Galois Theory
Concise Notes

MATH60037

Arnav Singh

Content from prior years assumed to be known.

Mathematics
Imperial College London
United Kingdom
April 12, 2023

Contents

1 What is Galois Theory?

1.1 Field extensions

Definition 1.1. *A **field homomorphism** a function $\phi : K_1 \to K_2$ that preserves the field operations $\forall a, b \in K_1$*

$$\phi(a+b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \phi(0_{K_1}) = 0_{K_2} \quad \phi(1_{K_1}) = \phi 1_{K_2}$$

Definition 1.2. *α **algebraic** over k if $f(\alpha) = 0$ for some $0 \neq f \in k[X]$, otherwise α **transcendental** over k*

*Extension $k \subset K$ **algebraic** if $\forall \alpha \in K, \alpha$ is algebraic over k*

Definition 1.3. *Consider field k and $f \in k[X]$. Say $k \subset K$ a **splitting field** for f if*

$$f(X) = a \prod_{i=1}^{n} (X - \lambda_i) \in K[X], \quad K = k(\lambda_1, \ldots, \lambda_n)$$

1.2 Galois correspondence

Theorem 1.4. *(Fundamental theorem of Galois Theory, Galois correspondency)*

Assume characteristic 0. Let $k \subset K$ be the splitting field of $f(X) \in k[X]$ Let

$$G = \{\sigma : K \to K \mid \sigma \text{ a field automorphism}, \sigma\,|_k = id_k\}$$

*Call this the **Galois group**. There is a one-to-one correspondence*

$$\{k \subset K_1 \subset K \mid K_1 \text{ a subfield }\} \leftrightarrow \{H \leq G \mid H \text{ a subgroup}\}$$

$$K_1 \leftrightarrow \{\sigma \in G \mid \forall k \in K_1, \sigma(\lambda) = \lambda$$

$$\{\lambda \in K \mid \forall \sigma \in H, \sigma(\lambda) = \lambda\} \leftrightarrow \{H \leq G\}$$

Definition 1.5. *$K \subset L$ is **finite** if L a finite-dimensional K-vector space. The **degree** of L over K is*

$$[L : K] = dim_K L$$

Theorem 1.6. *(Tower Law)*

Let $K \subset L \subset F$ Then

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

Theorem 1.7. *Suppose $f(X) in K[X]$ irreducible such that $f(\lambda) = 0$, then $[K(\lambda) : K] = deg\, f$*

2 Fundamental theorem of Galois Theory

2.1 Elementary facts

Definition 2.0. *$K \subset L, a \in L$. We say the **evaluation homomorphism***

$$e_a \colon K[X] \to K[a] \subset L, f(X) \mapsto f(a)$$

is a surjective ring homomorphism, where $K[a]$ the smallest subring of L containing K and a

Definition 2.1. *$f(X) = a_0 X^n + \ldots + a_n \in K[X]$ is **monic** if $a_0 = 1$*

Lemma 2.2. *.*

- *If a transcendental, e_a is injective and it extends to $\widetilde{e}_a : K(X) \to K(a)$ by*

$$DIAGRAMHERE$$

- *If a algebraic then $\ker e_a = \langle f_a \rangle$ where $f_a \in K[X]$ irreducible or prime, and unique if f monic, then called the **minimal polynomial of** $a \in L/K$. In this case*

$$DIARGRAM\ HERE$$

Corollary 2.3. *For $K \subset L$ and $a \in L$ algebraic over K*

- *$[K(a) : K] = deg\, f_a$, and*
- *If $K \subset F$ an extension*

$$\underset{K}{Em}(K(a), F) = \{b \in F \mid f_a(b) = 0\}$$

Corollary 2.4. *Let K a field and $f \in K[X]$. Then $\exists K \subset L$ s.t f has a root in L*

REMARK TO ADD HERE

2.2 Axiomatics

Proposition 2.5. *Fix $k \subset K$ and $k \subset L$ Then*

$$\# \underset{k}{Em}(K, L) \leq [K : k]$$

Proposition 2.6. *Suppose given 2 field extensions $k \subset K$ and $k \subset L$. Then there is a non-unique bigger common field containing both.*

$$DIAGRAM\ HERE$$

Formally: given $\sigma_1 \in Em(k, K)$ and $\sigma_2 \in Em(k, L)$ then $\exists \Omega, \phi_1 \in Em(k, \Omega)$ and $\phi_2 \in Em(L, \Omega)$ such that $\phi_1 \circ \sigma_1 = \phi_2 \circ \sigma_2$

