Chapter 4

Fields and Galois Theory

4.1 Field Extensions

4.1.1 $K[u]$ and $K(u)$

Def. *A field F is an* **extension field** *of a field K if $F \geq K$.*

Obviously, $F \geq K \implies 1_F = 1_K$.

Def. *When $F \geq K$, let $[F : K] := \dim_K F$ denote the dim of F over K.*

Def. *Let K be a field.*

$$\begin{aligned} K[x] &:= \text{the polynomial ring of } K, \\ K(x) &:= \left\{ \frac{f}{g} \mid f, g \in K[x], g \neq 0 \right\} \\ &= \text{the rational function field of } K = \text{the quotient field of } K[x]. \end{aligned}$$

If $F \geq K$ and $u \in F$, denote

$$\begin{aligned} K[u] &:= \text{the subring of } F \text{ generated by } K \text{ and } u \\ &= \{f(u) \mid f \in K[x]\}, \\ K(u) &:= \text{the subfield of } F \text{ generated by } K \text{ and } u \\ &= \{f(u)/g(u) \mid f, g \in K[x], g(u) \neq 0\}. \end{aligned}$$

Def. *Suppose $F \geq K$ and $u \in F$.*

- *u is called* **algebraic over** *K if $g(u) = 0$ for some nonzero polyn $g \in K[x]$;*
- *otherwise, u is called* **transcendental over** *K.*

Every $u \in F$ induces a ring homom

$$\phi_u : K[x] \to F, \qquad \phi_u(f) := f(u).$$

Since $K[x]$ is a PID,

$$\operatorname{Ker} \phi_u = \{f \in K[x] \mid f(u) = 0\} = (p_u)$$

for a monic polyn $p_u \in K[x]$.

Thm 4.1. *Suppose $F \geq K$.*

1. *if $u \in F$ is algebraic over K, then*

(a) $p_u(x)$ *is irreducible in* $K[x]$, *called the* **irreducible polynomial** *of* u *over* K, *denoted by* $irr(u, K) = p_u$. *For* $f \in K[x]$, $f(u) = 0$ *iff* $p_u \mid f$,

(b) *The ring* $K[u] = K(u) \simeq K[x]/(p_u)$ *is a field, and*

$$[K[u] : K] = [K(u) : K] = \deg p_u =: \deg_K(u) \quad \textit{(the } \textbf{degree} \textit{ of } u \textit{ over } K.)$$

Indeed, $K[u] = K(u)$ *has a* K*-basis* $\{1, u, u^2, \cdots, u^{n-1}\}$ *for* $n = \deg p_u$.

2. *if* $u \in F$ *is transcendental over* K, *then*

   (a) $p_u = 0$,

   (b) $K[u] \simeq K[x]$ *and* $K(u) \simeq K(x)$, *both have infinite dim over* K.

Ex.

1. $\mathbf{R} \geq \mathbf{Q}$, $u = \sqrt{3} + \sqrt[3]{2} \in \mathbf{R}$ *is algebraic over* $\mathbf{Q}$. *Then*

$$\begin{aligned} u - \sqrt{3} = \sqrt[3]{2} &\implies (u - \sqrt{3})^3 = 2 \\ &\implies u^3 + 9u - 8 = 3\sqrt{3}(u^2 + 1) \\ &\implies (u^3 + 9u - 8)^2 = 27(u^2 + 1)^2 \\ &\implies u^6 - 9u^4 - 16u^3 + 27u^2 - 144u + 37 = 0. \end{aligned}$$

Then $p(x) = x^6 - 9x^4 - 16x^3 + 27x^2 - 144x + 37$ *is the irred polyn of* $u = \sqrt{2} + \sqrt[3]{2}$ *in* $\mathbf{Q}$. *Any* $f \in \mathbf{Q}[x]$ *satisfies* $f(u) = 0$ *iff* $p \mid f$. $\mathbf{Q}[u] = \mathbf{Q}(u)$, $[\mathbf{Q}(u) : \mathbf{Q}] = 6$, *and* $\{1, u, \cdots, u^5\}$ *is a basis of* $\mathbf{Q}(u)$ *in* $\mathbf{Q}$.

2. $\mathbf{R} \geq \mathbf{Q}$, $\pi \in \mathbf{R}$ *is transcendental over* $\mathbf{Q}$. *Then* $\mathbf{Q}[\pi] \simeq \mathbf{Q}[x]$ *and* $\mathbf{Q}(\pi) \simeq \mathbf{Q}(x)$, *both have infinite dim.*

4.1.2 Field Extensions

Def.

- F *is a* **finite extension** *of* K *if* $[F : K] < \infty$,
- F *is an* **infinite extension** *of* K *if* $[F : K]$ *is infinite.*

Thm 4.2. *(proved) If* $F \geq E \geq K$, *then*

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

Moreover, $[F : K]$ *is finite iff* $[F : E]$ *and* $[E : K]$ *are finite.*

It implies the following theorem:

Thm 4.3. *$F \geq K$, $u \in F$. The foll are equiv:*

1. *u is algebraic over K,*
2. *$K(u)$ is a finite extension of K,*
3. *every $v \in K(u)$ is algebraic over K, and $\deg_K(v) \mid \deg_K(u)$.*

Def. *$F \geq K$ and $X \subseteq F$. Let $K[X]$ (resp. $K(X)$) denote the subring (resp. the subfield) of F generated by $K \cup X$.*

Def. *$F \geq K$ is a*

- **simple extension** *of K if $F = K(u)$ for some $u \in F$;*
- **finitely generated extension** *of K if $F = K(u_1, \cdots, u_n)$ for some $u_1, \cdots, u_n \in F$.*

Ex. *Every fin ext is a fin gen ext. The converse is false. e.g. $K(x)$ is a fin gen ext of K but not a fin ext of K.*

Def. *$F \geq K$ is an* **algebraic extension** *if every element of F is algebraic over K.*

Thm 4.4. *$F \geq K$ is a finite extension iff $F = K[u_1, \cdots, u_n]$ where each u_i is algebraic over K. In particular, finite extensions are algebraic extensions.*

Thm 4.5. *$F \geq E \geq K$. Then F is alg ext of K iff F is alg ext of E and E is alg ext of K.*

Ex. *$\mathbf{Q}(\sqrt{2})$ is algebraic extension over $\mathbf{Q}$, and $\mathbf{Q}(\sqrt{2}, \sqrt[5]{3})$ is an algebraic extension over $\mathbf{Q}(\sqrt{2})$. Then $\mathbf{Q}(\sqrt{2}, \sqrt[5]{3})$ is an algebraic extension over $\mathbf{Q}$. For example, both $\sqrt{2} - \sqrt[5]{3}$ and $\sqrt{2}\sqrt[5]{3}$ are algebraic numbers over $\mathbf{Q}$.*

Thm 4.6. *$F \geq K$. The set of all elements of F that are algebraic over K forms an intermediate field $\widehat{K}$ between F and K ($F \geq \widehat{K} \geq K$), called the* **algebraic closure of** *K* **in** *F. Moreover, every element of $F - \widehat{K}$ is transcendental over $\widehat{K}$.*

Remark.

