Field & Galois Theory

Yashas.N

Contents

1 Field Extension Theory **1**
1.1 Algebraic Extensions 2
1.2 Separable and Inseparable Extensions 4
1.3 Finite fields 5
1.4 Cyclotomic Extension 5

2 Galois Theory **6**
2.1 Galois groups of polynomials 9
2.2 Solvable and Radical extension . . . 10

1 Field Extension Theory

Prime Subfield

of a Field F is a subfield of F generated by its multiplicative identity 1. We know that this is isomorphic to Q or $\mathbb{Z}/pZ(=\mathbb{F}_p)$ depending on the Characteristic of F ($ch(F)$).

If K is a field containing a subfield F then K is said to be the extension field or extension of F Denoted by K/F (not to be confused with quotient group.)

Degree or Index

of a field extension K/F is the dimension of K as a Vector space over F and is denoted by $[K : F]$

Existence of Extension :

if F is a field and and $p(x) \in F[x]$ be an irreducible polynomial then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root.

(Given by $K = F[x]/(p(x))$ where $\pi : F[x] \to F[x]/(p(x))$ is considered and $x \to \theta$ then $p(\theta) = 0$ in K .)

if $p(x) \in F[x]$ is irreducible polynomial of degree n over field F, field $K = F[x]/(p(x))$ and $\theta = x \ (\mathbf{mod}\ p(x)) \in K$ then $\{1, \theta, \theta^2, .., \theta^{n-1}\}$ forms a basis of vector space K over F i.e. $[K : F] = n$ and

$$K = \{a_0 + a_1\theta + a_2\theta^2 + .. + a_{n-1}\theta^{n-1} | a_i \in F\}.$$

Operations in field extension via $p(x)$

■ addition is usual polynomial addition
■ multiplication is defined as $a(\theta)b(\theta) = r(\theta)$ where $a(x)b(x)$ is multiplied in $F[x]$ and divided by $p(x)$ to give remainder $r(x)$ which gives $r(\theta)$
■ as K is field each element has an inverse to find $a^{-1}(\theta)$: as $p(x)$ is irreducible in $F[x]$ and degree $a(x) <$ degree $p(x)$ we have $(a(x), p(x)) = 1 \implies \exists b(x), c(x) \in F\ {}_s|_t\ b(x)a(x) + c(x)p(x) = 1$, now $(\mathbf{mod}\ p(x))$ this we get $b(x)a(x) \equiv 1$ $(\mathbf{mod}\ p(x))$ i.e. $a^{-1}(\theta) = b(\theta)$.

$F(\alpha, \beta, ..)$

if $\alpha, \beta, .. \in K$ for some field extension K of F then the smallest subfield of K containing F and $\alpha, \beta, ..$ is called **field generated** by $\alpha, \beta, ..$ over F denoted by $F(\alpha, \beta, ..)$ i.e. for eg $F(\alpha)$ is nothing but the smallest field containing both F and α with condition that it is known some extension of F contains α.

Simple extension

if K field extension of F is such that $K = F(\alpha)$

if K field extension of F is such that for $p(x) \in F[x]$ irreducible and root α of $p(x)$ is contained in K i.e. $p(\alpha) = 0$ in K then for $F(\alpha)$ subfield generated by F, α in K we have

$$F(\alpha) \cong F[x]/(p(x)).$$

in K

so we get

$$F(\alpha) = \{a_0 + a_1\theta + a_2\theta^2 + ..$$

$$+ a_{n-1}\theta^{n-1} | a_i \in F\}.$$

(Note : according to this any roots of $p(x)$ are indistinguishable algebraically i.e. if α, β are roots same irreducible $p(x)$ in $F[x]$ then $F(\alpha) \cong F(\beta)$.)

if $F \cong F'$ (both fields) by isomorphism ϕ denoted by $\phi : F \xrightarrow{\sim} F'$, $p(x) \in F[x]$ irreducible, $p'(x) = \phi(p(x)) \in F'[x]$ and for α a root of $p(x)$ (in some extension), β a root of $\phi(p(x))$ (in some extension) then there exist an isomorphism $\sigma : F(\alpha) \to F'(\beta)$ extending ϕ (restriction of σ to F : $\sigma|_K$ is ϕ) which maps $\alpha \to \beta$. i.e.

