Notes on Galois Theory : 200cc

Ken Lee

Spring 2020

Contents

1 Field Extensions and the Essence of Galois Theory

Definition – Field Morphisms, Isomorphisms, Automorphisms

A *field morphism* $\iota : K \to L$ between fields is just a ring morphism, that is, a function satisfying the following :

1. (Additive) $\forall\, x, y \in K, \iota(x+y) = \iota(x) + \iota(y)$.
2. (Multiplicative) $\forall\, x, y \in K, \iota(xy) = \iota(x)\iota(y)$.
3. (Preserves One) $\iota(1) = 1$.

A bijective field morphism is called an *isomorphism*. In particular, isomorphisms of a field to itself are called *automorphisms*. We denote the set of all field automorphisms of a field L with $\mathrm{Aut}\, L$.

Theorem – Fields Embed into other Fields

Let $\iota : K \to L$ be a morphism of fields.

Then ι is injective. In particular, ι is a field isomorphism from K to its image.

Proof. Injectivity of ι is equivalent to $\iota^{-1}(0) = \{0\}$. Let $x \in \iota^{-1}(0)$. If it is non-zero, then there exists $y \in K$ such that $xy = 1$. Then $1 = \iota(1) = \iota(x)\iota(y) = 0$ which is a contradiction, since L is non-trivial. $\square$

Definition – Extensions of a Field, Extension Embeddings, Isomorphisms, Automorphisms

Let K be a field. Then a *K-extension* is a pair (L, ι_L) where L is a field and $\iota_L : K \to L$ is a field morphism. We say *L extends K*.

A *K-embedding* between two K-extensions $(L, \iota_L), (N, \iota_N)$ is a field morphism $\iota : L \to N$ such that $\iota \circ \iota_L = \iota_N$. We say K is *preserved* in such a map. If a K-embedding is bijective, it is called a *K-isomorphism*. In particular, K-isomorphisms from a K-extension to itself are called *K-automorphisms*.

The set of K-embeddings between $(L, \iota_L), (N, \iota_N)$ is denoted with $\mathrm{Emb}_K(\iota_L, \iota_N)$. If the field morphisms ι_L, ι_N are clear, we write $\mathrm{Emb}_K(L, N)$. In a similar manner, we denote the set of K-automorphisms of (L, ι_L) with $\mathrm{Aut}_K(\iota_L)$, or simply $\mathrm{Aut}_K L$ when ι_L is clear.

Definition – Fixed Subfields, Galois Extensions

Let L be a field. Then $\mathrm{Aut}\, L$ forms a group under function composition. Let G be a finite subgroup of $\mathrm{Aut}\, L$. We say *G acts on L*.

Then the *subfield fixed by G*, denoted L^G, is the field of elements in $a \in L$ such that for all $\sigma \in G$, $\sigma(a) = a$. Its inclusion into L is a field morphism, making L into an L^G-extension.

Let K be a field with (L, ι_L) as a K-extension. Then (L, ι_L) is called a *Galois* when $\iota_L K = L^G$ for some finite subgroup $G \subseteq \mathrm{Aut}\, L$. In this case, G is called a *Galois group of* (L, ι_L).

Definition – Antitone Galois Connection

Let $(I, \leq), (J, \leq)$ be partially ordered sets. Then an *antitone Galois connection between I and J* is a pair of maps $F : I \to J$ and $G : J \to I$ such that

1. (Antitonicity) For all $i_0 \leq i_1 \in I$ and $j_0 \leq j_1 \in J$, we have $F(i_1) \leq F(i_0)$ and $G(j_1) \leq G(j_0)$.
2. (Adjunction) For all $i \in I, j \in J$, we have $i \leq G(j) \Leftrightarrow j \leq F(i)$.

Theorem – Antitone Galois Connections gives Bijection on Images

Let $(I, \leq), (J, \leq)$ be partially ordered sets and $F : I \to J, G : J \to I$ an antitone Galois connection.

Then $G \circ F \circ G = G$ and $F \circ G \circ F = F$, that is to say $F : G(J) \to F(I)$ and $G : F(I) \to G(J)$ are bijections.

Proof. Straight forward. □

Corollary – The Antitone Galois Connection of Galois Theory

Let (L, ι_L) be a K-extension. Let I be the set of fields inside L containing $\iota_L K$, i.e. the set of K-extensions inside L. This is partially ordered by inclusion. Let J be the set of subgroups of the group of K-automorphisms of L, $\mathrm{Aut}_K L$. This is also partially ordered by inclusion.

Then the maps

$$\begin{aligned} \mathrm{Aut}_{-} L : I &\longrightarrow J & L^{-} : J &\longrightarrow I \\ E &\mapsto \mathrm{Aut}_E L & H &\mapsto L^H \end{aligned}$$

form an antitone Galois connection and are bijective on their images.

Theorem – Fundamental Theorem of Galois Theory

Let (L, ι_L) be a K-extension, I the partially ordered set of K-extensions inside L, and J the partially ordered set of subgroups of $\mathrm{Aut}_K L$. Let (L, ι_L) be Galois.

Then $\mathrm{Aut}_{-} L : I \to J$ and $L^{-} : J \to I$ are surjections.

Remark. The full fundamental theorem has more subtleties, but the essence of Galois theory is to characterise Galois extensions in order to exploit the bijection between subextensions and subgroups.

2 Finite Extensions and the Embedding Theorem

Definition – Extension Degree, Finite Extensions

Let (L, ι_L) be a K-extension. Then L has a natural K-vectorspace structure with scalar multiplication as $kl := \iota_L(k)l$ for $k \in K, l \in L$.