1. *Given a field K and an irreducible monic polynomial $p(x) \in K[x]$, we can always construct an algebraic extension $F \geq K$ such that the irred polyn of certain $u \in F$ in K is $p(x)$:*

(a) *The quotient ring* $F := K[x]/(p(x))$ *is a field since* $p(x)$ *is irreducible.*

(b) *Let* $\iota : K \to K[x]$ *be the canonical inclusion, and* $\pi : K[x] \to K[x]/(p(x))$ *the canonical projection. Then* $\pi\iota(K) \simeq K$ *and* $F \geq \pi\iota(K)$*.*

(c) *The element* $u := \pi(x) \in F$ *has irred polyn* $p(x)$ *in* $\pi\iota(K) \simeq K$*.*

2. *Any field* K *can be extended to an* **algebraic closure** *field* $\overline{K}$ *that contains the roots of all irreducible polynomials of* $K[x]$*, using Zorn's Lemma and the above remark. Any two algebraic closures of* K *are* K*-isomorphic (Hungerford, Thm V.3.6).*

4.2 Galois Theory

We will focus on Galois theory for finite extensions (i.e., fin gen alg exts).

4.2.1 K-automorphism

Thm 4.7. *$F \geq K$ and $u, v \in F$. Then $\phi_{u,v} : K(u) \to K(v)$ def by $\phi_{u,v}|_K = id|_K$ and $\phi_{u,v}(u) = v$ is a field isomorphism iff one the followings holds:*

1. *Both u and v are algebraic and $irr(u, K) = irr(v, K)$. u and v are said to be* **conjugate over** K.

2. *Both u and v are transcendental over K.*

Def. *Let $E \geq K$ and $F \geq K$. A map $\sigma : E \to F$ is a* **K-isomorphism** *if σ is both a field isomorphism and a K-mod isomorphism. If $E = F$, then σ is a* **K-automorphism**. *All K-automorphisms of F form a group $G(F/K) = Aut_K F$, called the* **Galois group of F over K**.

Remark.

1. *$\sigma : E \to F$ is a K-isomorphism iff σ is a field isomorphism that acts as identity map on K.*

2. *Let $B := \begin{cases} \mathbf{Q}, & \text{if } char\, F = 0, \\ \mathbf{Z}_p, & \text{if } char\, F = p, \end{cases}$ be the base field of F. Then a chain of fields*

$$F \geq F_1 \geq F_2 \geq \cdots \geq B$$

induces a chain of automorphism groups

$$\{1\} = G(F/F) \leq G(F/F_1) \leq G(F/F_2) \leq \cdots \leq G(F/B) = Aut(F).$$

Thm 4.8. *Let $F \geq K$ be an algebraic extension, and $\sigma \in G(F/K)$. Then $irr(u, K) = irr(\sigma(u), K)$ for every $u \in F$.*

Proof. A special case of Thm 4.7. □

Remark. *This important theorem can be used to determined all elements of $G(F/K)$ when $F = K(u_1, \cdots, u_n)$, in particular when $[F : K] < \infty$.*

Ex. *Consider* $K = \mathbf{Q}$ *and* $F = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. *Clearly* $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$ *and so* $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = 4$. *Then*

$$\mathbf{Q}(\sqrt{2}, \sqrt{3}) = 1\mathbf{Q} + \sqrt{2}\mathbf{Q} + \sqrt{3}\mathbf{Q} + \sqrt{6}\mathbf{Q}.$$

Then $G(F/K)$ *consists of 4 elements: (classified by their actions on generators* $\sqrt{2}$ *and* $\sqrt{3}$*)*

$G(F/K)$	1	σ	τ	$\sigma\tau = \tau\sigma$
image of $\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
image of $\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$

For example, $\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$.

Remark. $G(F/K)$ *stabilizes the algebraic closure of* K *in* F.

Ex. *Let* $F = \mathbf{Q}(\sqrt{2}, \sqrt{3}, x) \geq \mathbf{Q} = K$, *where* x *is transcendental over* $\mathbf{Q}$. *The algebraic closure of* K *in* F *is* $\widehat{K} = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. *Suppose* $\sigma \in G(F/K)$. *Then* $\sigma(\mathbf{Q}(\sqrt{2}, \sqrt{3})) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. *So* σ *sends* $\sqrt{2}$ *to* $\pm\sqrt{2}$, *sends* $\sqrt{3}$ *to* $\pm\sqrt{3}$, *and sends* x *to* $\dfrac{ax+b}{cx+d}$ *for* $a, b, c, d \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$ *and* $ad - bc \neq 0$ *(since from* $u = \sigma(x)$ *we should get a rational function expression of* x*). The group* $(\mathbf{Z}_2 \times \mathbf{Z}_2) \ltimes G(F/K) \simeq PGL(2, \widehat{K})$.

4.2.2 Splitting Field

Def. *A polyn* $f \in F[x]$ *is* **split** *over* F *(or to split in* $F[x]$*) if* f *can be written as a product of degree one polyns in* $F[x]$.

Ex. $F = \mathbf{Q}(\sqrt{2}, \sqrt[3]{3})$. *Then* $x^2 - 2$ *is split over* F, *but* $x^2 - 3$ *is not split over* F.

Def. *Suppose* $\overline{K} \geq F \geq K$. *Then*

1. *Let* $\{f_i \mid i \in I\}$ *be a set of polyns in* $K[x]$. F *is the* **splitting field over** K **of** $\{f_i \mid i \in I\}$ *if* F *is generated over* K *by the roots of all* f_i.

2. F *is a* **splitting field over** K *if* F *is the splitting field of some set of polynomials in* $K[x]$.

Ex. *Let* $\alpha_1, \cdots, \alpha_n$ *be the roots of* $f \in K[x]$ *in* $\overline{K}$. *The splitting field over* K *of* f *is* $F := K(\alpha_1, \cdots, \alpha_n)$. *Note that* $[F : K] \geq \deg f(x)$.

Ex. $\overline{K}$ *is a splitting field over* K *of* $K[x]$. *Every* $f \in K[x]$ *is split over* $\overline{K}$.

Ex. *$E := \mathbf{Q}(\sqrt{2}, \sqrt{3})$ splitting over $\mathbf{Q}$ of $\{x^2 - 2, x^2 - 3\}$. The polynomials $x^2 - 2$, $x^2 - 3$, $x^4 - 5x^2 + 6$, are split over E.*

Ex. *What is the splitting field F over $\mathbf{Q}$ of $x^3 - 2$? What are the elements of $G(F/Q)$?*

Thm 4.9. *Any two splitting fields of $S \subseteq K[x]$ over K are K-isomorphic.*

(c.f. Any two algebraic closures of K are K-isomorphic.)