$$\begin{gathered} \text{if } \phi : F \xrightarrow{\sim} F' \\ {}_s|_t\ \alpha \text{ root of } p(x)\ ,\ \beta \text{ root of } \phi(p(x)) \\ \text{then } \exists \sigma : F(\alpha) \xrightarrow{\sim} F'(\beta) \\ \text{by } \alpha \to \beta \text{ and } \sigma|_F = \phi \end{gathered}$$

represented as

$$\begin{array}{cccc} \sigma : & F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ & | & & | \\ \phi : & F & \xrightarrow{\sim} & F' \end{array}$$

1.1 Algebraic Extensions

Algebraic

an element $\alpha \in K$ extension of F is said to algebraic over F if α is root of some non zero $f(x) \in F[x]$

Transcendental

if α is non algebraic then it is said to be transcendental over F.

Algebraic extension

The extension K/F is called algebraic if every element of K is algebraic over F.

Minimal polynomial

if α is algebraic over F then there is unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ called **minimal polynomial** for α over F, which has α as a root and if $f(x) \in F[x]$ has α as a root then $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.
$m_{\alpha,F}(x)$ is simply written as $m_\alpha(x)$ if F is known and degree m_α is called **degree of** α

if L/F is an extension of fields and α is algebraic over both F, L then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$ (as $m_{\alpha,F}(x)$ is also a polynomial with root α in $L[x]$.)

If α is algebraic over F then

$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x)),$$
$$[F(\alpha) : F] = \text{degree } m_{\alpha,F} = \text{degree } \alpha.$$

α is algebraic over F iff the simple extension $F(\alpha)/F$ is finite i.e. of finite dimension.
more precisely if α is an element of an extension of degree n over F then α satisfies a polynomial of degree at most n over F conversely α satisfies a polynomial of degree n over F then the degree of $F(\alpha)$ over F is atmost n.

if extension K/F is finite then it is algebraic.

if $F \subseteq K \subseteq L$ are fields then

$$[L : F] = [L : K][K : F].$$

in particular degree of K/F divides degree of L/F
(holds even if degrees are infinite)

extension K/F is finitely generated if $K = F(\alpha_1, \alpha_2, .., \alpha_k)$. for some $\alpha_1, \alpha_2, .., \alpha_k \in K$.
$F(\alpha, \beta) = (F(\alpha))(\beta)$ i.e. $F(\alpha_1, \alpha_2, .., \alpha_k)$ can be inductively defines as $F((\alpha_1, \alpha_2, .. \alpha_{k-1}))(\alpha_k)$.

extension K/F is Finite iff K is generated by finite number of algebraic elements over F
more precisely a field generated over F by finite number of algebraic elements of degree $n_1, n_2, .., n_k$ is algebraic of degree $\leq n_1 n_2 .. n_k$.

if α, β are algebraic over F then $\alpha + \beta, \alpha\beta, \alpha^{-1} = 1/\alpha, \alpha/\beta$ belong to same $F(\alpha, \beta)$(field), thus are algebraic.

in extension L/F the collection of algebraic elements over F forms a subfield.

if K is algebraic over F and L is algebraic over K then L is algebraic over F.

Composite field

if K_1, K_2 are sub fields of K then let K_1K_2 denote the smallest subfield of K containing both K_1, K_2.
if K_1, K_2 be two finite extensions of F contained in K then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F].$$

equality holds iff $F-$ basis elements of one field is linearly independent of the other.

if $[K_1 : F] = n, [K_2 : F] = m$ and $(n, m) = 1$ then $[K_1K_2 : F] = nm = [K_1 : F][K_2 : F]$.

Quadratic Extension of fields with characteristics $\neq 2$

If $[K : F] = 2$ an α is any element of K not in F then $m_\alpha(x) = x^2 + bx + c$ for $b, c \in F$ note degree $m_\alpha(x) \neq 1$ as it means $\alpha \in F$. Now $F \subseteq F(\alpha) \subseteq K$ and $[F(\alpha) : F] = 2$,Thus $K = F(\alpha)$.
Now $\alpha = -b \pm \sqrt{b^2 - 4c}/2$ so as F is not of Characteristic 2 we can divide by 2 so we get $F(\alpha) = F(\sqrt{b^2 - 4c})$ where $b^2 - 4c$ is not a square in F. Thus **all extension of Degree 2 of F is of form** $F(\sqrt{D})$ for some non square D in F.