The *degree of* (L, ι_L) is the dimension of L as a K-vectorspace. We shall denote it with $[\iota_L : K]$. If the embedding of K into L is clear, then we write $[L : K]$. We the degree of (L, ι_L) is finite, we call (L, ι_L) a *finite* extension.

Theorem – Tower Law of Extension Degree

Let (L, ι_L) be a K-extension and (N, ι_N) a L-extension. $(N, \iota_N \circ \iota_L)$ is then a K-extension.

Then $[\iota_N \circ \iota_L : K] = [\iota_N : L][\iota_L : K]$.

Proof. Let $B_L \subseteq L$ be a ι_L-basis and $B_N \subseteq N$ a ι_N-basis. The claim is that $B_L B_N := \{ab \mid a \in B_L, b \in B_N\}$ is a $(\iota_N \circ \iota_L)$-basis of N and has cardinality $B_L \times B_N$.

(Cardinality) Let $(a_1, b_1), (a_2, b_2) \in B_L \times B_N$ such that $a_1 b_1 = a_2 b_2$. This is then a non-trivial L-linear combination of elements in B_N, contradicting linear independence of B_N. The cardinality is thus as desired.

(Linear Independence) Let $\sum_{(a,b) \in B_L \times B_N} \lambda_{a,b} ab = 0$ where $\lambda_{a,b} \in K$ and only finitely many are non-zero. Then we have $\sum_{b \in B_N} \left(\sum_{a \in B_L} \lambda_{a,b} a \right) b = 0$, giving $\sum_{a \in B_L} \lambda_{a,b} a = 0$ by linear independence of B_N, which in turn gives $\lambda_{a,b} = 0$ by linear independence of B_L.

(Spanning) Let $x \in N$. Since B_N is spanning, we have $\sum_{b \in B_N} \lambda_b b = x$ for some $\lambda_b \in L$, finitely many non-zero. Then since B_L is spanning, we have $\sum_{a \in B_L} \mu_{a,b} a = \lambda_b$ for each $b \in N_B$, where $\mu_{a,b} \in K$, finitely many non-zero. So $\sum_{(a,b) \in B_L \times B_N} \mu_{a,b} ab = x$ as desired. $\square$

Definition – Extension generated by a Subset, Evaluation Map, Algebraic Extension

Let (L, ι_L) be a K-extension and $A \subseteq L$. Then the *K-subextension generated by A* is defined as the intersection of all fields in L that contain $\iota_L K \cup A$. This is denoted with $K(A)$. If $A = \{a_1, \ldots, a_{|A|}\}$ is finite, then we just write $K(a_1, \ldots, a_{|A|})$. When $L = K(A)$, elements of A are referred to as *generators*. (L, ι_L) is called *finitely generated* when there exists finite $A \subseteq L$ such that $L = K(A)$.

Let $K[X], L[X]$ be the polynomial rings over K and L. Then ι_L induces a ring morphism $K[X] \to L[X]$ via $\sum_n f_n X^n \mapsto \sum_n \iota_L(f_n) X^n$. We will denote this map using ι_L as well. We can thus evaluate polynomials over K at an element $a \in L$ by the *evaluation map* $ev_a^{\iota_L} : f \mapsto ev_a(\iota_L f)$.

For $a \in L$, $ev_a^{\iota_L}$ is a ring morphism from $K[X]$ to L. Then for f in the kernel of $ev_a^{\iota_L}$, we say *a is a root of f*. If the kernel of $ev_a^{\iota_L}$ contains non-zero polynomials, then we say a is *algebraic over K*. When all elements of L are algebraic over K, (L, ι_L) is called an *algebraic extension*.

Lemma – Characterisation of Finite Simple Extensions

Let (L, ι_L) be a K-extension and $a \in L$. Then the following are equivalent :

1. $(K(a), \iota_L)$ is finite.
2. $(K(a), \iota_L)$ is algebraic.
3. a algebraic over K.

Proof. $(2 \Rightarrow 3)$ clear.

$(3 \Rightarrow 1)$ This follows from showing $K(a) = ev_a^{\iota_L} K[X]$. $K[X]$ is a PID so the kernel of ev_a is generated by one element, call it $\min(a, \iota_L)$. Since the image of $ev_a^{\iota_L}$ is a ring inside L which is an integral domain, it follows that $\min(a, \iota_L)$ is prime. Then since $K[X]$ is a PID, primes are irreducible and quotienting by irreducibles give a field, so $ev_a^{\iota_L} K[X]$ is a field. It is clear that $ev_a K[X] \subseteq K(a)$ and hence it equal to it.

$(1 \Rightarrow 3)$ If $K(a)$ is a finite dimensional K-vectorspace, then the set $\{a^n\}_{n \in \mathbb{N}}$ must be linearly dependent. This gives a polynomial $f \in K[X]$ such that $ev_a f = 0$.

$(1 \Rightarrow 2)$ Let $b \in K(a)$. Then by the Tower Law, $[K(b) : K] \leq [K(a) : K]$, which is finite. So by $(1 \Rightarrow 3)$, b is algebraic over K. □

Theorem – Characterisation of Finite Extensions

Let (L, ι_L) be a K-extension. Then the following are equivalent :

1. (L, ι_L) is finite.
2. (L, ι_L) is finitely generated and algebraic.
3. (L, ι_L) is finitely generated and the generators are algebraic over K.