Thm 4.10. *$F \geq K$, $[F : K] < \infty$. Let $\sigma : K \to K_1$ be a field isomorphism, and $\overline{K_1}$ an algebraic closure of K_1. The number of extensions of σ to a field isomorphism τ of F onto a subfield of $\overline{K_1}$ is finite, and is completely determined by F and K (so the number is not relative to K_1, $\overline{K_1}$, and σ.)*

Proof. It suffices to prove for simple extension $F = K(u)$ and then apply induction. Suppose

$$\operatorname{irr}(u, K) = p(x) = c_0 + c_1 x + \cdots + c_n x^n \in K[x].$$

Any extension of σ to $\tau : F \to F_1$ with $F_1 \leq \overline{K_1}$ is uniquely determined by $\tau(u)$, which is a root of

$$\operatorname{irr}(\tau(u), K_1) = p_\sigma(x) = \sigma(c_0) + \sigma(c_1)x + \cdots + \sigma(c_n)x^n \in K_1[x].$$

Therefore, the number of extensions of σ to an isomorphism of F onto a subfield of $\overline{K_1}$ equals to the number of distinct roots of $p_\sigma(x)$, or the number of distinct roots of $p(x)$, which is completely determined by F and K. □

Def. *Let $\overline{K} \geq F \geq K$ with $[F : K] < \infty$. The number of K-isomorphisms of F onto a subfield of $\overline{K}$ is the* **index of F over K**, *denoted by $\{F : K\}$.*

Remark.

1. *$\{F : K\}$ is called the separable degree $[F : K]_s$ of F over K in [Hungerford, Def. V.6.10].*
2. *$|G(F/K)| \leq \{F : K\}$. In fact, $|G(F/K)|$ divides $\{F : K\}$.*
3. *$\{F : K\} \leq [F : K]$. In fact, $\{F : K\}$ divides $[F : K]$.*

Thm 4.11. *If $F \geq L \geq K$ and $[F : K] < \infty$, then*

$$\{F : K\} = \{F : L\}\{L : K\}$$

Proof. There are $\{L : K\}$ many K-isomorphisms of L onto a subfield of $\overline{K}$. By Theorem 4.10, each such K-isomorphism has $\{F : L\}$ many extensions to a K-isomorphisms of F onto a subfield of $\overline{K}$. □

Remark.

1. *Compare: If $F \geq L \geq K$, then $[F : K] = [F : L][L : K]$.*

2. *By the Theorem, if $F = K(\alpha_1, \cdots, \alpha_r)$ is a finite extension of K, let $F_i := K(\alpha_1, \cdots, \alpha_i)$ so that $F_i = F_{i-1}(\alpha_i)$. Then*

$$\begin{aligned}\{F : K\} &= \{F : F_{r-1}\}\{F_{r-1} : F_{r-2}\} \cdots \{F_1 : K\} \\ &= \{F_{r-1}(\alpha_r) : F_{r-1}\} \cdots \{K(\alpha_1) : K\}\end{aligned}$$

   where

$$\{F_{i-1}(\alpha_i) : F_{i-1}\} = \text{the number of distinct roots in } irr(\alpha_i, F_{i-1}).$$

3. *When α is algebraic over K, the index $\{K(\alpha) : K\}$ equals the number of distinct roots of $irr(\alpha, K)$. So $\{K(\alpha) : K\} \leq [K(\alpha) : K]$ and thus $\{F : K\} \leq [F : K]$ in general.*

Ex. $F = \mathbf{Q}(\sqrt{2}, \sqrt[3]{3}) \geq \mathbf{Q} = K$. *Compute the order $|G(F/K)|$, the index $\{F : K\}$, and the degree $[F : K]$.*

Thm 4.12. *$F \geq K$ with $[F : K] < \infty$. F is a splitting field over K iff every K-isomorphism of F onto a subfield of $\overline{K}$ is a K-automorphism of F (i.e., in $G(F/K)$), iff $|G(F/K)| = \{F : K\}$.*

Cor 4.13. *$F \geq K$ splitting. Then every irred polyn in $K[x]$ having a zero in F splits in $F[x]$.*

4.2.3 Separable Extension

Def.

1. *A polyn $f \in K[x]$ is* **separable** *if in some splitting field of f over K every root of f is a simple root.*

2. *$F \geq K$. $u \in F$ is called* **separable over** *K if $irr(u, K)$ is separable.*

3. *$F \geq K$ is called a* **separable extension of** *K if every element of F is separable over K.*

Thm 4.14. *If $p(x) \in K[x]$ is an irred polyn, then every root of $p(x)$ has the same multiplicity.*

Proof. Suppose α and β are two roots of $p(x)$ with multiplicities m_α and m_β respectively, so that $(x-\alpha)^{m_\alpha}$ and $(x-\beta)^{m_\beta}$ are factors of $p(x)$. The K-isomorphism $\phi_{\alpha,\beta} : K(\alpha) \to K(\beta)$ that sends α to β can be extended (by Zorn's Lemma) to a K-automorphism $\overline{\phi} : \overline{K} \to \overline{K}$, and be further extended to a ring automorphism $\widetilde{\phi} : \overline{K}[x] \to \overline{K}[x]$. One has $\widetilde{\phi}(p(x)) = p(x)$ since $\widetilde{\phi}$ fixes every element of K. Then $\widetilde{\phi}((x-\alpha)^{m_\alpha}) = (x-\beta)^{m_\beta}$ and so $m_\alpha = m_\beta$. ☐

Remark. *$p(x) \in K[x]$ monic irreducible. Then $p(x) = \left[\prod_i (x-\alpha_i)\right]^m$, where m is the multiplicity of a root of $p(x)$, and α_i are distinct.*

1. *The multiplicity m divides $\deg p(x)$.*
2. *$\{K(\alpha_i) : K\} = \frac{1}{m} \deg p(x)$ divides $[K(\alpha_i) : K] = \deg p(x)$.*
3. *If $\operatorname{char} K = 0$, then $m \equiv 1$ and $\{F : K\} = [F : K]$ for any $F \geq K$. So any extension is a separable extension.*
4. *If $\operatorname{char} K = p$, then $\dfrac{[K(\alpha_i) : K]}{\{K(\alpha_i) : K\}} = m = p^r$ for some $r \geq 0$.*

3. and 4. can be proved by derivative technique.

Thm 4.15. *A finite extension $F \geq K$ is a separable extension of K iff $\{F : K\} = [F : K]$.*

$F \geq K$ fin ext. Then $|G(F/K)| \mid \{F : K\} \mid [F : K]$:

- F is splitting over K iff $|G(F/K)| = \{F : K\}$,
- F is separable over K iff $\{F : K\} = [F : K]$.

Thm 4.16. *$F \geq L \geq K$, $[F : K] < \infty$. Then F is separable over K iff F is separable over L and L is separable over K.*

Ex. *Let $K = \mathbf{Q}$ and $F = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Then $\{\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}\} = 4 = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}]$. So $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a separable extension over $\mathbf{Q}$.*

Thm 4.17 (Primitive Element Theorem)**.** *A finite separable extension $F \geq K$ is always a simple extension, i.e. $F = K(u)$ for some $u \in F$.*

Ex. $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$ *is a simple extension over $\mathbf{Q}$.*

Proof of Thm 4.17. If $|K| < \infty$, then F and K are finite fields. Then $F^* = \langle u \rangle$ for some $u \in F^*$ (to be shown later). Hence $F = K(u)$.