Splitting Field

The extension field K of F is a splitting field of $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F. i.e. K is the minimal field extension of F containing all roots of $f(x) \in F[x]$

Existence of Splitting Field

every $f(x) \in F[x]$ has a splitting field. (use induction on degree of polynomial)

Splitting field of a polynomial of degree n over F is degree at most $n!$ over F.

if $\phi : F \xrightarrow{\sim} F'$ is isomorphism of fields, $f(x) \in F[x]$, $\phi(f(x)) = f'(x) \in F'[x]$, E is splitting field of $f(x) \in F[x]$ and E' is splitting field of $f'(x) \in F[x]$ then there exist isomorphism $\sigma : E \xrightarrow{\sim} E'$ that extends ϕ. i.e.

$$\begin{array}{cccc} \sigma : & E & \xrightarrow{\sim} & E' \\ & | & & | \\ \phi : & F & \xrightarrow{\sim} & F' \end{array}$$

Any two splitting fields for a same polynomial $f(x) \in F[x]$ over F are isomorphic

Algebraic closure

Field $\bar{F}$ is called the closure of F if $\bar{F}$ is algebraic over F and every polynomial $f(x) \in F[x]$ splits completely over F. i.e. $\bar{F}$ contains all the algebraic elements of F.

Algebraically closed

Field K is algebraically closed if every polynomial with coefficients in K has a root in K.

if $\bar{F}$ is algebraic closure of a field F then $\bar{F}$ is algebraically closed.

Existence of Algebraic closure

Every field F contains a algebraically closed field K containing F

(use Artin's proof : for every monic poly $f(x) \in F[x]$ denote x_f as an indeterminate and in ring $F[.., x_f, ..]$ (an infinite variable polynomial field) prove ideal $I = \langle .., f(x_f), .. \rangle \forall f$ is proper thus contained in some maximal ideal M , let $K_1 = F[.., x_f, ..]/M$ (quotient) clearly K_1 contains an isomorphic copy of F and every poly $f \in F[x]$ has a root in K_1 namely x_f performing this same process to K_1 and further we get $F = K_0 \subseteq K_1 \subseteq K_2 .. \subseteq K_j \subseteq K_{j+1} \subseteq ..$ (not direct subsets but isomorphic) and let $K = \bigcup_{j \geq 0} K_j$ the K is algebraically closed and contains F

Now if K is algebraically closed field containing F then $\bar{F} \subseteq K$ containing elements of K algebraic over F is the algebraic closure of F.)

1.2 Separable and Inseparable Extensions

Separable and Inseparable

A polynomial $f(x) \in F[x]$ is separable if it has no multiple roots i.e. all its roots are distinct and has no repeated roots, if $f(x)$ is not separable then it is inseparable.

Algebraic definition of Derivative

if $f(x) = a_n x^n + a_{n-1} x^{n-1} + .. + a_1 x + a_0 \in F[x]$ define

$D_x f(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + .. + 2 a_2 x + a_1 \in F[x]$.

(D_x is usual analytic derivative w.r.t x but it can also viewed as a linear function on $F[x]$ by above definition so usual rules and properties (like product rule of derivative) follow even if there is no notion of 'limit' or any other analytical terms.)

Test for multiple root

$f(x)$ has a multiple root α iff α is also a root $D_x f(x)$

i.e. if α is the root of both $f(x), D_x f(x)$ i.e. the minimal polynomial of α divides both $f(x), D_x f(x)$ then α is multiple root of $f(x)$

Every irreducible polynomial over a field of characteristic 0 is separable, A polynomial over such a field is separable iff it is a product of distinct irreducible polynomial

(use $D_x p(x)$ is of degree less than one of degree of $p(x)$ a irreducible so must be relatively prime i.e. $(p(x), D_x p(x)) = 1$, and as distinct irreducible polynomials are relatively prime in char 0 field the second statement follows)