Proof. $(1 \Rightarrow 2)$ Let $A \subseteq L$ be a finite K-basis of L. Then $L = K(A)$ and all elements of L are algebraic by the characterisation of finite simple extensions.

$(2 \Rightarrow 3)$ clear.

($3 \Leftarrow 1$) Let A finite $\subseteq L$ such that $L = K(A)$ and all $a \in A$ are algebraic over K. If A is empty, $[L : K] = 1$. So let $a \in A$. Then by induction on the cardinality of A, $(K(A \setminus \{a\}), \iota_L)$ is a finite K-extension. Since a is algebraic over K, it is certainly algebraic over $K(A \setminus \{a\})$. So by the characterisation of finite simple extensions, $L = K(A \setminus \{a\})(a)$ is a finite $K(A \setminus \{a\})$-extension. Thus by the Tower Law, $[L : K] = [L : K(A \setminus \{a\})][K(A \setminus \{a\}) : K]$ is finite. □

Definition – Minimal Polynomial, Galois Conjugates

Let (L, ι_L) be a K-extension and $a \in L$ algebraic over K. We have seen that $\ker ev_a^{\iota_L}$ is generated by one element. It is the one of minimal degree, unique up to units. There is however a unique monic one. It is defined as the *minimal polynomial of a over K*, denoted $\min(a, \iota_L)$. If the embedding of K into L is clear, we write $\min(a, K)$.

Let (M, ι_M) be another K-extensions and $\alpha \in M$ also algebraic over K. Then a, α are called *Galois K-conjugates* when $\min(a, K) = \min(\alpha, K)$. It is not hard to check that being Galois K-conjugates is an equivalence relation the "set of elements in all K-extensions". [a]

[a] In case Bertrand Russell rises from his grave.

Lemma – Embedding Theorem for Finite Simple Extensions

Let (L, ι_L) be K-extensions and $a \in L$ algebraic over K.

Then for all K-extensions (N, ι_N), the set of Galois K-conjugates of a inside N bijects with $\mathrm{Emb}_K(K(a), N)$. In particular, $|\mathrm{Emb}_K(K(a), N)| \leq \deg \min(a, K) = [K(a) : K]$.

Proof. Let (N, ι_N) be a K-extension. Given a K-embedding $\phi : (K(a), \iota_L) \to (N, \iota_N)$, we have

$$ev_{\phi(a)}^{\iota_N}(\min(a, K)) = ev_{\phi(a)}^{\phi \circ \iota_L}(\min(a, K)) = \phi\left(ev_a^{\iota_L} \min(a, K)\right) = \phi(0) = 0$$

i.e. $\min(a, K)$ has $\phi(a)$ as a root. This shows $\phi(a)$ is not only algebraic, but $\min(\phi(a), K)$ divides $\min(a, K)$ as well. $\min(a, K)$ is irreducible, so $\min(\phi(a), K) = \min(a, K)$. Thus we have a map from $\mathrm{Emb}_K(K(a), N)$ to the set of Galois K-conjugates of a in N by $\phi \mapsto \phi(a)$. Since $K(a)$ is generated by a, the above map is injective.

Now let $\alpha \in N$ be a Galois K-conjugate of a. Then we have a chain of K-isomorphisms

$$K(a) \cong K[X]/(\min(a, K)) = K[X]/(\min(\alpha, K)) \cong K(\alpha)$$

which gives a K-embedding of $\phi_\alpha : (K(a), \iota_L) \to (N, \iota_N)$. Then $\phi_\alpha(a) = \alpha$ so our map is bijective. □

Lemma – Subextensions Partition Embeddings

Let (L, ι_L) an K-extension and E a field inside L containing $\iota_L K$. So (E, ι_L) is a K-extension and L is a E-extension. Let (N, ι_N) be another K-extension.

Then we have the following bijection

$$\mathrm{Emb}_K(L, N) \longleftrightarrow \bigsqcup_{\iota \in \mathrm{Emb}_K(E, N)} \mathrm{Emb}_E(L, \iota)$$

by sending $\iota_0 \mapsto (\iota_0, \iota_0)$ and inversely $(\iota, \iota_1) \mapsto \iota_1$. In particular when all these extensions are finite, we obtain : $|\mathrm{Emb}_K(L, N)| = \sum_{\iota \in \mathrm{Emb}_K(E,N)} |\mathrm{Emb}_E(L, \iota)|$.

Proof. Let $\iota_0 : L \to N$ be a K-embedding. Then ι_0 is naturally a K-embedding of E to N and it is also an E-embedding of L to (N, ι_0). Conversely, let $\iota : (E, \iota_L) \to (N, \iota_N)$ be a K-embedding and $\iota_1 : L \to (N, \iota)$ be a E-embedding. Then since $\iota_1 \circ \iota_L = \iota \circ \iota_L = \iota_N$, ι_1 is a K-embedding of L to N. Thus the forward and inverse maps are well-defined. They are clearly inverses over each other so we have the result. □

Remark. Despite its simplicity, the above lemma is *essential* for proofs inducting on the degree of extensions.

Theorem – Embedding Theorem for Finite Extensions

Let (L, ι_L) be a finite K-extension. Then by the characterisation of finite extensions, we have a finite $A \subseteq L$ such that $L = K(A)$ and all $a \in A$ are algebraic over K. Let (N, ι_N) be another K-extension, and suppose for all $a \in A$, $\min(a, K)$ has all its roots in N, that is to say $\iota_N \min(a, K)$ factorises into linear polynomials in $N[X]$.

