take derivative of S, $(x^q - x)' = q x^{q-1} - 1 = -1$, i.e. $\gcd(x^q - x, (x^q - x)') = 1$, which means $x^q - x$ no multiple roots.

Hence, $|S| = q = \deg(x^q - x)$. We set $\mathbb{F}_q := S$.

As for uniqueness, $|\mathbb{F}_q - \{0\}| = q - 1$ and $\alpha^{q-1} = 1$ which implies $\alpha^q - \alpha = 0$ containing 0 luckily. □

Note. In a field with characteristic p, $p\alpha = 0$ for all $\alpha \in A$.

Lemma 6.2. *$E = \mathbb{F}_{q^n}$ is unique in A.*

Note 6.3. Namely, the field extension $A > E > \mathbb{F}_q$ is unique.

Proof. Note that $n = [E : \mathbb{F}_q] = \dim_{\mathbb{F}_q}(E)$. So there exists a basis of E over $\mathbb{F}_q$, $u_1, u_2, \ldots, u_n$, such that $\forall \alpha \in E$, $\alpha = b_1 u_1 + \cdots + b_n u_n$, where $b_i \in \mathbb{F}_q$ are unique. $|E| = q^n$. Then by Theorem 6.1, we have done. □

From above lemma, we can immediately get following:

Theorem 6.4. *Suppose there is a field extension $\mathbb{F}_{q^n} / \mathbb{F}_q$, then for every $m | n$, there is a unique $\mathbb{F}_{q^m}$. Alternatively, If E is an intermediate field of $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$, then there must exist a unique m, such that $\mathbb{F}_{q^m} = E$ and $m | n$.*

This theorem means that the number of intermediate field E is equal to the number of positive integer divisors of n.

Theorem 6.5. *$\mathbb{F}_{q^n} / \mathbb{F}_q$ is Galois.*

Proof. $\mathbb{F}_{q^n} = \operatorname{Split}_{\mathbb{F}_q}(x^{q^n} - x)$, $\mathbb{F}_{q^n} / \mathbb{F}_q$ is normal. Every element $\alpha \in \mathbb{F}_{q^n}$ is a root of $x^{q^n} - x$ (no multiple roots), hence separable over $\mathbb{F}_q$. Hence, the extension is Galois. □

Theorem 6.6. *$\mathbb{F}_{q^n} / \mathbb{F}_q$ is cyclic, i.e. $\operatorname{Gal}(\mathbb{F}_{q^n} : \mathbb{F}_q) = \langle \sigma \rangle = \{\sigma^0 = \operatorname{Id}, \sigma, \ldots, \sigma^{n-1}\}$, where σ is defined as Frobenius automorphism*

$$\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n},$$

$$\sigma \mapsto \sigma(\alpha) = \alpha^q.$$

Proof. $\forall \alpha, \beta \in \mathbb{F}_{q^n}$, $\sigma(\alpha + \beta) = (\alpha + \beta)^q = \alpha^q + \beta^q = \sigma(\alpha) + \sigma(\beta)$, $\sigma(\alpha\beta) = (\alpha\beta)^q = \alpha^q \beta^q = \sigma(\alpha)\sigma(\beta)$ and $\sigma(1) = 1^q = 1$. So σ is a homomorphism.

If $\sigma(\alpha) = \sigma(\beta) \Rightarrow \alpha^q = \beta^q = (\alpha - \beta)^q = 0 \Longrightarrow \alpha = \beta$. Hence σ is injective. σ injective means surjective. Hence, σ is an automorphism. $\sigma \in \operatorname{Aut}(\mathbb{F}_{q^n})$.

Restriction in $\mathbb{F}_q$: $\forall a \in \mathbb{F}_q$, $\sigma(a) = a^q = a$. Then $\sigma \in \operatorname{Aut}(\mathbb{F}_{q^n} / \mathbb{F}_q) = \operatorname{Gal}(\mathbb{F}_{q^n}, \mathbb{F}_q)$.

For $\forall \alpha \in \mathbb{F}_{q^n}$, $\sigma^n(\alpha) = \alpha^{q^n} = \alpha$, hence, $\sigma^n = \mathrm{Id}$.

For any $1 \leqslant m < n$, $\sigma^m \neq \mathrm{Id}$. If note, suppose $\sigma^m = \mathrm{Id}$, then $\sigma^m(\alpha) = \alpha^{q^m} = \alpha$, i.e. α are a root of $x^{q^m} - x$ which contradicts to the minimal polynomial $x^{q^n} - x$. $\square$

So we have a relation of extension of fields and inclusion of subgroups as follows

$$\begin{array}{ccccc} \mathbb{F}_{q^n} & — & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^n}) & = & \{\mathrm{Id}\} \\ | & & | & & \\ \mathbb{F}_{q^m} & — & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^m}) & = & \langle \sigma^m \rangle \\ | & & | & & \\ \mathbb{F}_q & — & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & = & \langle \sigma \rangle \end{array}$$

And $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \frac{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)}{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_{q^m})} = \langle \sigma \rangle / \langle \sigma^m \rangle = \langle \sigma^{n/m} \rangle$.

Theorem 6.7. *Let $f(x) \in \mathbb{F}_q(x)$, irreducible over $\mathbb{F}_q$ with* $\mathrm{def}(f) = n$. *Then $f(x) | x^{q^n} - x$.*

Proof. Let α be a root of $f(x)$, then α is also a root of $x^{q^n} - x$, since $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, which means $f(x) | x^{q^n} - x$. $\square$

Theorem 6.8. $x^{q^n} - x = \prod_{m|n}$ monic irreducible polynomials $f(x)$ over $\mathbb{F}_q$ of $\deg(f) = n$.

Proof. Note that $x^{q^m} - x | x^{q^n} - x$. In fact, $q^m - 1 | q^{n-1} - 1 \Longrightarrow x^{q^{m-1}} - 1 | x^{q^{n-1}} - 1 \Longrightarrow x^{q^m} - x | x^{q^n} - x$. Distinct no multiple root divisors. $\square$

Consider $\mathbb{F}_{q^{n_1}}, \mathbb{F}_{q^{n_2}}, \ldots, \mathbb{F}_{q^{n_m}} \subseteq \mathbb{F}_{q^N}$, where $N = \mathrm{lcm}\,(n_1, n_2, \ldots, n_m)$. Define

$$\mathbb{F}_{q^\infty} = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n},$$

then it is a field.

Theorem 6.9. $\mathbb{F}_{q^\infty}$ *is the smallest algebraically closed field containing* $\mathbb{F}_q$ *and* $\mathbb{F}_{q^\infty}/\mathbb{F}_q$ *is algebraic.*

Proof. Let $f(x) \in \mathbb{F}_{q^\infty}[x]$, with $\deg(f) \geqslant 1$. WLOG, we may assume $f(x)$ is irreducible over $\mathbb{F}_{q^\infty}$,

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

There exists N, such that $a_0, \ldots, a_{n-1} \in \mathbb{F}_{q^N}$. Then $f(x) \in \mathbb{F}_{q^N}[x]$. All roots of $f(x)$ will be in $\mathrm{Split}_{\mathbb{F}_{q^N}}(f) := K$, while $K = \mathbb{F}_{q^{N/m}} \subseteq \mathbb{F}_{q^\infty}$ (can not be finite). All subfield is finite and algebraic, then $\mathbb{F}_{q^\infty}$ is algebraic. $\square$

Remark 6.10. $\mathbb{F}_{q^n} - \{0\} = \langle \alpha \rangle = \{\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{q^n - 2}\}$, then $\mathbb{F}_{q^n} = \mathbb{F}(\alpha)$.

Index