Frobenius endomorphism

if F is field of characteristic p then $\forall a, b \in F$ $(a+b)^p = a^p + b^p$, $(ab)^p = a^p b^p$

so the map $\varphi : F \to F$ by $\varphi(a) = a^p$ is injective homomorphism

if F is a finite field with characteristic p then every element of F is a p^{th} power in F i.e. Frobenius endomorphism is bijective in F this is denoted by $F = F^p$ (as the map is not trivial)

Every irreducible polynomial over a finite field F is separable and a polynomial in $F[x]$ is separable iff it is product of distinct irreducible polynomials in $F[x]$

(the only problem that may occur is if $D_x p(x) = 0$

in this case if $\mathtt{Char}\ F = p$ then $p(x) = q(x^p) = a_m(x^p)^m + .. + a_0 = b_m^p(x^p)^m + .. + b_0^p = (b_m x^m + .. + b_0)^p$ by frobenius endomorphism thus a contradiction to $p(x)$ being reducible)

Separable extension

K is said to be separable over F if every element of K is a root of separable polynomial over F

Perfect Fields

A field K is perfect if it is of characteristic p and every element of K is p^{th} power in K. And any field of characteristic 0 is perfect.

Every finite extension of a perfect field is separable. In particular, every finite extension of either $\mathbb{Q}$ or a finite field is separable.

1.3 Finite fields

$Z_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field of characteristic p for prime p and is minimal field of characteristic p i.e. any field $\mathbb{F}$ with characteristic p contains an isomorphic field to Z_p

if $\mathbb{F}$ is a finite field then it is of characteristic p a prime in $\mathbb{Z}^+$

if $\mathbb{F}$ is finite field of characteristic p then $|\mathbb{F}| = p^n$ for some $n \in \mathbb{Z}^+$
(use : $\mathbb{F}$ is a finite vector field over Z_p as $Z_p \subseteq \mathbb{F}$ (the subfield generated by $1 \in \mathbb{F}$) thus finite dimensional so $[\mathbb{F} : Z_p] = n < \infty$)

$x^{p^m} - x$ is separable over $Z_p[x]$ with exactly p^m roots (in some extension)
Now the roots of this polynomial is closed under addition, subtraction, multiplication, and inverses so is the splitting field of $x^{p^m} - x$ thus
Finite fields of any order p^n exists and is unique upto isomorphism. So is denoted by $\mathbb{F}_{p^n}$ (the notation leads to $Z_p = \mathbb{F}_p$)

Representation of Finite fields

From all above points we get that

$$(\mathbb{F}_{p^n}, +) \cong \overbrace{Z_p \times Z_p \times .. \times Z_p}^{n \text{ times}}.$$
$$(\mathbb{F}^*_{p^n}, \times) \cong Z_{p^n - 1}.$$

■ A is a subfield of $\mathbb{F}_{p^n}$ iff $|A| = p^m$ for some divisor m of n
■ $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{(m,n)}}$

1.4 Cyclotomic Extension

1.4.1 Preliminaries

$d|n$ iff $x^d - 1 | x^n - 1$
(for converse use if $n = qd + r$ then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$)

Roots of $x^n - 1$ are of form $e^{2\pi k i/n}$ for $k = 0, 1, .., n-1$

n^{th} root of unity

the splitting field of $x^n - 1$ over $\mathbb{Q}$ and as F^* is cyclic for any field F and the roots of unity in this field is closed under multiplication (prove) so is generated by an element of $\mathbb{C}$. i.e. the roots of $x^n - 1$ in $\mathbb{Q}$ form a cyclic group (under multiplication)

Primitive n^{th} root of unity

A generator of n^{th} root of unity is called primitive n^{th} root of unity
clearly there are precisely $\varphi(n)$ (euler's φ-function) primitive n^{th} root of unity (as the roots form a multiplicative cyclic group)