Then $0 < |\mathrm{Emb}_K(L, N)| \leq [L : K]$ and is equal when for all $a \in A$, $\min(a, K)$ has *no repeated* roots in N, i.e. $\iota_N \min(a, K)$ has no repeated factors in $N[X]$.

Proof. If A is empty, then the theorem is true. So let $a \in A$ and let $E = K(A \setminus \{a\})$. Then by induction on the cardinality of A, $0 < |\mathrm{Emb}_K(E, N)| \leq [E : K]$ and is equal when for all $a_1 \in A \setminus \{a\}$, $\iota_N \min(a_1, K)$ has no repeated roots. Let $\iota \in \mathrm{Emb}_K(E, N)$. Now $L = E(a)$. Since a is a root of $\min(a, K)$, it is a root of $\iota_L \min(a, K)$, so $\min(a, E)$ divides $\iota_L \min(a, K)$. Then since $\min(a, K)$ has all its roots in N, $\min(a, E)$ also has all its roots in N. So by the characterisation of finite simple extensions, gives

$$0 < |\mathrm{Emb}_E(L, \iota)| \leq \sum_{\iota \in \mathrm{Emb}_K(E,N)} |\mathrm{Emb}_E(L, \iota)| = |\mathrm{Emb}_K(L, N)|$$

To complete the induction, now suppose for all $a \in A$, $\min(a, K)$ has no repeated roots in N. Then by induction, $|\mathrm{Emb}_K(E, N)| = [E : K]$. Furthermore, by the embedding theorem for finite simple extensions, for all $\iota \in \mathrm{Emb}_K(E, N)$, $\mathrm{Emb}_E(L, \iota)$ bijects with the set of Galois E-conjugates of a in (N, ι). But since $\iota_N \min(a, K)$ has no repeated factors neither does $\iota \min(a, E)$, so it follows that the number of Galois E-conjugates of a in (N, ι) equals the degree of $\min(a, E)$, which is equal to $[E(a) : E] = [L : E]$. Thus the induction is complete by the tower law

$$|\mathrm{Emb}_K(L, N)| = \sum_{\iota \in \mathrm{Emb}_K(E,N)} |\mathrm{Emb}_E(L, \iota)| = |\mathrm{Emb}_K(E, N)|[L : E] = [E : K][L : E] = [L : K]$$

□

3 Normal Extensions

Definition – Normal Extension

Let (L, ι_L) be a K-extension and $f \in K[X]$. Then we say ι_L *splits* f when $\iota_L f$ factorises into linear factors in $L[X]$. If the embedding of K into L is clear, we just say L splits f.

Suppose (L, ι_L) is algebraic. Then it is called *normal* when for all $a \in L$, it contains all the Galois

K-conjugates of a, i.e. L splits $\min(a, K)$.

Theorem – Splitting Polynomials
Let K be a field and $f \in K[X] \setminus K$. Then there exists a K-extension (L, ι_L) such that f has a root in L. In particular, there exists a K-extension that splits f.

Proof. Since f is non-constant and $K[X]$ is a UFD, there exists an irreducible f_1 that divides f. Let $L = K[X]/(f_1)$. Then since f_1 is irreducible and $K[X]$ is a PID, L is a field and thus a K-extension. Note that the image of the monomial X in L is a root of f_1, and hence a root of f. To split f, use the above procedure to inductively construct a desired extension. $\square$

Theorem – Characterisation of Finite Normal Extensions
Let (L, ι_L) be a finite K-extension. Then the following are equivalent :

1. (Contains all Galois K-Conjugates) (L, ι_L) normal.
2. (Contains all Galois K-Conjugates of Generators) There exists $A \subseteq L$ a finite set of generators of (L, ι_L) such that for all $a \in A$, a is algebraic over K and L splits $\min(a, K)$.
3. (is a Splitting Field) There exists a polynomial $f \in K[X]$ such that L splits f and is generated by the roots of f in L.
4. (Image Invariance) For all K-extensions (N, ι_N) and two $\iota_0, \iota_1 \in \mathrm{Emb}_K(L, N)$, $\iota_0 L = \iota_1 L$.

Proof. $(1 \Rightarrow 2 \Rightarrow 3)$ is clear.

$(3 \Rightarrow 4)$ The key is that roots of f remain roots of f under K-extension morphisms.

Let $\iota_L f(X) = \prod_{k=1}^{\deg f} (X - a_k)$ where $a_k \in L$. Then $(\iota_0 \circ \iota_L) f(X) = \prod_{k=1}^{\deg f} (X - \iota_0(a_k))$. Since $\iota_0 \circ \iota_L = \iota_1 \circ \iota_L$, we have for every a_l that

$$0 = \iota_1(ev_{a_l}^{\iota_L} f) = ev_{\iota_1(a_l)}^{\iota_1 \circ \iota_L} f = ev_{\iota_1(a_l)}^{\iota_0 \circ \iota_L} f = \prod_{k=1}^{\deg f} (\iota_1(a_l) - \iota_0(a_k))$$

Hence for all a_l, there exists a_k such that $\iota_1(a_l) = \iota_0(a_k)$. Since $L = K(a_1, \ldots, a_{\deg f})$, this shows that $\iota_1 L \subseteq \iota_0 L$. By symmetrical argument, $\iota_0 L \subseteq \iota_1 L$ as well.

