Galois, Fields and Algebras

Naveensurya V
naveen24@iisertvm.ac.in

January 29, 2025

This document contains the LaTeX notes of Dr Viji Thomas, and it was LaTeXed by me, Naveensurya. It covers all the definitions and theorems mentioned in class, but the **proofs in this document may not be the same as those taught by Dr Viji**; they represent my approach to the proofs. I have added additional theory, which I studied from reference books. These theory are marked with the ‡ symbol. Some proofs are not included in these notes. For those, you can refer to standard textbooks such as Artin, Dummit and Foote, or Cambridge Notes. Any comments, doubts, or corrections are welcome.

I plan to update this document regularly on GitHub. For regular updates, please check this link.

Contents

1 First half of Galois Theory

1.1 Basic Definitions

Definition 1.1. *Let L/K be a field extension and* ***Automorphism*** *of L/K is defined as*

$$Aut(L/K) := \{\phi : L \to L|\ \phi(k) = k,\ \forall k \in K\}$$

Definition 1.2. *Let $U \subseteq Aut(L/K)$ then $\mathscr{F}(U)$ is defined as*

$$\mathscr{F}(U) := \{x \in L|\ \Psi(x) = x,\ \forall \Psi \in U\}$$

Remark 1. *In most of textbooks, authors use L^U instead of $\mathscr{F}(U)$ to denote fixed fields*

Definition 1.3. *Let $Z \subset L$ be a intermediate field between L and K then $\mathscr{G}(Z)$ is defined as*

$$\mathscr{G}(Z) := Aut(L/Z)$$

Lemma 1.1. *Let $U \subseteq Aut(L/K)$ and $Z \subset L$ be a intermediate field between L and K*

(a) $U \subseteq \mathscr{G} \circ \mathscr{F}(U) := Aut(L/\mathscr{F}(U))$

(b) $Z \subseteq \mathscr{F} \circ \mathscr{G}(Z)$

(c) $\mathscr{F}$ *is inclusion reversing. i.e,* $U_1 \subseteq U_2 \implies \mathscr{F}(U_2) \subseteq \mathscr{F}(U_1)$

(d) $\mathscr{G}$ *is inclusion reversing. i.e,* $Z_1 \subseteq Z_2 \implies \mathscr{G}(Z_2) \subseteq \mathscr{G}(Z_1)$

(e) $\mathscr{G} = \mathscr{G} \circ \mathscr{F} \circ \mathscr{G}$

(f) $\mathscr{F} = \mathscr{F} \circ \mathscr{G} \circ \mathscr{F}$

Proof.

(a) $\Psi \in U \implies \Psi(x) = x\ \forall x \in U \implies \Psi \in Aut(L/\mathscr{F}(U)) = \mathscr{G} \circ \mathscr{F}(U)$.

(b) $x \in Z \implies \Psi(x) = x\ \forall \Psi \in Aut(L/Z) \implies x \in \mathscr{F}(Aut(L/Z)) = \mathscr{F} \circ \mathscr{G}(Z)$.

(f) From (a) $U \subseteq \mathscr{G} \circ \mathscr{F}(U)$ and by (c) $\mathscr{F} \circ \mathscr{G} \circ \mathscr{F}(U) \subseteq \mathscr{F}(U)$. Replace Z from $\mathscr{F}(U)$ in (b) to obtain
$\mathscr{F}(U) \subseteq \mathscr{F} \circ \mathscr{G} \circ \mathscr{F}(U)$

$\square$

1.2 Dedekind Theorem

Theorem 1.1. ***[Dedekind's theorem on linear independence of characters.]*** *Distinct field automorphisms $\sigma_1, \dots, \sigma_n$ from $L \to L$ are linearly independent on the L-vector space of all mappings from $L \to L$*

Proof. It trivial holds for $n = 1$. let us assume it is true for $n = k$ i.e, if $\sum_{i=1}^{k} \lambda_i \sigma_i = 0 \implies \lambda_i = 0 \; \forall i$.