Suppose K is an infinite field. By induction, we may assume that $F = K(v, w)$ for some $v, w \in F$. Let $p = \text{irr}(v, K)$ and $q = \text{irr}(w, K)$. Let $v_1 = v, v_2, \cdots, v_m$ and $w_1 = w, w_2, \cdots, w_n$ be the roots of p and q in F. Then v_i's are distinct since F is separable. Similarly, w_j's are distinct. As K is infinite, there is $a \in K$ such that $a \neq \dfrac{v_i - v}{w - w_j}$ for all i and all $j \neq 1$. Let $u := v + aw$ and $E := K(u)$. Then $F \geq E \geq K$. We show that $w \in E$. Obviously, $\text{irr}(w, E) \mid \text{irr}(w, K) = q$. Define $f := p(u - ax) \in E[x]$. Then $f(w) = p(v) = 0$ and so $\text{irr}(w, E) \mid f$. However, $f(w_j) \neq 0$ for $j \neq 1$. Therefore, $\gcd(q, f) = x - w$ and $\text{irr}(w, E) = x - w$. So $w \in E$. Then $v = u - aw \in E$ so that $F = E = K(u)$ is a simple extension. $\square$

So inseparable extensions exist in some characteristic p infinite fields.

Def. *$F \geq K$. $u \in F$ is* **purely inseparable** *over K if $irr(u, K) = (x - u)^m$ (m must be a power of p). F is a* **purely inseparable extension of** *K if every element of F is purely inseparable over K.*

Prop 4.18. *If $F \geq L \geq K$, then F is purely insep over K iff F is purely insep over L and L is purely insep over K.*

Thm 4.19. *Let $F \geq K$, $[F : K] < \infty$, and $char K = p$. Then $\alpha \in F$ is purely insep iff $\alpha^{p^r} \in K$ for some $r \in \mathbf{N}$.*

Ex. *Let $K := \mathbf{Z}_p(y)$ (p prime, y transcendental over $\mathbf{Z}_p$). The polyn $x^p - y$ is inseparable irreducible over K. If $u \in \overline{K}$ is a root of $x^p - y$, then u is purely insep over K.*

Remark. *$F \geq K$. The set of all elements of F purely insep over K forms a field T, the* **purely inseparable closure of** *K* **in** *F. Then $F \geq T \geq K$, F is separable over T, and T is purely inseparable over K.*

Similarly, there exists L, the **separable closure of** *K* **in** *F, such that $F \geq L \geq K$, F is purely inseparable over L, and L is separable over K.*

4.2.4 Galois Theory

Def. *$F \geq K$. For a subgroup $H \leq G(F/K)$, the set*

$$F_H := \{u \in F \mid \sigma(u) = u \ \ \textit{for every} \ \ \sigma \in H\}$$

is an intermediate field between F and K, called the **fixed field of** *H* **in** *F.*

Lem 4.20. *Let $F \geq K$. Then*

1. *a field $L \leq F \implies L \leq F_{G(F/L)}$;*
2. *a subgroup $H \leq G(F/K) \implies H \leq G(F/F_H)$.*

(exercise)

Def. *A finite extension $F \geq K$ is a* **finite normal extension of** *K if $|G(F/K)| = \{F : K\} = [F : K]$, i.e., F is a separable splitting field of K.*

Let $F \geq K$ be a finite separable extension. Then $F = K(u)$ for some $u \in F$. The splitting field L over K of $\operatorname{irr}(u, K)$ satisfies that $L \geq F \geq K$, where $L \geq K$ is a normal extension.

Lem 4.21. *$\overline{K} \geq F \geq L \geq K$. If F is a finite normal extension of K, then F is a finite normal extension of L. The group $G(F/L) \leq G(F/K)$. Moreover, two K-automorphisms $\sigma, \tau \in G(F/K)$ induce the same K-isomorphism of L onto a subfield of $\overline{K}$ iff σ and τ are in the same left coset of $G(F/L)$ in $G(F/K)$.*

Proof. If F is the splitting field of a set of polynomials of $K[x]$ over K, then F is the splitting field of the same set of polynomials of $L[x]$ over L. So F is splitting over L. Moreover, "F is separable over K" implies that "F is separable over L". Thus F is a finite normal extension over L.

Two automorphisms $\sigma, \tau \in G(F/K)$ satisfy that $\sigma|_L = \tau|_L$ iff $(\sigma^{-1} \circ \tau)|_L = 1|_L$, iff $\sigma^{-1} \circ \tau \in G(F/L)$, iff $\tau \in \sigma \cdot G(F/L)$, that is, σ and τ are in the same left coset of $G(F/L)$. □

Thm 4.22 (Fundamental Theorem of Galois Theory)**.** *Let F be a finite normal extension of K (i.e. $|G(F/K)| = \{F : K\} = [F : K]$). Let L denote an intermediate field ($F \geq L \geq K$). Then $L \leftrightarrow G(F/L)$ is a bijection of the set of all intermediate fields between F and K onto the set of all subgroups of $G(F/K)$. Moreover,*

1. *$L = F_{G(F/L)}$ for every intermediate field L with $F \geq L \geq K$.*
2. *$H = G(F/F_H)$ for every subgroup $H \leq G(F/K)$.*
3. *L is a normal extension of K if and only if $G(F/L)$ is a normal subgroup of $G(F/K)$. In such situation,*

$$G(L/K) \simeq G(F/K)/G(F/L)$$

4. *The subgroup diagram of $G(F/K)$ is the inverted diagram of the intermediate field diagram of F over K.*

Galois theory implies that: To understand the field extensions in $F \geq K$, it suffices to understand the group structure of $G(F/K)$.

Proof. (Sketch)

1. Every automorphism in $G(F/L)$ leaves L fixed. So $L \subseteq F_{G(F/L)}$. Note that F is normal over L. Given $\alpha \in F - L$, there is another root $\beta \in F - L$ of the polynomial $\text{irr}(\alpha, L)$. By Thm 4.7, There is an automorphism in $G(F/L)$ that sends α to β. So every $\alpha \in F - L$ is not fixed by $G(F/L)$. Hence $F_{G(F/L)} \subseteq L$. So $L = F_{G(F/L)}$.

2. Let $H \leq G(F/K)$. Every element of H leaves F_H fixed. So $H \leq G(F/F_H)$. It remains to prove that $|H| \geq |G(F/F_H)|$ $(= [F : F_H])$ so that $H = G(F/F_H)$. Since F is a finite normal (=separable+splitting) extension over F_H, we can write $F = F_H(\alpha)$ for some $\alpha \in F - F_H$. Suppose $H := \{\sigma_1, \cdots, \sigma_{|H|}\}$. Denote

$$f(x) := \prod_{i=1}^{|H|} (x - \sigma_i(\alpha)) \in F[x].$$

Every $\sigma_k \in H \leq G(F/K)$ induces a ring automorphism of $F[x]$, with

$$\sigma_k(f(x)) = \prod_{i=1}^{|H|} (x - \sigma_k\sigma_i(\alpha)) = \prod_{i=1}^{|H|} (x - \sigma_i(\alpha)) = f(x).$$

So the coefficients of $f(x)$ are in F_H and $f(x) \in F_H[x]$. The group H contains identity automorphism. So there is some $\sigma_i(\alpha) = \alpha$. So $f(\alpha) = 0$. Then $\text{irr}(\alpha, F_H) \mid f(x)$. So

$$|G(F/F_H)| = [F : F_H] = [F_H(\alpha) : F_H] = \deg(\alpha, F_H) \leq \deg f(x) = |H|.$$

Therefore $H = G(F/F_H)$.