$(4 \Rightarrow 1)$ Let $a \in L$. Since (L, ι_L) is finite, $\min(a, K)$ exists. We do not know if L splits $\min(a, K)$, but there exists an L-extension (M, ι_M) such that M splits $\min(a, K)$. We seek to show that all Galois K-conjugates of a in M are in $\iota_M L$. So let $\alpha \in M$ be a Galois K-conjugate of a. We have the following situation.

$$\begin{tikzcd} K \arrow[r, "\iota_L"] & K(a) \arrow[r, "\subseteq"] \arrow[dr, "\phi_\alpha"'] & L \arrow[d, "\iota_M"] \\ & & M \end{tikzcd}$$

By the embedding theorem for finite simple extensions, there exists $\phi_\alpha \in \mathrm{Emb}_K(K(a), M)$ that maps $a \mapsto \alpha$. Suppose we have an $\iota_1 \in \mathrm{Emb}_{K(a)}(L, \phi_\alpha)$. Then certainly $\iota_1 \in \mathrm{Emb}_K(L, \iota_M \circ \iota_L)$. Also, trivially $\iota_M \in \mathrm{Emb}_K(L, \iota_M \circ \iota_L)$. So $\iota_1 L = \iota_M L$ implies $\alpha \in \iota_M L$ as desired. It thus suffices to give an $\iota_1 \in \mathrm{Emb}_{K(a)}(L, \phi_\alpha)$. Well, since (L, ι_L) is finite, it is also a finite $K(a)$-extension, so it is generated by some finite subset B whose elements are all algebraic over $K(a)$. Then we can extend M so that it splits all $\min(b, K(a))$ for $b \in B$. Thus by the embedding theorem, we have an $\iota_1 \in \mathrm{Emb}_{K(a)}(L, \phi_\alpha)$. □

4 Separable Extensions

> **Definition – Characteristic of a Field**
>
> Let K be a field. $\mathbb{Z}$ is generated by 1 and ring morphisms must preserve 1, so there is a unique ring morphism $\mathbb{Z} \to K$. Its image is an ID since K is an ID. So by $\mathbb{Z}$ PID, its kernel is generated by either zero or a (positive) prime. This is defined as the *characteristic of K*, denoted $\mathrm{Char}K$.

Remark – Freshmen's Dream. If $\mathrm{Char}K = 0$, then K is naturally a $\mathbb{Q}$-extension. On the other hand, if $\mathrm{Char}K = p > 0$, then K is naturally a $\mathbb{Z}/(p)$-extension.

In the latter case, by the binomial theorem, we have for all $a, b \in K$, $(a+b)^p = a^p + b^p$. This innocent-looking result is known as *Freshmen's Dream*, and turns out to be very useful.

> **Definition – Formal Derivative, Separable Polynomial**
>
> Let K be a field and $f = \sum_{0 \leq n} f_n X^n \in K[X]$. Then the *formal derivative of f* is defined to be $f' = \sum_{0<n} n f_n X^{n-1}$.
>
> f is said to be *separable* when for all K-extensions in which f splits, f has no repeated roots. If otherwise, f is called *inseparable*.

> **Theorem – Characterisation of Inseparable Irreducible Polynomials**
>
> Let K be a field and $f \in K[X]$ irreducible. Then the following are equivalent :
>
> 1. (Repeated Root) f is inseparable.
> 2. (Intrinsic Definition) $(f, f') \neq 1$.
> 3. (Another Intrinsic Definition) $f' = 0$.
> 4. (Characteristic Non-zero) $\mathrm{Char}K = p \neq 0$ and there exists an irreducible separable $g \in K[X]$ with $n > 0$ such that $f(X) = g(X^{p^n})$.
> 5. (All Roots Repeated) There exists a K-extension in which f splits and all its roots are repeated.

Proof. $(1 \Rightarrow 2)$ Let (L, ι_L) be a K-extension in which f splits and has repeated roots. Then by the product rule (which is straightforwardly proven by induction), $(\iota_L f, (\iota_L f)') \neq 1$. If $(f, f') = 1$, then there exists polynomials g, h such that $gf + hf' = 1$, which implies $\iota_L(g)\iota_L(f) + \iota_L(h)\iota_L(f') = \iota_L(g)\iota_L(f) + \iota_L(h)(\iota_L f)' = 1$, which contradicts with $(\iota_L f, (\iota_L f)') \neq 1$.

($2 \Rightarrow 3$) Since f is irreducible and $K[X]$ is PID, either f divides f' or $(f, f') = 1$. By assumption, we must have the first case. But then if $f' \neq 0$, its degree would be well-defined, and hence we would have $\deg f' < \deg f \leq \deg f'$, which is a contradiction. So $f' = 0$.

($3 \Rightarrow 4$) Let $f = \sum_{0 \leq k \leq \deg f} f_k X^k$. Since $f' = 0$, we have its leading coefficient $(\deg f)(f_{\deg f}) = 0$, which implies $\deg f = 0 \in K$. This shows that the kernel of the unique ring morphism $\mathbb{Z} \to K$ is non-trivial, and hence $\mathrm{Char} K = p \neq 0$ for some prime $p \in \mathbb{Z}$. Then for all non-zero coefficients f_k of f, we have $k f_k = 0$, which implies $k = 0 \in K$, Thus $k \in \mathbb{Z}$ is in the kernel of $\mathbb{Z} \to K$, and hence $k = k_p p$ for some $k_p \in \mathbb{Z}_{>0}$. Letting $g_1(X) = \sum_{0 \leq k \leq \deg f} f_k X^{k_p}$, we obtain $f(X) = g_1(X^p)$. Irreducibility of f implies irreducibility of g_1. So if g_1 is separable, we are done. And if not, then by ($1 \Rightarrow 3$) we have g_1 satisfying (3). Since $\deg g_1 < \deg f$, by induction there exists a irreducible separable polynomial $g \in K[X]$ with $n > 0$ such that $g_1(X) = g(X^{p^n})$, in which case we are also done.