If $\sum_{i=1}^{k+1} \lambda_i \sigma_i = 0$. Since, σ_i's are distinct field isomorphism $\exists s \in L$ such that $\sigma_1(s) \neq \sigma_{k+1}(s)$. then by applying r we get

$$\sum_{i=1}^{k+1} \lambda_i \sigma_i(r) = 0 \tag{1}$$

and apply for rs we get

$$\sum_{i=1}^{k+1} \lambda_i \sigma_i(r) \sigma_i(s) = 0 \tag{2}$$

$\sigma_{k+1}(s) * (1) - (2) \implies$

$$\sum_{i=1}^{k} \lambda_i \sigma_i(r)(\sigma_{k+1}(s) - \sigma_i(s)) = 0 \tag{3}$$

by induction hypothesis $\lambda_1(\sigma_{k+1}(s) - \sigma_1(s)) = 0$ it implies $\lambda_1 = 0$ by induction we can claim $\lambda_i = 0 \forall i \in \{1, 2, \dots, k+1\}$

□

Definition 1.4. *Let L/K be a field extension. we can view L as vector space over K and **degree of extension** is defined as*

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

Lemma 1.2. *Suppose $[V_1 : K] = n$ and $[V_2 : K] = m$, then*

$$dim_K\big(Hom_K(V_1, V_2)\big) = mn$$

Proof. let $\{a_1, a_2, \dots, a_n\}$ and $\{b_1, b_2, \dots, b_m\}$ be basis of V_1 and V_2 w.r.t field K . Let $\sigma : V_1 \to V_2$ be a homomorphism . Let $a \in V_1$. then $\exists \lambda_i \in K$ such that

$$a = \lambda_1 a_1 + \cdots + \lambda_n a_n$$

$$\sigma(a) = \sigma(\lambda_1 a_1 + \cdots + \lambda_n a_n) = \lambda_1 \sigma(a_1) + \cdots + \lambda_2 \sigma(a_n)$$

then σ can be determined by where each basis of V_1 is mapped to V_2 . There are mn possibles values **(why?)**

□

Lemma 1.3. *Let L/K be a finite field extension. Then*

$$Aut(L/K) \leq [L : K]$$

Proof. Since every isomorphism from $L \to L$ fixes K is also a homomorphism from $L \to L$ fixes K **(why?)**

$$Aut(L/K) \leq dim_L\big(Hom_K(L, L)\big) = \frac{dim_K\big(Hom_K(L, L)\big)}{dim_K(L)} = dim_K(L)$$

□

1.3 Artin Theorem

Definition 1.5. *Let $U \subseteq Aut(L/K)$ be a finite subgroup. Then the* ***U-trace*** *of $\alpha \in L$ is defined as*

$$tr_U(\alpha) := \sum_{\sigma \in U} \sigma(\alpha)$$

Definition 1.6. ‡ *Let R be a ring. The* ***characteristic*** *of R, denoted $char(R)$, is the smallest positive integer n such that*

$$n \cdot 1_R = 0,$$

where 1_R is the multiplicative identity of R . If no such integer exists, then the characteristic of R is defined to be 0.

Theorem 1.2. ‡ *Let F be a finite field. $char(F)$ is a prime number.*

Proof. Let F be a finite field. By definition, the characteristic of a field is the smallest positive integer n such that

$$n \cdot 1_F = 0,$$

where 1_F is the multiplicative identity in F.

Assume for contradiction that $\text{char}(F) = n$ is not prime, so $n = ab$, where a and b are integers greater than 1. Then we have

$$n \cdot 1_F = (ab) \cdot 1_F = 0.$$

But this implies that the characteristic divides ab, meaning it should also divide a or b, contradicting the assumption that n is not prime. Therefore, the characteristic must be prime. □

Lemma 1.4. *$tr_U : L \to \mathscr{F}(U)$ is a K-linear map. If $char(K) \nmid |U|$, then $tr_U : L \to \mathscr{F}(U)$ is surjection.*

Proof. It is not difficult to see tr_U is K-Linear map.