3. L is a normal extension over K
iff L is splitting (and separable) over K;
iff $\sigma(\alpha) \in L$ for any $\alpha \in L$;
(notice that $L = F_{G(F/L)}$) iff $\tau\sigma(\alpha) = \sigma(\alpha)$ for every $\tau \in G(F/L)$;
iff $\sigma^{-1}\tau\sigma(\alpha) = \alpha$;

iff $\sigma^{-1}\tau\sigma \in G(F/L)$ for every $\tau \in G(F/L)$ and $\sigma \in G(F/K)$;
iff $G(F/L)$ is a normal subgroup of $G(F/K)$.

Suppose L is a normal extension over K. We show that $G(L/K) \simeq G(F/K)/G(F/L)$. Since L is splitting over K, if $\sigma \in G(F/K)$ then $\sigma|_L \in G(L/K)$. Define $\phi : G(F/K) \to G(L/K)$ by $\phi(\sigma) := \sigma|_L$. Then ϕ is a group homomorphism. On one hand, every $\widetilde{\gamma} \in G(L/K)$ can be extended to an element $\gamma \in G(F/K)$, with $\phi(\gamma) = \gamma|_L = \widetilde{\gamma}$. So ϕ is onto. On the other hand, $\mathrm{Ker}\,(\phi) = G(F/L)$. Therefore,

$$G(L/K) \simeq G(F/K)/G(F/L).$$

4. The statements 1. and 2. build up the bijection between the set of intermediate fields of F over K and the set of subgroups of $G(F/K)$ in desired order.

□

The following Lagrange's Theorem on Natural Irrationalities discloses further relations on Galois correspondence.

Thm 4.23. *If L and M are intermediate fields between F and K such that L is a finite normal extension of K, then the field (L, M) is finite normal extension of M and $G((L,M)/M) \simeq G(L/L \cap M)$. (show by graph)*

Proof. The idea is to show that: if L is the splitting field over $L \cap M$ of an irred polyn $f \in (L \cap M)[x]$, then (L, M) is the splitting field over M of f. This makes the correspondence. □

Ex. *(HW) Let $K := \mathbf{Q}$ and $F := \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Then $G(F/K)$ consists of 4 elements $\{\iota, \sigma, \tau, \sigma\tau\} \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$:*

$$\begin{aligned}
\iota(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &:= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\
\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &:= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &:= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\
\sigma\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &:= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\end{aligned}$$

The intermediate field diagram of F over K and the subgroup diagram of $G(F/K)$ are inverted to each other.

Ex. *Let $F = \mathbf{Q}(\sqrt[3]{2}, \mathbf{i}\sqrt{3})$ be the splitting field of $(x^3 - 2)$ over $K = \mathbf{Q}$.*

1. *Describe the six elements of $G(F/K)$ by describing their actions on $\sqrt[3]{2}$ and $\mathbf{i}\sqrt{3}$. (done)*

2. *To what group we have seen before is* $G(F/K)$ *isomorphic? (done)*
3. *Give the diagrams for the subfields of* F *and for the subgroups of* $G(F/K)$*.*

4.3 Illustration of Galois Theory

4.3.1 Some Examples

Def. *The* **Galois group of a polynomial** $f \in K[x]$ **over a field** K, *denoted by* $G(f/K)$, *is the group* $G(F/K)$ *where* F *is a splitting field over* K *of* f.

When $K = \mathbf{Q}$, the preceding examples show

1. the Galois group of $(x^2-2)(x^2-3) \in \mathbf{Q}[x]$ is $\mathbf{Z}_2 \times \mathbf{Z}_2$, and
2. the Galois group of $x^3 - 2 \in \mathbf{Q}[x]$ is $S_3 = D_3$.

Here S_n denotes the group of permutations of n letters, and D_n denotes the symmetric group of a regular n-gon.

Ex. *The Galois group of* $x^3 - 1 \in \mathbf{Q}[x]$ *is* $\mathbf{Z}_2$, *which is totally different from the Galois group of* $x^3 - 2 \in \mathbf{Q}[x]$.

Ex. *Find the Galois groups of the following polynomials in* $\mathbf{Q}[x]$*:*

1. $x^4 + 1$. *(*$\mathbf{Z}_2 \times \mathbf{Z}_2$*)*
2. $x^4 - 1$. *(*$\mathbf{Z}_2$*)*
3. $x^4 - 2$. *(*D_4*. See p.275 of [Hungerford, V.4])*

The Galois group G of an irreducible separable polynomial $f(x) \in K[x]$ of degree $n = 2, 3, 4$ has been classified [see Hungerford, V.4].

1. $n = 2$, then G must be $S_2 \simeq \mathbf{Z}_2$.
2. $n = 3$, then G could be S_3 or $A_3 \simeq \mathbf{Z}_3$.
3. $n = 4$, then G could be S_4, A_4, D_4, $\mathbf{Z}_4$, or $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Let us discuss the Galois group of irreducible $f(x) \in \mathbf{Q}[x]$ of degree 3.

Def. *char* $K \neq 2$*;* $f \in K[x]$ *a polyn with distinct roots* $u_1, \cdots, u_n$. $F = K(u_1, \cdots, u_n)$ *the splitting field over* K *of* f. *Denote*

$$\Delta = \prod_{i<j} (u_i - u_j) \in F;$$

define the **discriminant** *of* f *as* $D = \Delta^2$.

Prop 4.24. *Let K, f, F and Δ be as in preceding definition.*

1. *For each $\sigma \in G(F/K) \leq S_n$, σ is an even [resp. odd] permutation iff $\sigma(\Delta) = \Delta$ [resp. $\sigma(\Delta) = -\Delta$].*

2. *The discriminant $\Delta^2 \in K$.*

Cor 4.25. *$F \geq K(\Delta) \geq K$. Consider $G = G(F/K) \leq S_n$. In the Galois correspondence, the subfield $K(\Delta)$ corresponds to the subgroup $G \cap A_n$. In particular, G consists of even permutations iff $\Delta \in K$.*

Cor 4.26. *Given a degree 3 irred separable polyn $f(x) = x^3 + bx^2 + cx + d \in K[x]$, let*

$$g(x) = f(x - b/3) = x^3 + px + q.$$

Then **the discriminant of $f(x)$ is $\Delta^2 = -4p^3 - 27q^2 \in K$**.

1. *If $-4p^3 - 27q^2$ is a square in K, then $G(f/K) = A_3 \simeq \mathbf{Z}_3$;*

2. *If $-4p^3 - 27q^2$ is not a square in K, then $G(f/K) = S_3$.*

Ex. *Consider the foll irred polyns in $\mathbf{Q}[x]$:*

1. *$f(x) = x^3 - 2$. Then $\Delta^2 = -27 \times 2^2$ is not a square in $\mathbf{Q}$. So $G(f/\mathbf{Q}) = S_3$ (as we have proved).*

2. *$f(x) = x^3 + 3x^2 - x - 1$. Then $g(x) = f(x - 3/3) = x^3 - 4x + 2$ is irreducible. The discriminant of $f(x)$ is $-4(-4)^3 - 27(2)^2 = 148$, which is not a square in $\mathbf{Q}$. Thus $G(f/\mathbf{Q}) = S_3$.*

3. *$f(x) = x^3 - 3x + 1$ is irreducible. The discriminant is $-4(-3)^3 - 27(1)^2 = 81$, which is a square in $\mathbf{Q}$. So $G(f/\mathbf{Q}) = A_3 \simeq \mathbf{Z}_3$.*

In general, it is difficult to compute the Galois group of an irreducible polynomial of degree $n \geq 5$. There is a special result:

Thm 4.27. *p is prime, $f(x) \in \mathbf{Q}[x]$ an irred polyn of deg p with exactly two nonreal roots in $\mathbf{C}$, then $G(f/\mathbf{Q}) = S_p$.*

4.3.2 Finite Groups as Galois Groups

Thm 4.28. *Let G be the Galois group of an irreducible separable polynomial $f(x) \in K[x]$ of degree n. Then $G \leq S_n$ and $n \mid |G| \mid n!$.*

Next we show that every finite group is the Galois group of a finite normal extension.