1.4.2 Main Concept

Cyclotomic Field

if ζ_n is primitive n^{th} root of unity then $\mathbb{Q}(\zeta_n)$ is called cyclotomic field of n^{th} root of unity

let μ_n denote the group of n^{th} roots of unity over $\mathbb{Q}$ (only the roots)
Define the n^{th} cyclotomic polynomial

$$\Phi_n(x) = \prod_{\zeta \text{ primitive } \in \mu_n} (x - \zeta) = \prod_{\substack{1 \le a \le n \\ (a,n)=1}} (x - \zeta_n^a)$$

now

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta)$$

if $d|n$ then $\zeta_d^n = 1$ so

$$x^n - 1 = \prod_{d|n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitive}}} (x - \zeta)$$

$$\implies x^n - 1 = \prod_{d|n} \Phi_d(x).$$

$$\implies n = \sum_{d|n} \varphi(d)$$

Cyclotomic Polynomial $\Phi_n(x)$ is irreducible monic polynomial of $\mathbb{Z}[x]$ of degree $\varphi(x)$ so the degree of Cyclotomic field of n^{th} root of unity over $\mathbb{Q}$ is $\varphi(n)$ i.e.

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

2 Galois Theory

An automorphism σ of K field is said to fix $\alpha \in K$ if $\sigma(\alpha) = \sigma\alpha = \alpha$ and σ fixes F if it fixes every element of F
if K/F is a field extension let $\mathbf{Aut}(K/F)$ denote all the automorphisms of K that fix F.
clearly $\mathbf{Aut}(K/F)$ is subgroup of $\mathbf{Aut}(K)$ (under composition as group operations.)

Permutation Property

if K/F is field extension and $\alpha \in K$ is algebraic over F then for any $\sigma \in \mathbf{Aut}(K/F)$, $\sigma\alpha$ is a root of minimal polynomial for α over F i.e.
$\mathbf{Aut}(K/F)$ permutes the roots of irreducible polynomials or any polynomial with coefficients in F having α as a root also has $\sigma\alpha$ as a root

If $H \ll \mathbf{Aut}(K)$ (H subgroup of $\mathbf{Aut}(K)$) then the collection of elements F that are fixed by all elements of H is a subfield of K.

Reversal property

- if $F_1 \subseteq F_2 \subseteq K$ are subfields of K then $\mathbf{Aut}(K/F_2) \ll \mathbf{Aut}(K/F_1)$ and
- if $H_1 \ll H_2 \ll \mathbf{Aut}(K)$ and associated fixed fields are F_1 of H_1, F_2 of H_2 then $F_2 \subseteq F_1$

if E is the splitting field over of $f(x) \in F[x]$ then

$$|\mathbf{Aut}(E/F)| \le [E : F]$$

equality holds iff $f(x)$ is separable over F
(use induction on $[E : F]$)

$\mathbf{Aut}(\mathbb{R}/\mathbb{Q}) = 1$ only
(prove these elements are continuous thus are trivial)

Galois Extension

for K/F a finite extension then K is said to be Galois over F and K/F is Galois extension if $|\mathbf{Aut}(K/F)| = [K : F]$ and the $\mathbf{Aut}(K/F)$ is called the Galois group of K/F. (if K/F is Galois .)
clearly If K is splitting field over F of some separable polynomial in $F[x]$ then K/F is Galois.

If $\sigma_1, \sigma_2, .., \sigma_n$ are distinct embeddings of a field K into a field L then These are linearly independent as functions on K.

if $G = \{\sigma_1 = 1, \sigma_2, .., \sigma_n\}$ is subgroup of $Aut(K)$ for K field and if F is the fixed field of G then

$$[K : F] = n = |G|$$

if K/F finite extension then

$$|Aut(K/F)| \leq [K : F]$$

from above two points we have if G is any finite subgroup of $Aut(K)$, if F is the fixed field of G then K/F is Galois with Galois group G.

If $G_1 \neq G_2$ are distinct finite subgroups of $Aut(K)$ then their fixed fields are distinct

Alternative Definition of Galois Extension

K/G is Galois iff

- K is the splitting field of some separable polynomial over F.