($4 \Rightarrow 5$) Let $f(X) = g(X^{p^n})$ where $g \in K[X]$ is irreducible and separable, and $n > 0$. Then there exists a K-extension (L, ι_L) such that L splits g. Let $A \subseteq L$ be the set of roots of g. Then $\iota_L f = \prod_{a \in A}(X^{p^n} - a)$. Now, there exists a L-extension (M, ι_M) so that M splits all the $X^{p^n} - a$. For $a \in A$, let $t_a \in M$ such that $(t_a)^{p^n} - \iota_M(a) = 0$. Then by Freshmen's dream, we are done.

$$(\iota_M \circ \iota_L) f = \prod_{a \in A}(X^{p^n} - \iota_M(a)) = \prod_{a \in A}(X - t_a)^{p^n}$$

($5 \Rightarrow 1$) clear. $\square$

Definition – Separable Closure, Separable Extension, Purely Inseparable

Let (L, ι_L) be an algebraic K-extension. Then the *separable closure of K in (L, ι_L)* is defined to be the set of all $a \in L$ such that $\min(a, K)$ is separable. We shall denote it with $S(\iota_L)$, or simply $S(L)$ when the embedding of K into L is clear.

Clearly, $\iota_L K \subseteq S(\iota_L)$. (L, ι_L) is called *separable* when $S(\iota_L) = L$, and *purely inseparable* when $S(\iota_L) = \iota_L K$.

Remark. The characterisation of inseparable, irreducible polynomials implies in characteristic zero, purely inseparable if and only if trivial. We thus limit the following to fields with positive characteristic.

Theorem – Characterisation of Finite Purely Inseparable Extensions in Positive Characteristic

Let (L, ι_L) be a finite K-extension where $\mathrm{Char} K = p > 0$. Then the following are equivalent :

1. (L, ι_L) purely inseparable.
2. For all $a \in L$, there exists $n \geq 0$ such that $a^{p^n} \in \iota_L K$. In fact, $\min(a, K)(X) = X^{p^n} - k$ for some $k \in K$.
3. For all K-extensions (N, ι_N), $|\mathrm{Emb}_K(L, N)| \leq 1$.

Proof. ($1 \Rightarrow 2$) Let $a \in L$. WLOG $a \notin \iota_L K$, for the other case is clear. Then by the characterisation of inseparable, irreducible polynomials, let $\min(a, K)(X) = g(X^{p^n})$ for some separable, irreducible g and $n > 0$. It suffices to show that g is linear. But since g is irreducible, and in fact monic, $g = \min(a^{p^n}, K)$. Then g separable and L purely inseparable implies $a^{p^n} \in S(L) = \iota_L K$, which implies g is linear.

$(2 \Rightarrow 3)$ Let (N, ι_N) be a K-extension. If $\mathrm{Emb}_K(L, N)$ is empty, we are done, so let $\iota_1, \iota_2 \in \mathrm{Emb}_K(L, N)$ and we will show they are equal. Let $a \in L$. By assumption, $a^{p^n} = \iota_L(k)$ for some $n \geq 0$ and $k \in K$. Then $\iota_1(a)^{p^n} = \iota_N(k) = \iota_2(a)^{p^n}$, which implies $\iota_1(a) = \iota_2(a)$ by Freshmen's dream.

$(3 \Rightarrow 1)$ Let $a \in S(L)$. By the embedding theorem for finite simple extensions, it suffices to give a K-extension (N, ι_N) such that (N, ι_N) splits $\min(a, K)$ and $|\mathrm{Emb}_K(K(a), N)| = 1$. To this end, let A finite $\subseteq L$ with $L = K(A)$. Let (N, ι_N) be an K-extension that splits $\min(a, K)$ and $\min(x, K)$ for all $x \in A$. Then by the embedding theorem for finite extensions applied twice, $1 \leq |\mathrm{Emb}_K(K(a), N)|$ *and* any $\iota \in \mathrm{Emb}_K(K(a), N)$ lifts to some $\iota' \in \mathrm{Emb}_K(L, N)$. By assumption, $|\mathrm{Emb}_K(L, N)| = 1$ so $|\mathrm{Emb}_K(K(a), N)| = 1$.

□

> **Theorem – Separable Decomposition of Finite Extensions**
> Let (L, ι_L) be a finite K-extension. Then $S(L)$ is a field and thus naturally a separable K-extension. Furthermore, L as a $S(L)$-extension is purely inseparable.

Proof. ($S(L)$ field) Let $a, b \in S(L)$ with $b \neq 0$. To show $a + b, -a, ab, b^{-1} \in S(L)$, it suffices to show the stronger statement that for all $x \in K(a, b)$, $\min(x, K)$ is separable.

So let $x \in K(a, b)$ and (N, ι_n) be a K-extension that splits $\min(x, K)$. By extending N, WLOG N splits $\min(a, K)$ and $\min(b, K)$, too. Then by separability of $\min(a, K), \min(b, K)$,

$$[K(x) : K] = \frac{[K(a, b) : K]}{[K(a, b) : K(x)]} = \frac{\sum_{\iota \in \mathrm{Emb}_K(K(x), N)} |\mathrm{Emb}_{K(x)}(K(a, b), \iota)|}{[K(a, b) : K(x)]} \leq |\mathrm{Emb}_K(K(x), N)|$$

and hence $[K(x) : K] = |\mathrm{Emb}_K(K(x), N)|$. By the embedding theorem finite simple extensions, $\min(x, K)$ has no repeated roots in N.