Alternatively: $\exists k \subset \Omega$ such that $Em_k(K, \Omega)$ and $Em_k(L, \Omega)$ are both non-empty

Proposition 2.7. *Let L be any field and G a finite group action on L as automorphism. Let*

$$K = G^* = Fix\, G = L^G = \{\lambda \in L \mid \forall \sigma \in G, \sigma(\lambda) = \lambda\}$$

Consider $Aut_K\, L = K^\dagger$. Then the obvious inclusion $G \subset K^\dagger = (G^*)^\dagger$ is an equality, so G is all of $K^\dagger$.
Remark

We have to contextualise half of the Galois correspondence

$$\{F \mid k \subset F \subset \Omega\} \leftrightarrow \{G \mid G \leq \underset{k}{Aut}\, \Omega\}$$
$$F \leftrightarrow \underset{k}{Aut}\, \Omega = F^\dagger$$
$$Fix\, G = G^* \leftrightarrow G$$

Lemma 2.8. *$K \subset L$ a finite extension of degree $[L : K] \leq \#G$*

2.3 Galois correspondence

Definition 2.9. *$k \subset K$ is **normal** if*

$$\forall k \subset \Omega, \forall \sigma_1, \sigma_2 \in Em_k(K, \Omega), \exists \sigma \in Em_k(K, K), \sigma_2 = \sigma_1 \circ \sigma$$

Equivalently $k \subset K$ is normal if

$$\forall k \subset \Omega, \forall \sigma_1, \sigma_2 \in Em_k(K, \Omega), \sigma_2(K) \subset \sigma_1(K)$$

Remark

Will see later that $k \subset K$ is normal if and only if $\exists f(X) \in k[X]$ such that K a splitting field of f

Lemma 2.10. *Suppose $k \subset K$ normal. Consider $k \subset L \subset K$ Then also $L \subset K$ is normal*

Definition 2.11. *$k \subset K$ is* ***separable*** *if $\forall k \subset K_1 \subset K_2 \subset K$, if $K_1 \neq K_2$ then $\exists k \subset \Omega$ and embeddings $x \in Em_k(K_1, \Omega)$ and $y_1, y_2 \in Em_k(K_2, \Omega)$ such that*

DIAGRAM HERE

That is $y \mid_{K_1} = x$ but $y_1 \neq y_2$
We have that embeddings separate fields. Will see that

- *in Char 0, everything is separable*
- *in Char p there are good ways to decide if a field is separable*

Lemma 2.12. *Suppose $k \subset K \subset L$ Then $k \subset L$ separable if and only if $k \subset K, K \subset L$ is separable*

Theorem 2.13. *(Fundamental theorem of Galois theory, Galois correspondence)*
Let $k \subset K$ be normal and separable. Let $G = Em_k(K, K)$ then there is a one-to-one correspondence

$$\{k \subset L \subset K\} \leftrightarrow \{H \leq G\}$$
$$L \to L^\dagger = \{\sigma \in G \mid \forall \lambda \in L, \sigma(\lambda) = \lambda\}$$
$$H^* = \{\lambda \in K \mid \forall \sigma \in H, \sigma(\lambda) = \lambda\} \leftarrow H$$

Lemma 2.14. *Suppose $k \subset K$ normal. Then for all towers $k \subset F \subset K \subset \Omega$, the natural restriction*

$$\rho : Em_k(K, \Omega) \to Em_k(F, \Omega)$$

is surjective

Corollary 2.15. *Suppose $k \subset K$ normal. Then for all towers $k \subset F \subset K \subset \Omega$*

$$Em_k(F, K) \to Em_k(F, \Omega)$$

is also surjective

3 Normal and separable extensions

3.1 Normal extensions

Theorem 3.1. *For finite $k \subset K$, the following are equivalent*

1. *$\forall f \in k[X]$ irreducible, either f has no roots in K or f splits completely in K*
2. *$\exists f \in k[X]$ not necessarily irreducible such that K is a splitting field of f*
3. *$k \subset K$ is normal*

Proposition 3.2. *Let $k \subset L$ be a field extension. Then there exists a tower $k \subset L \subset K$ such that $k \subset K$ is normal*

3.2 Separable polynomials

Definition 3.3. *A polynomial $f \in k[X]$ is* ***separable*** *if it has $n = deg(f)$ distinct roots in any field $k \subset K$ such that $f \in K[X]$ splits completely*
Remark
It is not completely obvious that this definition is independent of K - use the fact that 2 splitting fields are isomorphic.