If $x \in \mathscr{F}(U)$ then $\phi(x) = x \quad \forall \phi \in U$

$$tr_U(x) = \sum_{\sigma \in U} \sigma(x) = x.|U|$$

since $char(K) \nmid |U|$, $x \times |U| \neq 0$

$$tr_U\left(\frac{x}{|U|}\right) = x$$

it proves tr_U is surjection. $\square$

Lemma 1.5. *tr_U is not identitically zero.*

Proof. by Theorem 1.1 distinct automorphisms are Linearly Independent. and tr_U is just addition of distinct automorphisms its linear combination can't be 0. $\square$

Theorem 1.3. ***[Artin]*** *Let $U \subseteq Aut(L/K)$ be a finite subgroup. Then $[L : \mathscr{F}(U)] = |U|$ and $\mathscr{G} \circ \mathscr{F}(U) = U$*

Proof. Exercise. $\square$

Corollary 1. *If L/K is a finite field extension , then $\mathscr{G} \circ \mathscr{F} \equiv id$*

1.4 Galois extension

Definition 1.7. *An extension L/K is **Galois extension** if*

$$\mathscr{F} \circ \mathscr{G}(K) = K$$

Equivalently, $\mathscr{F}(Aut(L/(K))) = K$

Corollary 2. *Let $G \subseteq Aut(L)$ be a finite subgroup and let $K := \mathscr{F}(G)$. Then L/K is a galois extension and $Aut(L/K) = G$*

Proof. $\square$

Corollary 3. *Let L/K be a finite extension . Then L/K is Galois $\iff$ $|Aut(L/K)| = [L : K]$*

Example 1. $Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{id, \sigma : \sqrt{2} \mapsto -\sqrt{2}\}$

Example 2. $Aut(\mathbb{R}/\mathbb{Q}) = \{id\}$

Proof. let's begin with a claim
claim: If there exists non identity function $\sigma : \mathbb{R} \to \mathbb{R}$ such that $\sigma(q) = q \ \forall q \in \mathbb{Q}$ then σ is increasing and continuous function
proof of claim. let $p < q$ such that $p, q \in \mathbb{R}$ then

$$\sigma(q-p) = \sigma\big((\sqrt{q-p})^2\big) = \sigma^2(\sqrt{q-p}) \geq 0 \implies \sigma(p) \leq \sigma(q)$$

let $p, q \in \mathbb{R}$ such that $p < q$ $|q-p| < 1/m < \epsilon$ here we choose $m \in \mathbb{N}$ .i.e, $\frac{-1}{m} < q - p < \frac{1}{m}$

$$\implies \frac{-1}{m} = \sigma\left(\frac{-1}{m}\right) < \sigma(q) - \sigma(p) < \sigma\left(\frac{1}{m}\right) = \frac{1}{m} \text{ i.e, } |\sigma(q) - \sigma(p)| < 1/m$$

this proves the continuity of σ by choosing $\delta = \frac{1}{m} < \epsilon$ ▲

Since $\mathbb{Q}$ is dense in $\mathbb{R}$, $\forall x \in \mathbb{R} - \mathbb{Q}$ $\exists \{x_n\} \in \mathbb{Q}$ such that x_n converges to x . $\sigma(x_n) = x_n$ and σ is continuous implies $\sigma(x) = x$. □

2 Field Theory

2.1 Review from Ring Theory

Definition 2.1. *An Ideal I of Ring R is* ***maximal ideal*** *if $I \neq R$ and for any ideal $I \leq J \leq R$, either $I = J$ or $J = R$*

Definition 2.2. *An Ideal I of a Ring R is* ***prime ideal*** *if $I \neq R$ and for whenever $a, b \in R$ such that $a.b \in I$, then $a \in I$ or $b \in R$*