Let $y_1, \cdots, y_n$ be indeterminates. The field $F := \mathbf{Q}(y_1, \cdots, y_n)$ consists of all rational functions of $y_1, \cdots, y_n$. Every permutation $\sigma \in S_n$ induces a map $\overline{\sigma} \in G(F/\mathbf{Q})$ by

$$\overline{\sigma}\left(\frac{f(y_1, \cdots, y_n)}{g(y_1, \cdots, y_n)}\right) := \frac{f(y_{\sigma(1)}, \cdots, y_{\sigma(n)})}{g(y_{\sigma(1)}, \cdots, y_{\sigma(n)})}.$$

Denote $\overline{S}_n := \{\overline{\sigma} \mid \sigma \in S_n\} \leq G(F/\mathbf{Q})$. The subfield of F fixed by $\overline{S}_n$ is $K = \mathbf{Q}(s_1, \cdots, s_n)$, where $s_1, \cdots, s_n$ are the following symmetric functions of $y_1, \cdots, y_n$ over $\mathbf{Q}$:

$$\begin{aligned} s_1 &:= y_1 + y_2 + \cdots + y_n, \\ s_2 &:= y_1y_2 + y_1y_3 + \cdots + y_{n-1}y_n, \\ &\cdots\cdots \\ s_n &:= y_1y_2\cdots y_n \end{aligned}$$

Now $F = K(y_1, \cdots, y_n)$, and

$$\begin{aligned} f(x) &:= (x - y_1)(x - y_2)\cdots(x - y_n) \\ &= x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \in K[x] \end{aligned}$$

So $F = \mathbf{Q}(y_1, \cdots, y_n)$ is the splitting field of $f(x)$ over $K = \mathbf{Q}(s_1, \cdots, s_n)$, where $y_1, \cdots, y_n$ are the roots of $f(x)$. Every element of $G(F/K)$ permutes the n roots of $f(x)$. This shows that:

1. $G(F/K) = \overline{S}_n \simeq S_n$ and $|G(F/K)| = n!$.

2. (**Every finite group is the Galois group of a finite normal extension**) By Cayley's Theorem, every finite group H is isomorphic to a subgroup of certain S_n. By Galois theory, there is an intermediate field F_0 such that $\mathbf{Q} \geq F \geq F_0 \geq K$, and $H \simeq G(F/F_0)$.

3. It is an open problem that which finite group is the Galois group of a finite normal extension over a given field (e.g. $\mathbf{Q}$).

4.4 Cyclotomic Extensions

Def. *The splitting field F of $x^n - 1$ over K is the* **cyclotomic extension of K of order n**.

Def. *An element $u \in \overline{K}$ is a* **primitive n-th root of unity** *if $u^n = 1$ and $u^k \neq 1$ for any positive integer $k < n$.*

The cyclotomic extension of order n is related to the **Euler function** $\varphi(n)$, where $\varphi(n)$ is the number of integers i such that $1 \leq i \leq n$ and $\gcd(i, n) = 1$. If $n = p_1^{m_1} \cdots p_k^{m_k} = \prod_{i=1}^k p_i^{m_i}$ is the prime factorization of n (where p_i are distinct primes), then

$$\varphi(n) = \prod_{i=1}^{k} [p_i^{m_i - 1}(p_i - 1)] = n \prod_{i=1}^{k} (1 - 1/p_i)$$

When $d \mid n$, $\varphi(d)$ equals to the number of integers i such that $1 \leq i \leq n$ and $\gcd(i, n) = n/d$. Therefore, $\sum_{d|n} \varphi(d) = n$.

4.4.1 Cyclotomic extensions over Q

Let $\overline{\mathbf{Q}} \subset \mathbf{C}$. Consider the splitting field of $x^n - 1$ over $\mathbf{Q}$. There exists a primitive n-th root of unity $\zeta \in \mathbf{C}$. All the other primitive n-th roots of unity are ζ^i where $1 \leq i \leq n$ and $\gcd(i, n) = 1$. So there are $\varphi(n)$ elements conjugate to ζ over $\mathbf{Q}$. Denote

$$g_n(x) = \prod_{\substack{1 \leq i \leq n \\ \gcd(i,n)=1}} (x - \zeta^i).$$

Then $g_n(x) = \mathrm{irr}(\zeta, \mathbf{Q}) \in \mathbf{Q}[x]$ has degree $\varphi(n)$. $g_n(x)$ is called **the n-th cyclotomic polynomial over $\mathbf{Q}$**.

Thm 4.29. *Let $F = \mathbf{Q}(\zeta)$ be a cyclotomic extension of order n of the field $\mathbf{Q}$, and $g_n(x)$ the n-th cyclotomic polynomial over $\mathbf{Q}$. Then*

1. *$g_n(x) \in \mathbf{Z}[x]$ and $g_n(x)$ is irreducible in $\mathbf{Z}[x]$ and $\mathbf{Q}[x]$. Moreover,*

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

2. *$[F : \mathbf{Q}] = \varphi(n)$, where φ is the Euler function.*

3. *The Galois group* $G(F/\mathbf{Q})$ *of* $x^n - 1$ *is isomorphic to the multiplicative group of units in the ring* $\mathbf{Z}_n$*.*

Ex. *If* p *is a prime, then the Galois group of* $x^p - 1 \in \mathbf{Q}[x]$ *is isomorphic to the cyclic group* $\mathbf{Z}_{p-1}$*.*

Ex. *Consider the cyclotomic extension* F_n *of degree* n *over* $\mathbf{Q}$*:*

1. $n = 9 = 3^2$*. Then* $\varphi(9) = 3 \cdot 2 = 6$*. The multiplicative group in* $\mathbf{Z}_9$ *is* $A = \{1, 2, 4, 5, 7, 8\}$*. Notice that* 2 *generates* A*. So* $G(F_9/\mathbf{Q}) \simeq A \simeq \mathbf{Z}_6$*.*

2. $n = 12 = 2^2 \cdot 3$*. Then* $\varphi(12) = 2 \cdot 2 = 4$*. The multiplicative group in* $\mathbf{Z}_{12}$ *is* $A = \{1, 5, 7, 11\} \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_2$*. So* $G(F_{12}/\mathbf{Q}) \simeq A \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_2$*.*

3. *Likewise,* $G(F_8/\mathbf{Q}) \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_2$ *and* $G(F_{14}/\mathbf{Q}) \simeq \mathbf{Z}_6$*.*

4.4.2 Cyclotomic Extensions over K

If $\operatorname{char} K = p \neq 0$ and $n = mp^t$ with $\gcd(p, m) = 1$, then $x^n - 1 = (x^m - 1)^{p^t}$, so that a cyclotomic extension of order n coincides with one of order m.