(L is a purely inseparable $S(L)$-extension) The case of $S(L) = L$ is clear, so WLOG $S(L) \subsetneq L$. Then by the characterisation of inseparable, irreducible polynomials, let $0 < p = \mathrm{Char} K = \mathrm{Char} S(L)$. We may now use the second characterisation of finite purely inseparable extensions. Let $a \in L$. WLOG $a \notin S(L)$. Then by the characterisation of inseparable, irreducible polynomials, there exists a separable, irreducible $g \in K[X]$ with $n > 0$ such that $\min(a, K)(X) = g(X^{p^n})$. Irreducibility of g implies $g = \min(a^{p^n}, K)$, which by separability of g, implies $a^{p^n} \in S(L)$ as desired. □

> **Theorem – Characterisation of Finite Separable Extensions**
> Let (L, ι_L) be a finite K-extension. Then the following are equivalent :
>
> 1. (L, ι_L) separable.
> 2. There exists finite $A \subseteq L$ such that $L = K(A)$ and for all $a \in A$, $\min(a, K)$ separable.
> 3. For all K-extensions (N, ι_N) where all $\min(a, K)$ are split for $a \in L$, $0 < |\mathrm{Emb}_K(L, N)| = [L : K]$

Proof. $(1 \Rightarrow 2)$ Characterisation of finite extensions.

$(2 \Rightarrow 3)$ Embedding theorem.

$(3 \Rightarrow 1)$ $[S(L) : K] = |\mathrm{Emb}_K(S(L), N)| = \sum_{\iota \in \mathrm{Emb}_K(S(L), N)} |\mathrm{Emb}_{S(L)}(L, \iota)| = |\mathrm{Emb}_K(L, N)| = [L : K]$. □

5 The Galois Correspondence

Theorem – Characterisation of Galois Extensions
Let (L, ι_L) be a K-extension. Then (L, ι_L) is finite, normal, separable if and only if (L, ι_L) is Galois. Furthermore, the Galois group of (L, ι_L) is always $\operatorname{Aut}_K L$ and $[L : K] = |\operatorname{Aut}_K L|$.

Proof. $(\Rightarrow)$ We must give a finite subgroup $G \subseteq \operatorname{Aut} L$ such that $\iota_L K = L^G$. The claim is that $G = \operatorname{Aut}_K L$ works.

We first show that $\iota_L K = L^G$. It suffices $L^G \subseteq \iota_L K$. Let $a \in L^G$. It suffices that $\min(a, K)$ is linear. Since L is normal, L splits $\min(a, K)$. By separability of $\min(a, K)$, it suffices to show the only Galois K-conjugate of a in L is a. Let $\alpha \in L$ be a Galois K-conjugate of a. It suffices to give $\phi_\alpha^L \in G = \operatorname{Aut}_K L$ such that $\phi_\alpha^L(a) = \alpha$. First by the characterisation of finite simple extensions, there exists $\phi_\alpha \in \operatorname{Emb}_K((K(a), \iota_L), (L, \iota_L))$ such that $\phi_\alpha(a) = \alpha$. Then by normality of (L, ι_L) and the embedding theorem for finite extensions, there exists $\phi_\alpha^L \in \operatorname{Emb}_{K(a)}(L, (L, \phi_\alpha))$. ϕ_α^L is as desired.

Finiteness of G follows from the embedding theorem for finite extensions.

$$|G| = |\operatorname{Aut}_K L| = |\operatorname{Emb}_K(L, L)| \leq [L : K]$$

$(\Leftarrow)$ Let G be a finite subgroup of $\operatorname{Aut} L$ such that $\iota_L K = L^G$. WLOG we replace K with L^G. We first show that L is algebraic, normal and separable over L^G. Let $a \in L$. Ideally, if L is normal over L^G, then it contains all Galois L^G-conjugates of a, which are precisely images of a under L^G-automorphisms by the embedding theorem for finite simple extensions and finite extensions. From this, we conjecture that

$$\min(a, K)(X) = \prod_{\alpha \in \operatorname{Orb}(a)} (X - \alpha)$$

where $\operatorname{Orb}(a) := \{\sigma(a) \,|\, \sigma \in G\}$. This suffices since the right exists, and is separable and split by L. For the claim, it suffices that $\prod_{\alpha \in \operatorname{Orb}(a)}(X - \alpha)$ is in $L^G[X]$ and irreducible. The first follows from any $\sigma \in G$ permuting $\operatorname{Orb}(a)$. The latter follows since any $f \in L^G[X]$ that has a as a root must also have all of $\operatorname{Orb}(a)$ as roots via $0 = \sigma(ev_a f) = ev^\sigma_{\sigma(a)} f = ev_{\sigma(a)} f$ for any $\sigma \in G$.