Definition 2.3. *$a \in R$ is* ***irreducible*** *if $a \neq 0, a$ is not a unit , and if $a = xy$, then x or y is a unit*

Theorem 2.1. *For PID*

$$\textit{Irreducible} \iff \textit{Prime} \iff \textit{Maximal}$$

Lemma 2.1. *Let R be a Integral domain containing a field F . If R is finite dimensional vector space over F then R is a field*

2.2 Kronecker Theorem

Lemma 2.2. *Let $p(x)$ $inF[x]$ be a irreducible polynomial and F be a field then $\frac{F(x)}{(p(x))}$ is field.*

Proof. Straightforward from definitions □

Theorem 2.2. ***[Kronecker]*** *let F be a field and let $F(x)$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root*

Definition 2.4. *Let F be a field and $\alpha_1, \ldots, \alpha_n$ be some elements not in F then* ***smallest field containing*** *F* ***and*** *$\alpha_1, \ldots, \alpha_n$ is defined as $F(\alpha_1, \ldots, \alpha_n)$ and we call $F(\alpha_1)$ as* ***Simple extension*** *which is field generated by adjoining one element.*

Theorem 2.3. *[**Universal Property of quotients Groups**]Let $N \trianglelefteq G$, and let $\phi : G \to H$ be a group homomorphism such that $H \subseteq \ker(\phi)$. Then there is a unique homomorphism $\phi' : G/N \to H$ such that the following diagram commutes:*

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, dashed, "\exists!\phi'"'] & \end{tikzcd}$$

Theorem 2.4. *[**Universal Property of quotients Rings**] Let $I \trianglelefteq R$ be a ideal , and let $\phi : R \to J$ be a ring homomorphism such that $I \subseteq \ker(\phi)$. Then there is a unique homomorphism $\phi' : R/I \to J$ such that the following diagram commutes:*

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\pi"'] & J \\ R/I \arrow[ur, dashed, "\exists!\phi'"'] & \end{tikzcd}$$

Remark 2. *The above theorem also holds for Vector spaces*

Theorem 2.5. *Let F be a Field and $p(x) \in F[x]$. Let α be a root of $p(x)$ in some extension $K \supseteq F$. Then*

$$F(\alpha) \cong \frac{F[x]}{(p(x))}$$

.

Proof. By Kronecker's theorem we know $\frac{F[x]}{(p(x))}$ exists and it is a field which contains both F and element α . If we prove $\frac{F[x]}{(p(x))}$ is the smallest field which contains F and element α we are done.

□

Theorem 2.6. *let $\phi : F \to F'$ be a isomorphism and α be a root of $p(x) \in F[x]$ be a irreducible polynomial. β be a root of $p'(x) := \phi(p(x))$. Then the isomorphism ϕ extends to an isomorphism $\psi : F(\alpha) \to F'(\beta)$. i.e, $\psi|_F : F \to F'$ is the isomorphism ϕ*
(Refer - Dummit and Foote p.no - 541)

Proof. Hint.

$$\begin{tikzcd}
F(\alpha) \arrow[r, dashed, "\psi"] & F'(\beta) \\
\frac{F[x]}{(p(x))} \arrow[u, "\cong"] \arrow[r, "\tilde{\phi}"] & \frac{F'[x]}{(p'(x))} \arrow[u, "\cong"] \\
F[x] \arrow[u] \arrow[r, "\phi'"] & F'[x] \arrow[u] \\
F \arrow[u, hook] \arrow[r, "\phi"] & F' \arrow[u, hook]
\end{tikzcd}$$

□

2.3 Algebraic Extension

Definition 2.5. *Let L/K be Field extension. $\alpha \in L$ is said to be* ***algebraic over*** *K if there exists a polynomial $f(x) \in K[x]$ with $f(\alpha) = 0$. If α is not algebraic then it is* ***transcendental***