(and Further more then ever irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K)

- F is precisely the set of elements fixed by $Aut(K/F)$

(note: in general the fixed field maybe larger than F)

Fundamental Theorem of Galois Theory

if K/F is a Galois Extension and $G = Gal(K/F) = Aut(K/F)$ then there is a bijection

$$\left\{ \begin{array}{cc} & K \\ \text{Subfields E} & | \\ \text{of } K & E \\ \text{containing } F & | \\ & F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{cc} & \{1\} \\ \text{Subgroups} & | \\ H \text{ of } G & H \\ & | \\ & G \end{array} \right\}$$

by the correspondence

$$E \rightarrow \left\{ \begin{array}{c} \text{The elements of} \\ G \text{ fixing } E \end{array} \right\}$$

$$\left\{ \begin{array}{c} \text{The fixed field} \\ \text{of } H \end{array} \right\} \leftarrow H$$

With properties :

- Inclusion reversal : if E_1, E_2 correspond to H_1, H_2 respectively then $E_1 \subseteq E_2$ iff $H_2 \ll H_1$
- $[K : E] = |H|$ and $[E : F] = |G : H|$.
- K/E is always Galois with $Gal(K/E) = H$.
- E/F is Galois iff H is normal subgroup in G , then $Gal(E/F) \cong G/H$(quotient group).
- if E_1, E_2 correspond to H_1, H_2 respectively then $E_1 \cap E_2$ corresponds to group $\langle H_1, H_2 \rangle$ and the composite field E_1E_1 corresponds to $H_1 \cap H_2$.

Diagrammatically

$$\left\{ \begin{array}{ccccc} K & \longleftrightarrow & \{1\} & & \text{always Galois,} \\ | & & | & \rightarrow & Gal(K/E) = H \\ E & \longleftrightarrow & H & & \\ | & & | & \rightarrow & \text{Galios iff } H \trianglelefteq G, \\ F & \longleftrightarrow & G & & [E : F] = |G : H| \end{array} \right\}$$

Galois Groups of finite field

As any finite field is of form $\mathbb{F}_{p^n}$ (unique upto isomorphism) for some prime p and integer $n \geq 1$ and as this field is isomorphic to splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ so $\mathbb{F}_{p^n}/\mathbb{F}$ is Galois with Cyclic Galois of order n (Z_n) which is generated by Frobenius automorphism σ_p which maps $a \mapsto a^p$ in $\mathbb{F}_{p^n}$ i.e.

$$Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle$$

so which implies that finite field $\mathbb{F}_{p^n}$ is a simple extension

since even for finite field the splitting field of polynomial of type $x^{p^n} - x$ has p^n elements, this can increase with n we get any **Any algebraically closed field must be infinite**

if K/F is Galois extension and F'/F is any extension then KF'/F' is Galois extension with galois group

$$Gal(KF'/F') \cong Gal(K/K \cap F')$$

Diagrammatically

$$
\begin{tikzcd}
& KF' \arrow[dl, dash] \arrow[dr, dash, "Gal(KF'/F')"] & \\
K \arrow[dr, dash, "Gal(K/K\cap F')"'] \arrow[ddr, dash, dashed, "Galois"'] \arrow[rr, phantom, "\cong"] & & F' \arrow[dl, dash] \\
& K\cap F' \arrow[d, dash] & \\
& F &
\end{tikzcd}
$$

if K/F is Galois extension and F'/F is any extension then

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}$$

if K_1/F and K_2/F are Galois extensions then
$K_1 \cap K_2$ is Galois over F
K_1K_2 composite field is Galois over F and is isomorphic to subgroup
$H = \{(\sigma, \tau) | \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2}$ for $\sigma \in Gal(K_1/F), \tau \in Gal(K_2/F)\}$
Diagrammatically

Galois : - -

$$
\begin{tikzcd}
& K_1K_2 \arrow[dl, dash, dashed] \arrow[dr, dash, dashed] & \\
K_1 \arrow[dr, dash, dashed] \arrow[ddr, dash, dashed] & & K_2 \arrow[dl, dash, dashed] \arrow[ddl, dash, dashed] \\
& K_1 \cap K_2 \arrow[d, dash, dashed] & \\
& F &
\end{tikzcd}
$$

and if $K_1 \cap K_2 = F$ we have

$$Gal(K_1K_2/F) = Gal(K_1/F) \times Gal(K_2/F)$$

Galois Closure

if E/F is any finite extension then there exist a Galois extension K of F containing E and is minimal extension i.e. if there is any other such extension K_1 then K_1 contains an isomorphic subfield to K which again is Galois over F , here K is called Galois closure of E over F
(use : the composite of splitting fields of minimal polynomial of basis elements of E over F is such extension.)