Remark 3.0. *Derivative*

$$D\colon k[X] \to k[X], X^n \mapsto nX^{n-1}$$

Having the following properties

- *D is k-linear, that is $\forall \lambda, \mu \in k, \forall f, g \in k[X]$*

$$D(\lambda f + \mu g) = \lambda Df + \mu Dg$$

- *Leibnitz rule, $\forall f, g \in k[X]$*

$$Dfg = fDg + gDf$$

Proposition 3.4. *$f(X) \in k[X]$ is separable if and only if $gcd(f, Df) = 1$*

Lemma 3.5. *Let $f, g \in k[X]$ and $c = gcd(f, g) \in k[X]$*
Let $k \subset L$ an extension, then $c = gcd(f, g) \in L[X]$

Theorem 3.6. *$f \in k[X]$ irreducible is inseparable if and only if*

- *$ch(k) = p > 0$, and*
- *$\exists h \in k[X]$ such that $f(X) = h(X^p)$*

Definition 3.7. *A field k in $ch(k) = p > 0$ is **perfect** if $\forall a \in k$ there exists $b \in k$ such that $b^p = a$*

Proposition 3.8. *If k is perfect then $f \in k[X]$ is irreducible implies that $f(X)$ is separable*

Definition 3.9. *Consider $k \subset L$. An element $a \in L$ is **separable** over k if the minimal polynomial $f(X) \in k[X]$ of a is a separable polynomial*

3.3 Separable degree

Definition 3.10. *Let $k \subset K$. Choose $K \subset \Omega$ such that $k \subset \Omega$ is normal. Define the **separable degree** as*

$$[K : k]_s = \#Em_k(K, \Omega)$$

Remark
$[K : k]_s$ does not depend on $K \subset \Omega$. Suppose $k \subset \Omega_1$ and $k \subset \Omega_2$ are normal. Then there exists a bigger field $\widetilde{\Omega}$ such that $\Omega_1 \subset \widetilde{\Omega}, \Omega_2 \subset \widetilde{\Omega}$ Then

$$Em_k(K, \Omega_1) = Em_k(K, \widetilde{\Omega}) = Em_k(K, \Omega_2)$$

Remark
Restate definition of separable extension. Recall $k \subset K$ separable if for all towers $k \subset K_1 \subset K_2 \subset K$ there exists $\Omega, y : K_1 \to \Omega, x_1, x_2 : K_2 \to \Omega$ such that $x_1 \neq x_2$ and $x_1 |_{K_1} = x_2 |_{K_2} = y$ so $[K_2 : K_1] \neq 1$. Thus $k \subset K$ separable if for all towers $k \subset K_1 \subset K_2 \subset K$ $[K_2 : K_1]_s = 1$ implies that $K_1 = K_2$

Theorem 3.11. *(Tower Law)*
$\forall k \subset K \subset L$

$$[L : K]_s = [L : K]_s [K : k]_s$$

3.4 Separable extensions

Recall that for $k \subset K$, said $a \in K$ separable if minimal polynomial of $f(X) \in k[X]$ of a is separable polynomial

Theorem 3.12. *$k \subset K$ is separable if and only if $[K : k]_s = [K : k]$*

Corollary 3.13. *For all towers $k \subset K \subset L$ if $k \subset K$ and $K \subset L$ are separable then $k \subset L$ is separable*

Corollary 3.14. *$k \subset K$ is separable if and only if $\forall a \in K$, a is separable over k*

Lemma 3.15. *Let $k \subset L \subset K$. For $\lambda \in K$, λ is separable over k implies that λ is separable over L*

4 Examples

4.1 Biquadratic extensions

Let

$$K \subset K\left(\sqrt{a \pm \sqrt{b}}\right) = L, \quad c = a^2 - b, \quad \beta = \sqrt{b} \notin K, \quad \alpha = \sqrt{a+\beta} \in L, \quad \alpha' = \sqrt{a-\beta} \in L$$