Now we consider the cyclotomic extensions where $\operatorname{char} K = 0$ or $\operatorname{char} K$ does not divide n. Let ζ denote a primitive n-th root of unity over K. Then all primitive n-th root of unity over K are ζ^i for $1 \leq i \leq n$ and $\gcd(i, n) = 1$. However, some ζ^i may not be conjugate to ζ over K anymore. We have

$$\operatorname{irr}(\zeta, K) \mid g_n(x) = \prod_{\substack{1 \leq i \leq n \\ \gcd(i,n)=1}} (x - \zeta^i),$$

where $g_n(x)$ is called **the n-th cyclotomic polynomial over** K. Moreover, the following theorem says that $\deg(\zeta, K) \mid \deg g_n(x) = \varphi(n)$.

Thm 4.30. *Let* K *be a field such that* $\operatorname{char} K$ *does not divide* n*, and* F *a cyclotomic extension of* K *of order* n*.*

1. $F = K(\zeta)$*, where* $\zeta \in F$ *is a primitive* n*-th root of unity.*

2. $G(F/K)$ *is isomorphic to a subgroup of order* d *of the multiplicative group of units of* $\mathbf{Z}_n$*. In particular,* $[F : K] = |G(F/K)| = d$ *divides* $\varphi(n)$*.*

3. $x^n - 1 = \prod_{d|n} g_d(x)$*. Moreover,* $\deg g_n(x) = \varphi(n)$*, and the coefficients of* $g_n(x)$ *are integers (in* $\mathbf{Z}$ *or* $\mathbf{Z}_p$*, depending on* $\operatorname{char} K$*).*

Ex. *If ζ is a primitive 5th root of unity in* $\mathbf{C}$*, then*

1. $\mathbf{Q}(\zeta)$ *is a cyclotomic extension of* $\mathbf{Q}$ *of order* 5*, with* $G(\mathbf{Q}(\zeta)/\mathbf{Q}) \simeq \mathbf{Z}_4$.
2. $\mathbf{R}(\zeta)$ *is a cyclotomic extension of* $\mathbf{R}$ *of order* 5*, with* $G(\mathbf{R}(\zeta)/\mathbf{R}) \simeq \mathbf{Z}_2$. ζ *satisfies that* $\zeta + 1/\zeta = 2Re(\zeta)$. *So* $irr(\zeta, \mathbf{R}) = x^2 - 2Re(\zeta)\, x + 1$.

4.5 Galois Theory on Finite Fields

4.5.1 Structure of Finite Fields

Examples of finite fields include $\mathbf{Z}_p$ for primes p. We will see that every finite field F has a prime characteristic p, and $F \simeq \mathbf{Z}_p(\alpha)$ where $\alpha \in \overline{Z}_p$ is a *primitive root* of $x^{p^n-1} - 1$ in $\mathbf{Z}_p[x]$.

The characteristic of a field F is either 0 or a prime p.

1. If $\operatorname{char} F = 0$, then F is an extension of $\mathbf{Q}$.

2. If $\operatorname{char} F = p$ for a prime p, then F is an extension of $\mathbf{Z}_p$. A finite field F is simply a finite extension of $\mathbf{Z}_p$.

Thm 4.31. *Let E be a finite extension of F with $[E : F] = m$, where F is a finite field of q elements. Then E has q^m elements. In particular, the finite field E contains exactly p^n elements for $p = \operatorname{char} E$ and $n = [E : \mathbf{Z}_p]$.*

Thm 4.32. *For every prime power p^n, there is a unique (up to isomorphism) finite field $GF(p^n)$ which contains exactly p^n elements. If $\overline{\mathbf{Z}_p} \geq GF(p^n) \geq \mathbf{Z}_p$, the elements of $GF(p^n)$ are precisely the roots of $x^{p^n} - x \in \mathbf{Z}_p[x]$ in $\overline{\mathbf{Z}_p}$.*

• The multiplicative group $\langle F^*, \cdot\rangle$ of nonzero elements of a finite field F is cyclic.

• A finite extension E of a finite field F is a simple extension of F. Because if $|E| = p^n$ (i.e. E is a finite extension of $F := \mathbf{Z}_p$), let $\alpha \in \overline{Z}_p$ be a primitive $(p^n - 1)$-th root of unity, then $E = \mathbf{Z}_p(\alpha) = F(\alpha)$.

• For $\alpha \in \overline{\mathbf{Z}}_p$, the degree $\deg(\alpha, \mathbf{Z}_p) = n$ iff $\mathbf{Z}_p(\alpha) = \mathrm{GF}(p^n)$, iff α is a primitive $(p^n - 1)$-root of unity in $\overline{\mathbf{Z}}_p$.

Ex. *That are $\varphi(p^n-1)$ many primitive (p^n-1)-roots of unity in $GF(p^n)$. So the number of degree n irreducible polynomials in $\mathbf{Z}_p[x]$ is equal to $\frac{\varphi(p^n-1)}{n}$. Moreover, $x(x^{p^n-1} - 1) = x^{p^n} - x \in \mathbf{Z}_p[x]$ is the product of all degree m irreducible polynomials for $m \mid n$.*

• If $\mathrm{GF}(p^n) \geq \mathrm{GF}(p^m) \geq \mathbf{Z}_p$, then $m \mid n$. So it is easy to draw the intermediate field diagram of $\mathrm{GF}(p^n)$. Moreover, every $\mathrm{GF}(p^n)$ is a normal extension over $\mathbf{Z}_p$ and $\mathrm{GF}(p^m)$ for $m \mid n$.

4.5.2 Galois Groups of Finite Fields

Thm 4.33. *If F is a field of characteristic p and r is a positive integer, then $\sigma_r : F \to F$ given by $\sigma_r(u) = u^{p^r}$ is a $\mathbf{Z}_p$-monomorphism of fields.*

It is clear that $\sigma_r \sigma_s = \sigma_{r+s}$.

Cor 4.34.

1. $G(GF(p^n)/\mathbf{Z}_p) = \{1, \sigma_1, \sigma_2, \cdots, \sigma_{n-1}\} \simeq \mathbf{Z}_n$.
2. *When* $m \mid n$, $G(GF(p^n)/GF(p^m)) = \{1, \sigma_m, \sigma_{2m}, \cdots, \sigma_{(\frac{n}{m}-1)m}\} \simeq \mathbf{Z}_{n/m}$.
3. $G(\overline{Z_p}/\mathbf{Z}_p) \gneq \{\cdots, \sigma_{-2}, \sigma_{-1}, 1, \sigma_1, \sigma_2, \cdots\} \simeq \mathbf{Z}$.

Ex. $x^3 - 3x + 1 \in \mathbf{Z}_5[x]$ *is irreducible. The Galois group of* $x^3 - 3x + 1$ *over* $\mathbf{Z}_5$ *is* $\{1, \sigma_1, \sigma_2\} \simeq \mathbf{Z}_3$.