We now prove that $[L : L^G]$ is finite, and in fact, $[L : L^G] \leq |G|$. This requires one galaxy-brain idea, that $|G| = \dim_L(G \to L)$, where $G \to L$ is the L-vectorspace of functions from G to L. It thus suffices to show that for any L^G-linearly independent $X \subseteq L$, there is an L-linearly independent $X_1 \subseteq G \to L$ with $|X| = |X_1|$. Let $X \subseteq L$ be L^G-linearly independent. Then for each $x \in X$, we have $ev_x : G \to L, \sigma \mapsto \sigma(x)$. Since $id \in G$, $\{ev_x\}_{x \in X}$ bijects with X. We wish to show $\{ev_x\}_{x \in X}$ is L-linearly independent. This is equivalent to showing for all finite $X_0 \subseteq X$, $\{ev_x\}_{x \in X_0}$ is L-linearly independent.

Let $X_0 \subseteq X$ be finite and $\sum_{x \in X_0} \lambda_x ev_x = 0$ with $\lambda_x \in L$. Suppose there exists $x_0 \in X_0$ such that $\lambda_{x_0} \neq 0$. To get a contradiction, it suffices to show for all $x \in X_0$, $\lambda_x \in L^G$, for then by evaluating at $id \in G$, we have $0 = \sum_{x \in X_0} \lambda_x x$, implying all $\lambda_x = 0$. So let $\sigma \in G$. By rescaling, WLOG $\lambda_{x_0} = 1$. Then for all $\rho \in G$,

$$\sum_{x \in X_0 \setminus \{x_0\}} (\lambda_x - \sigma(\lambda_x)) ev_x(\rho) = \sum_{x \in X_0} \lambda_x ev_x(\rho) - \sigma\left(\sum_{x \in X_0} \lambda_x ev_x(\sigma^{-1} \circ \rho)\right) = 0$$

i.e. we have a L-linear combination of $\{ev_x \mid x \in X_0 \setminus \{x_0\}\}$ yielding zero. By induction on the size of X_0, $\lambda_x = \sigma(\lambda_x)$ for all $x \in X_0$. Thus for all $x \in X_0$, $\lambda_x \in L^G$ as desired.

The fact that $G = \operatorname{Aut}_{L^G} L$ follows from $|G| \le |\operatorname{Aut}_{L^G} L| = [L : L^G] \le |G|$. This concludes the proof. $\square$

> **Lemma – Lifting Normality and Separability**
>
> Let (L, ι_L) be a K-extension, $E \subseteq L$ a field containing $\iota_L K$ so that (E, ι_L) be naturally a K-extension. Then the following are true.
>
> 1. If (L, ι_L) is a normal K-extension, then $(L, \mathbb{1}_E)$ is a normal E-extension.
> 2. If (L, ι_L) is a separable K-extension, then $(L, \mathbb{1}_E)$ is a separable E-extension.

Proof. (1) Easy via the first characterisation of finite normal extensions.

(2) Let (L, ι_L) be separable and $a \in L$. Then $\min(a, E) | \iota_L \min(a, K)$. It suffices to show for all $g, f \in E[X]$, $g|f$ and f separable implies g separable. Let $g, f \in E[X]$, $g \mid f$ and f separable. Let (M, ι_M) be an E-extension where g splits. By extending (M, ι_M), WLOG f splits in M as well. Then f having no repeated roots implies g has no repeated roots. $\square$

> **Theorem – Fundamental Theorem of Galois Theory**
>
> Let (L, ι_L) be a Galois K-extension, I the partially ordered set of K-extensions inside L, and J the partially ordered set of subgroups of $\operatorname{Aut}_K L$.
>
> Then $\operatorname{Aut}_- L : I \to J$ and $L^- : J \to I$ are surjections and hence bijections. Furthermore, we have the following :
>
> 1. (Degree equals Index) Let $E \in I$. Then $[E : K] = [\operatorname{Aut}_K L : \operatorname{Aut}_E L]$.
> 2. (Group Action) Let $E \in I$. Then for all $\sigma \in \operatorname{Aut}_K L$, $\operatorname{Aut}_{\sigma E} L = \sigma \operatorname{Aut}_E L \sigma^{-1}$.
> 3. (Normality) Let $E \in I$. Then E is a normal K-extension if and only if $\operatorname{Aut}_E L$ is a normal subgroup of $\operatorname{Aut}_K L$. In this case, we have the isomorphism $\operatorname{Aut}_K E \cong \operatorname{Aut}_K L / \operatorname{Aut}_E L$.

Proof. Surjectivity of $\operatorname{Aut}_- L, L^-$ and (1) follows from lifting normality and separability and the characterisation of Galois extensions. (2) follows from definition.

(3) First, E normal K-extension implies $\operatorname{Aut}_E L$ normal follows from the characterisation of finite normal extensions and (2).

Now let $E \in I$ such that $\operatorname{Aut}_E L$ is a normal subgroup of $\operatorname{Aut}_K L$. Then by (2), for all $\sigma \in \operatorname{Aut}_K L$, $\sigma E = L^{\operatorname{Aut}_{\sigma E} L} = L^{\sigma \operatorname{Aut}_E L \sigma^{-1}} = L^{\operatorname{Aut}_E L} = E$. We thus have a natural group morphism $\operatorname{Aut}_K L \to \operatorname{Aut} E, \sigma \mapsto \sigma$. Let G be its image. The kernel is clearly $\operatorname{Aut}_E L$, so by the first isomorphism theorem for groups, we have $G \cong \operatorname{Aut}_K L / \operatorname{Aut}_E L$. Then $E^G = E \cap L^{\operatorname{Aut}_K L} = E \cap \iota_L K = \iota_L K$, thus E is a Galois K-extension, in particular normal. We have thus also shown that $\operatorname{Aut}_K E \cong \operatorname{Aut}_K L / \operatorname{Aut}_E L$. $\square$