Defining property of Simple extension

if K/F is finite extension then is simple extension i.e. $K = F(\alpha)$ iff there are only finitely many subfields of K containing F.

Primitive element Theory

if K/F is finite and separable then K/F is simple extension.
In particular any finite extension of fields of characteristics 0 (or any perfect field) is simple extension
(use : K is the finite subgroup of Galois closure of K over F so as there are only finitely many subgroups of this group in the galois group and above point.)

Cyclotomic Extensions theory

Clearly $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois (for ζ_n a primitive n^{th} root of unity)
and $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ this isomorphism is given by $\sigma \to a \pmod{n}$ where $\sigma_a \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is defined as $\sigma_a(\zeta_n) = \zeta_n^a$
(this is the case as all elements of galois group map the primitive element to another primitive element thus $(n, a) = 1$ only.)

if $n = p_1^{a_1}p_2^{a_2}..p_k^{a_k} \in \mathbb{Z}$ where $p_i's$ are prime in $\mathbb{Z}, a_i \in \mathbb{Z}^+$ then

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_{p_2^{a_2}})/\mathbb{Q}) \times .. \times Gal(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q}).$$

(which in terms of isomorphism of rings (fields) is purely Chinese remainder theorem)

Abelian Extension

K/F is abelian extension if K/F is galois and $Gal(K/F)$ the galois group is abelian.
By Fundamental Theorem of Finite abelian groups, Fundamental theorem of Galois theory and the existence of groups which contain cyclotomic product groups stated above (by C.R.T and number theory) we have
if G is any finite abelian group then there is a subfield K of a Cyclotomic extension field with

$$Gal(K/\mathbb{Q}) \cong G$$

And if K is some finite abelian extension of $\mathbb{Q}$ then K is contained in some Cyclotomic extension of $\mathbb{Q}$

Class field Theory

it is the study abelian extension of arbitrary finite extension F of $\mathbb{Q}$. The study of the arithmetic of such abelian extensions and the search for similar results for non-abelian extensions are rich and fascinating areas of current mathematical research.

2.1 Galois groups of polynomials

To study polynoinals of finite degree with arbitrary coefficients from a field F we see the coefficients as indeterminates (sort of like variables) this type of study leads to several generalisations and ultimately classifying galios group of polynomials of small degree as can be seen below

elementary symmetric functions

if $x_1, x_2, .., x_n$ are indeterminates then elementary symmetric functions $s_1, s_2, .., s_n$ are defined by

$$\begin{aligned} s_1 &= x_1 + x_2 + .. + x_k \\ s_2 &= x_1x_2 + x_1x_3 + .. + x_2x_3 + x_2x_4 + \\ &\quad .. + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2..x_k \end{aligned}$$

Now general polynomial of degree n is polynomial whose roots $x_1, x_2, .., x_n$ are indeterminates i.e.
$= (x - x_1)(x - x_2)..(x - x_n)$
$= x^n - s_1x^{n-1} + s_2x^{n-1} + .. + (-1)^n s_n$
which gives a relation of roots and elementary symmetric functions in these roots which also continues as follows

$F(x_1, x_2, .., x_n)$ is the splitting field of $F(s_1, s_2, .., s_n)$ and clearly is Galois extension.

now the symmetric group S_n acts on $F(x_1, x_2, .., x_n)$ of all rational functions in n variables by permuting the corresponding variables so by this we have
the fixed field of S_n acting on $F(x_1, x_2, .., x_n)$ of all rational functions in n variables is the field of rational functions in their elementary symmetric functions $F(s_1, s_2, .., s_n)$
A rational function $f(x_1, x_2, .., x_n)$ is symmetric if is is not changed by any permutation in variables $x_1, x_2, .., x_n$
Any Symmetric function can be decomposed as rational function in elementary symmetric functions

Existence of S_n Galois group

general polynomial of degree n $x^n - s_1x^{n-1} + s_2x^{n-1} + .. + (-1)^n s_n$ over $F(s_1, s_2, .., s_n)$ is separable with Galois group S_n (i.e. if there is no relations among $s_1, s_2, .., s_n$ the coefficients of a polynomial of degree n then the Galois group of the the field generated by its coefficients is S_n the maximum of its kind)