We know that $\pm\alpha, \pm\alpha'$ are roots of

$$f(X) = X^4 - 2aX^2 + c$$

Not assuming that $f(X)$ is irreducible. Let

$$\delta = \alpha + \alpha' \quad \delta' = \alpha - \alpha', \quad \gamma = \alpha\alpha' = \sqrt{c}$$

Then

$$\gamma^2 = c, \quad \delta^2 = 2(\alpha+\gamma), \quad \delta^2 = 2(\alpha-\gamma), \quad \delta\delta' = 2\beta, \quad \alpha = \frac{\delta+\delta'}{2}, \quad \alpha' = \frac{\delta-\delta'}{2}$$

and we have $\pm\delta, \pm\delta'$ are roots of

$$g(Y) = Y^4 - 4aY^2 + 4b$$

Then L is the splitting field of g. Assume

1. $ch(K) \neq 2$ and
2. b is not a square in K , that is $[K(\beta) : K] = 2$

Claim that the extension $K \subset L$ is separable.
It is the splitting field of $f(X)$ Need to check that $gcd(f, Df) = 1$ where

$$Df = 4X^3 - 4aX = 4X(X^2 - a)$$

f, Df have no common roots since $X = 0$ not a root of f and $X = \pm\sqrt{a}$ not a root of f, as $b \neq 0$

Theorem 4.1. *Assume 1 and 2 from before*

1. *Suppose bc, c are not square. Then*
$$[L : K] = 8, \quad G = \mathcal{D}_8$$
and $f(X)$ is irreducible

2. *Suppose bc square, so c not square. Then*
$$[L : K] = 4, \quad G = \mathcal{C}_4$$
and $f(X)$ is irreducible

3. *Suppose c a square, so bc is not a square. Then*
   - *either $2(\alpha+\gamma)$ and $2(\alpha-\gamma)$ are both not square in K then*
   $$[L : K] = 4, \quad G = \mathcal{C}_2 \times \mathcal{C}_2$$
   and $f(X)$ is irreducible
   - *or one of $2(\alpha+\gamma)$ or $2(\alpha-\gamma)$ is a square in K, but not the other, then*
   $$[L : K] = [K(\beta) : K] = 2, \quad G = \mathcal{C}_2$$
   and $f(X)$ is reducible

Lemma 4.2. *Let $B \in F$ and $A \in F$ be not square in F. If B is square in $F(\sqrt{A})$ then either B is square in F or AB square in F*

4.2 Finite fields

Theorem 4.3. *Fix a prime $p > 0$. Then $\forall m \in \mathbb{Z}_{\geq 1} \exists$ a unique, up to non-unique isomorphism, finite field with $q = p^m$ elements. The notation is $\mathbb{F}_q$*

$$G = Gal(\mathbb{F}_q/\mathbb{F}_p) = \mathbb{Z}/m\mathbb{Z}$$

4.3 Symmetric polynomials

Consider

$$f(X) = (X - x_1)\cdots(X - x_n) = X^n - \sigma_1 X^{n-1} + \cdots \pm \sigma_n \in K(x_1, \cdots, x_n)[X]$$

where

$$\sigma_1 = \sigma_1(x_1, \cdots, x_n) = \sum_{i \leq i \leq n} x_i, \quad \sigma_2 = \sigma_2(x_1, \cdots, x_n) = \sum_{i \leq i \leq j \leq n} x_i x_j, \quad \cdots$$

Here $\sigma_1 \in K[x_1, \ldots, x_n]$ are the **elementary symmetric polynomials**. Let

$$\delta = \prod_{\text{roots of } f} (x_i - x_j), \quad \Delta = \delta^2 = \prod_{\text{roots of } f} (x_i - x_j)^2$$

Definition 4.4. *$\sigma \in K[x_1, \ldots, x_n]$ is symmetric if and only if $\forall g \in S_n$*

$$\sigma(x_{g(1)}, \ldots, x_{g(n)}) = \sigma(x_1, \ldots, x_n)$$

Theorem 4.5. *Consider a degree n separable polynomial $f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \in k[x]$. Let $k \subset L$ be the splitting field of f. Then $G \subset \mathcal{A}_n$ if and only if Δ is a square in k*