Ex. *Describe the Galois correspondence between the intermediate fields of* $GF(p^{12})$ *over* $\mathbf{Z}_p$ *and the subgroups of* $G(GF(p^{12})/\mathbf{Z}_p)$.

• If $\alpha \in \overline{\mathbf{Z}}_p$ has $\deg(\alpha, \mathbf{Z}_p) = [\mathbf{Z}_p(\alpha) : \mathbf{Z}_p] = n$, then all the $\mathbf{Z}_p$-conjugates of α in $\overline{\mathbf{Z}}_p$ are

$$\{1(\alpha), \sigma_1(\alpha), \sigma_2(\alpha), \cdots, \sigma_{n-1}(\alpha)\} = \{\alpha, \alpha^{p^1}, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}\}.$$

The irreducible polynomial of α over $\mathbf{Z}_p$ is

$$\mathrm{irr}(\alpha, \mathbf{Z}_p) = \prod_{k=0}^{n-1} \left(x - \alpha^{p^k}\right)$$

Similarly, when $m \mid n$, the irreducible polynomial of α over $\mathrm{GF}(p^m)$ is

$$\mathrm{irr}(\alpha, \mathrm{GF}(p^m)) = \prod_{k=0}^{\frac{n}{m}-1} \left(x - \alpha^{p^{km}}\right)$$

4.6 Radical Extensions

4.6.1 Solvable Groups

Def. *A finite group G is* **solvable** *if there exists a subgroup sequence*

$$\{1\} = G_0 \leq G_1 \leq G_2 \cdots \leq G_n = G \tag{4.1}$$

such that $G_i \lhd G_{i+1}$ and G_{i+1}/G_i is an abelian group for $i = 0, \cdots, n-1$.

Remark. *If H is a finite abelian group, then there exists a subgroup sequence*

$$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_t$$

such that H_{i+1}/H_i is a cyclic group of prime order. So after making a refinement on the equence (4.1), we may assume that $G_i \lhd G_{i+1}$ and G_{i+1}/G_i is an (abelian) cyclic group of prime order.

We give another definition of solvable groups using derived subgroups. The **commutator subgroup** G' of G is the subgroup of G generated by the set $\{aba^{-1}b^{-1} \mid a, b \in G\}$.

Lem 4.35. *$G' \lhd G$, and G' is the minimal normal subgroup of G such that G/G' is an abelian group.*

Let

$$G^{(0)} = G, \quad G^{(1)} = G', \quad \cdots, \quad G^{(i+1)} = (G^{(i)})', \quad \cdots$$

Then $G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$ and $G^{(i)} \rhd G^{(i+1)}$ for $i = 0, 1, 2, \cdots$. The group $G^{(i)}$ is called **the i-th derived subgroup of G**.

Lem 4.36. *A finite group G is solvable iff $G^{(n)} = \{1\}$ for some n.*

Ex.

1. *D_4 is solvable. Every finite group of order p^n for a prime p is solvable.*
2. *A_4 is solvable.*
3. *A_5 is insolvable. Indeed, A_5 is the smallest insolvable group.*

Thm 4.37. *If G is a finite solvable group, then every subgroup and every quotient group of G are solvable.*

Equivalently, if G contains an insolvable subgroup or quotient group, then G is also insolvable.

A remarkable result by W. Feit and J. Thompson claims that every finite group of odd order is solvable.

4.6.2 Radical Extensions

Def. *An extension field F of K is a* **radical extension** *of K if $F = K(u_1, \cdots, u_n)$, some powers of u_1 lies in K and for each $i \geq 2$, some power of u_i lies in $K(u_1, \cdots, u_{i-1})$.*

In other words, $F = K(u_1, \cdots, u_n)$ is a radical extension of K if each of u_i can be expressed by finite step operations of $+, -, \cdot, /$, and $\sqrt[n]{\ }$ on certain elements of K.

Def. *Let K be a field and $f \in K[x]$. The equation $f(x) = 0$ is* **solvable by radicals** *if there exists a radical extension F of K such that the splitting field E of f over K satisfies that $K \subset E \subset F$.*

Thm 4.38. *If F is a radical extension field of K and E is an intermediate field, then $G(E/K)$ is a solvable group.*

Here E is not required to be splitting or seperable over K.

Thm 4.39. *If $f(x) \in K[x]$ is separable over K, and E is the splitting (normal) field of $f(x)$ over K, then $f(x) = 0$ is solvable by radicals if and only if $G(E/K)$ is a solvable group.*

Ex. *When $\mathrm{char}\, K = 0$, or $p := \mathrm{char}\, K$ does not divide $n!$ where $n := \deg f(x)$, the polynomial $f(x)$ is separable. So we can apply the theorem.*

Ex. *A_5 is insolvable. So S_5 is insolvable. There exists a degree 5 polynomial (a quintic) $f(x) \in K[x]$ that has Galois group isomorphic to S_5. Then some roots of $f(x) = 0$ are insolvable by radicals.*

For example, the Galois group of $f(x) = x^5 - 4x + 1 \in \mathbf{Q}[x]$ is S_5, which is insolvable. So $x^5 - 4x + 1 = 0$ is insolvable by radicals over $\mathbf{Q}$.

Thus it is impossible to find a general radical formula to solve the roots of a generic polynomial of degree $n \geq 5$.

Ex. *There are some famous geometric construction problems using a straightedge and a compass. A number α is* **constructible** *if α can be obtained by using straightedge and compass (initially with unit width) finitely many times.*

It is easy to see that: if α and $\beta \neq 0$ are constructible, then so are $\alpha \pm \beta$, $\alpha \cdot \beta$, and α/β. So the set of all constructible numbers form a field. The curves drawn by straightedge and compass are of degrees 1 and 2. If a field K consists of constructible numbers, and $\deg(\alpha, K) = 2$, then α

is constructible. In fact, every constructible number can be obtained by a sequence of field extensions

$$Q = F_0 \subset F_1 \subset F_2 \subset \cdots, \qquad [F_{i+1} : F_i] = 2.$$

So α *is constructible iff* α *is algebraic over* $\mathbf{Q}$ *and* $\deg(\alpha, \mathbf{Q}) = 2^m$. *Therefore, using straightedge and compass,*

1. *trisecting a generic angle is impossible;*
2. *doubling the volume of a cube is impossible;*
3. *(Gauss) a regular* n*-gon is constructible iff* $\cos \frac{2\pi}{n}$ *is constructible, iff a primitive* n*-root of unity, say* ζ*, is constructible, iff* $irr(\zeta, \mathbf{Q}) = \varphi(n) = 2^m$*, iff* n *is a product of a power of* 2 *and some distinct odd primes of the form* $p = 2^t + 1$*. However, if* t *has an odd factor* $s > 1$*, then* $2^{t/s} + 1$ *divides* $2^t + 1$*. So* $t = 2^k$ *and thus* $p = 2^{2^k} + 1$ *(called a Fermat prime). Overall, a regular* n*-gon is constructible iff* $n = 2^\ell p_1 p_2 \cdots p_q$*, where* p_i *are distinct Fermat primes. The following regular* n*-gons are constructible using straightedge and compass:*

   $$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, \cdots, 120, \cdots, 256, \cdots$$

   However, the regular 9*-gon is inconstructible.*