Discriminant

discriminant D of $x_1, x_2, ..x_n$ is

$$D = \prod_{i<j}(x_i - x_j)^2.$$

now clearly D is a symmetric function but $\sqrt{D}$ is not and an element of S_n fixes $\sqrt{D}$ iff it can be decomposed into even number of transpositions i.e. iff it is an element of A_n alternating group of S_n

Immediately from above point we get Galois group of $f(x) \in F[x]$ is a subgroup of A_n iff the discriminant D is a square of an element of F.
(this is the case as $\sqrt{D}$ is fixed by every element of galios group means that i.e. $\sqrt{D} \in F$)
(if $D = 0$ for $f(x)$ then there is a multiple root in $f(x)$.)

2.2 Solvable and Radical extension

Cyclic extension

K/F field extension is cyclic if it is Galois and its Galois group is cyclic.

Simple Radical Extensions

Extensions of a field F obtained by adjoining the n^{th} root of an element in F i.e. of type $F(\sqrt[n]{a})$ for $a \in F$.

Since all the roots of the polynomial $x^n - a$ for $a \in F$ differ by factors of the n^{th} roots of unity, adjoining one such root will give a Galois extension if and only if this field contains the n^{th} roots of unity.

If F field is of characteristic not dividing n which contains the n^{th} roots of unity. Then the extension $F(\sqrt[n]{a})$for $a \in F$ is cyclic over F of degree dividing n .
(prove the homomorphism $\phi : Gal(F(\sqrt[n]{a})/F) \to \mu_n$ n^{th} roots of unity group by $\sigma \sqrt[n]{a} = \zeta_\sigma \sqrt[n]{a}$ for $\sigma \to \zeta_\sigma$ is injective)

Lagrange Resolvent

if K/F is cyclic extension of degree n , F is not of characteristic dividing n i.e. $ch(F) \not| n$, σ the generator of $Gal(K/F)$, $\alpha \in K$ and for any n^{th} root of unity ζ Lagrange resolvent is given by

$$\begin{aligned}(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) \\ +.. + \zeta^{n-1}\sigma^{n-1}(\alpha)\end{aligned}$$

now $\sigma(\alpha, \zeta) = \zeta^{-1}(\alpha, \zeta)$ so $\sigma(\alpha, \zeta)^n = (\alpha, \zeta)$

Any cyclic extension of degree n over F of $ch(F) \not| n$ which contains n^{th} root of unity is of form $F(\sqrt[n]{a})$ for some $a \in F$.

Root Extension

for field F of characteristic 0 an element α is algebraic over F and it can be solved in terms of radicals (addition, subtraction, multiplication and division) if $\alpha \in K$ which can be obtained by successive simple radical extensions like
$F = K_0 \subset K_2 \subset .. \subset K_s = K$ where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$ for $i = 0, 1, 2.., s-1$ such a Field K is called Root extension of F

Solvable by radicals

a polynomial $f(x) \in F[x]$ is solvable by radicals if all of its roots are solvable by radicals

Cyclicity and Root extension theorem

if α is contained in root extension K of F then α is contained in root extension which is Gaois over F and in resulting chain K_{i+1}/K_i is cyclic

Solvablity theorem

Polynomial $f(x)$ can be solved by radicals iff its Galois Group is a **Solvable Group**
(refer group theory recall finite group is solvable iff there exist a chain in which each successive quotient group is cyclic as in above point)

Insovablity of quintic and higher degree polynomial

Clearly as S_n for $n \geq 5$ is not a solvable group and the existence of general polynomial with Galois group S_n proves the fact that polynomials of degree ≥ 5 cannot be solved by radicals.
(use A_n for $n \geq 5$ is non abelian simple group and show $[S_n, S_n] = A_n$ and $[A_n, A_n] = A_n$ thus the groups in derived series of S_n is never $\{1\}$ so is S_n is not solvable (refer Derived series in Group theory))

2 References

[1] David S. Dummit, Richard M. Foote : Abstract Algebra, John Wailey & sons, 3, (2004).