Definition 2.6. *Let L/K is said to be* ***algebraic extension*** *if for all $\alpha \in L$ is algebraic over K*

Lemma 2.3. *Let α be algebraic over K. Then there exists unique monic irreducible polynomial $m_{\alpha,K}(x) \in K[x]$ that has α as a root. If $f(x) \in K[x]$ has α as a root then $m_{\alpha,K}(x)$ divides $f(x)$ in $K[x]$*

Definition 2.7. *Let α be algebraic over K.* ***Minimal polynomial*** *of α over K is defined as monic irreducible polynomial $m_{\alpha,K}(x) \in K[x]$ that has α as a root.*

Lemma 2.4. *Let L/F be a field extension and $\alpha \in L$ is algebraic over $F \iff [F(\alpha) : F] < \infty$*

Lemma 2.5. ***[Tower Law]*** *let $F \subseteq K \subseteq L$ be field extension then*

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

Proof. If some extension is infinite there is nothing to show. Lets assume everything is finite extensions. $[L : K] := m$ and $[K : F] := n$ and choose basis $\{a_1, \ldots, a_n\}$ of L over K similarly basis of K over F is $\{b_1, \ldots, b_m\}$. Then $\{a_i.b_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ forms basis of L over F **(why?)**. this proves $[L : F] = mn$ $\square$

Lemma 2.6. *Let L/K be finite extension, Then it is algebraic*

Theorem 2.7. *An extension L/K is finite $\iff \exists \alpha_1, \ldots, \alpha_n \in L$ such that α_i is algebraic over K and $L = K(\alpha_1, \ldots, \alpha_n)$*

Corollary 4. *L/K is a Field extension. $\alpha, \beta \in L$ are algebraic over K. Then $\alpha \pm \beta, \frac{\alpha}{\beta}$ and $\alpha * \beta$ are also algebraic over K*

Corollary 5. *Let L/K be a field extension .The set of all elements of L that are algebraic over K forms a subfield of L which contains K*

Theorem 2.8. *$F \subseteq K \subseteq L$ are field extension , suppose L/K and K/F are algebraic, L/F is algebraic.*

2.4 Splitting Fields

Definition 2.8. *If K/F is an field extension and $f(x) \in F[x]$. f is said to be* ***split over*** *K if*

$$f(x) = \lambda \prod_{i=1}^{n} (x - \alpha_i),\ \alpha_i \in K \text{ and } \lambda \in F$$

Definition 2.9. *K is called the* ***splitting field*** *of $f(x) \in F[x]$ if it satisfies the following conditions*

(i) $f(x)$ splits over K

(ii) K is the smallest field in which $f(x)$ splits

Theorem 2.9. ***[Existence of Splitting field]***
Let $f(x) \in F[x]$ with $deg(f(x)) = n$. There is an extension field K of F where $f(x)$ has a root and with $[K : F] \leq n$ Furthermore, there exists an extension field L/K with $[L : F] \leq n!$ where $f(x)$ splits over L

Theorem 2.10. *‡* ***[Uniqueness of Splitting Fields]*** *Let F be a field, and let $f(x)$ be a polynomial in $F[x]$. Suppose that E_1 and E_2 are two splitting fields of $f(x)$ over F. Then, E_1 and E_2 are isomorphic as fields over F.*

Theorem 2.11. ***[Isomorphism Extension]*** *Let $\sigma : K \to K'$ be an isomorphism of fields. Let L be a splitting field of $f(x) \in K[x]$ and L' be a splitting field of $\sigma(f(x)) \in K'[x]$. Then $[L : K] = [L' : K']$ and the number of extensions $\tilde{\sigma} : L \to L'$ is at most $[L : K]$*

Proof. (Proof is same as what is taught in class.)
The proof proceeds by induction on $n = [L : K]$.