Theorem 4.6. *Consider an irreducible cubic polynomial $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$ and $k \subset L$ be the splitting field then $G = \mathcal{S}_3$ iff Δ is not a square in k, and $G = \mathcal{A}_3 = \mathcal{C}_3$ iff Δ is square in k*

5 Irreducible polynomials

Proposition 5.1. *Suppose $f(X) = a_0 + \ldots + a_d X^d \in \mathbb{Z}[X]$ has a root $\frac{p}{q} \in \mathbb{Q}$ with $gcd(p, q) = 1$ then $[p \mid a_0]$ and $q \mid a_d$*

Lemma 5.2. *(Gauss' Lemma)*
Suppose $f(X) = a_0 + \ldots + a_d X^d \in \mathbb{Z}[X]$ for $gcd(a_0, \ldots, a_d) = 1$ factorises non-trivially in $\mathbb{Q}[X]$. Then it factors non-trivially in $\mathbb{Z}[X]$

Corollary 5.3. *if $f(X)$ is prime in $\mathbb{F}_p[X]$ for some p, then it is prime in $\mathbb{Q}[X]$*

Corollary 5.4. *(Eisenstein)*
$f(X) = a_0 + \ldots + a_d X^d \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$ if there exists p prime such that $\not| a_d$ but $p \mid a_i$ for $i < d$ and $p^2 \not| a_0$

6 Reduction modulo prime

Theorem 6.1. *Let $f(X) \in \mathbb{Z}[X]$ be monic of degree $n, \mathbb{Q} \subset K$ be the splitting field of f and $G = Gal(K/\mathbb{Q}) \subset S_n$. For p prime, denote by $\overline{f}$ as f viewed in $\mathbb{F}_p[X]$. If there exists p such that $\overline{f} \in \mathbb{F}_p[X]$ has n distinct roots ina splitting field and $\overline{f} = \prod_{i=1}^{k} \overline{f}_i(X) \in \mathbb{F}_p[X]$ with $\overline{f}_i \in \mathbb{F}_p[X]$ irreducible of degree n_i then there exists $\sigma \in G \subset \mathcal{S}_n$ of cycle decomposition type*

$$(n_1)\ldots(n_k)$$

Proposition 6.2. *Suppose that r is prime and let $G \subset \mathcal{S}_r$ be a subgroup. If G contains an r-cycle and one transposition then $G = \mathcal{S}_r$*

Definition 6.3. *The **character** of a monoid P to K is $\chi : P \to K$ such that*

- $\chi(0) = 1$, *and*
- $\chi(a+b) = \chi(a)\chi(b)$ *for all* $a, b \in P$

Theorem 6.4. *Linear independence of characters, Dedekind independence theorem*
Let K a field and P a monoid, such as $P = \mathbb{N}$. Any set of distinct non-zero characters

$$\chi_1 : P \to K, \quad \dots \quad \chi_n : P \to K, \dots$$

is linearly independent in the vector space $\{f : P \to K\}$

Theorem 6.5. *Let $f(X) \in \mathbb{Z}[X]$ be degree n monic, $\mathbb{Q} \subset K$ be the splitting field of f , $G = Gal(K/\mathbb{Q}) \subset \mathcal{S}_n$ and $\lambda_1, \dots \lambda_n \in K$ be the roots of $f(X)$. Let p be a prime. Denote by $\overline{f}$ the image f modulo p. Assume $\overline{f}$ is separable. Let $\mathbb{F}_p \subset F$ be a splitting field for $\overline{f}$, so $\overline{f}$ has n distinct roots in F . Let $R \subset K$ be the subring generated by the roots of f, so $R = \mathbb{Z}[\lambda_1, \dots, \lambda_n]$ Then*

1. *there exists a ring homomorphism $\psi : R \to F$*
2. *if $\psi' : R \to F$ a ring homomorphism then ψ' induces a bijection*

$$\phi' : \{\text{roots of } f(X) \text{ in } R\} \to \{\text{roots of } \overline{f} \text{ in } F\}$$

3. *$\psi' : R \to F$ a ring homomorphism if and only if there exists $\sigma \in G$ such that $\psi' = \psi \circ \sigma$*