Base case:
If $n = 1$, then $L = K$ and $f(x)$ splits over $K[x]$ and hence $\sigma(f(x))$ splits over $K'[x]$.
$\therefore [L : K] = [L' : K']$ and these is at most 1 extension of σ to $\tilde{\sigma} : L \to L'$

Assumption:
We will assume $n = [L : K] > 1$. Since L is the splitting field of $f(x)$ over K, L is generated by *adjoining* roots of $f(x)$ over K to field K. Since $[L : K] > 1$, $\exists$ a root α of $f(x)$ in L but not in K. We will fix this root for the rest of proof.

Induction step:
let $m(x) \in K[x]$ be the minimal polynomial of α over K.
The candidates of $\tilde{\alpha}$ come from the root of $\tilde{\sigma}(m) = \sigma(m)$.

Now we will show that $m)x)$ has a root in L'.

$$m(x)|f(x) \implies (\sigma m)(x)|(\sigma f)(x)$$

Since $m(x)$ is monic and irreducible, $(\sigma m)(x)$ is monic and irreducible in $K'[x]$.

Since $f(x)$ splits $L[x]$, $m(x)$ splits in $L[x]$.
$\therefore$ $(\sigma m)(x)$ splits in $L'[x]$ and has all roots in $L'[x]$. choose a root β of $(\sigma m)(x)$ in L' set $d := deg(m(x)) = deg((\sigma m)(x))$

$$\begin{tikzcd}
L \arrow[rr, "\tilde{\phi}"] & & L' \\
K(\alpha) \arrow[u, hook] \arrow[rr, dashed, "\exists!\ \phi'"] & & K'(\beta) \arrow[u, hook] \\
K \arrow[u, hook] \arrow[rr, "\sigma"] & & K' \arrow[u, hook]
\end{tikzcd}$$

Since L is the splitting foeld of $f(x)$ over $K[x]$, L is also the splitting field of $f(x)$ over $k(\alpha)[x]$.
Similarly L' is the splitting field of σF over $K'[x]$. Hence L' is also the splitting field of σF over $K(\beta)[x]$.

$$\text{Note that. } [L : K(\alpha)] = \frac{[L : K]}{d} < [L : K]$$

By induction

$$[L : K] = [L : K(\alpha)][k(\alpha) : K] = [L' : K'(\beta)][K'(\beta) : K'] = [L' : K']$$

It remains to show that σ has at most $[L : K]$ extensions to an Isomorphism $L \to L'$.
First we show that every isomorphism $\tilde{\sigma} : L \to L'$ extending σ arises as the extension of some intermediate field isomorphism σ' from $K(\alpha)$ to a subfield of L'.

we already know that $\tilde{\sigma}(\alpha)$ has to be a root of σm set $\beta = \tilde{\sigma}(\alpha)$.
Since, $\tilde{\sigma}|_K = \sigma$, the restriction of σ of $K(\alpha)$ is the field morphism that us σ on K that sends α to β,

$$\tilde{\sigma}|_{K(\alpha)} : K(\alpha) \to K' \text{ and } \tilde{\sigma} : \alpha \mapsto \beta$$

Therefore $\tilde{\sigma}$ on L is a lift of the intermediate isomorphism $\sigma' := \tilde{\sigma}|_{K(\alpha)}$ By the induction on degrees of splitting field , σ' lifts to at most $[L : K(\alpha)]$ isomorphism $\tilde{\sigma} : L \to L'$.

Since σ' is determined by $\sigma'(\alpha)$, which is a root of $(\sigma m)(x)$, these are at most $d := deg((\sigma m)(x))$ choices for $\sigma'(\alpha)$.

The no. of isomorphism $L \to L'$ which lifts σ is the no. of maps σ' coming out of $K(\alpha)$ times the no. of extensions of each σ' to an isomorphism $L \to L'$ and this is at most $[L : K(\alpha)]$

$\therefore$ in total it is at most $d * [L : K(\alpha)] = [L : K]$ □