An 8 hours course in Galois theory

Ken Lee

Autumn 2024

Contents

1 The main theorem of Galois theory

We show an example of the fundamental theorem of Galois theory. Consider the polynomial $f(T) = T^3 - 2 \in \mathbb{Q}[T]$. Let $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{C}$ be the roots of f.

Slogan : Galois theory studies the "symmetries" of roots of polynomials

To make this precise, let us first investigate the field obtained by chucking in $\alpha_0, \alpha_1, \alpha_2$ to $\mathbb{Q}$. Define

$$\mathbb{Q}_f := \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) := \text{ smallest field in } \mathbb{C} \text{ containing } \mathbb{Q}, \alpha_0, \alpha_1, \alpha_2$$

Question 0 : What does $\mathbb{Q}_f$ look like? We try to describe $\mathbb{Q}(\alpha_0)$ first. Consider the map $T \mapsto \alpha_0$

$$\begin{tikzcd}
\mathbb{Q}[T] \arrow[r, "T\mapsto\alpha_0"] \arrow[d, dashed] & \mathbb{C} \\
\mathbb{Q}(\alpha_0) \arrow[ur, "\subseteq"'] &
\end{tikzcd}$$

The image is $\mathbb{Q}[\alpha_0]$ the collection of polynomial expressions in α_0 with coefficients in $\mathbb{Q}$. Since $f \in \mathbb{Q}[T]$ is irreducible[1] we have $\mathbb{Q}[\alpha_0] = \mathbb{Q}[T]/(f)$ and hence this has a $\mathbb{Q}$-basis $1, \alpha_0, \alpha_0^2$.

- *Exercise 1 : show that for a field K and an K-algebra A which is finite dimensional as a K-vector space and an integral domain, A must be field.*

It follows that $\mathbb{Q}[\alpha_0]$ is a field and hence

$$\mathbb{Q}[\alpha_0] = \mathbb{Q}(\alpha_0)$$

Now we do a trick by observing that

$$\left(\frac{\alpha_1}{\alpha_0}\right)^3 = 2/2 = 1$$

Later on, we will give a way of checking when a polynomial has repeated roots so assume for now that all $\alpha_0, \alpha_1, \alpha_2$ are distinct. Then we get $\alpha_1 = \alpha_0\omega$ for some $\omega \neq 1 = \omega^3$, and similarly $\alpha_2 = \alpha_0\omega^2$. The ω, ω^2 here are called a *primitive cube roots of unity*. They are both roots of the polynomial $T^2 + T + 1 \in \mathbb{Q}[T]$. In the next section, we will be able to show that $\omega \notin \mathbb{Q}(\alpha_0)$. Taking this for granted for now, $T^2 + T + 1$ does not have a root in $\mathbb{Q}(\alpha_0)$, so it is irreducible in $\mathbb{Q}(\alpha_0)[T]$. It follows that

$$\mathbb{Q}[\alpha_0, \omega] \simeq \mathbb{Q}[\alpha_0][T]/(T^2 + T + 1)$$

As a $\mathbb{Q}[\alpha_0]$-vector space, this has dimension two and hence is again a field by Exercise 1. We deduce **Answer 0 :**

$$\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) = \mathbb{Q}[\alpha_0, \omega] = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$$

We now define *the Galois group of f* as

$$G_f := \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) := \{\sigma : \mathbb{Q}_f \to \mathbb{Q}_f \text{ s.t. } \sigma \text{ ring morphism and } \forall\, \lambda \in \mathbb{Q}\,,\, \sigma(\lambda) = \lambda\}$$

Question 1 : Why is this the "symmetries" of $\alpha_0, \alpha_1, \alpha_2$? Observation : any $\sigma \in G_f$ must permute $\{\alpha_0, \alpha_1, \alpha_2\}$. This is ***the* trick** that underlies Galois theory :

$$f(\sigma(\alpha_i)) = (\sigma(\alpha_i))^3 - 2 = \sigma(\alpha_i^3 - 2) = 0$$

Hence we have a well-define group morphism

$$G_f \to \mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\}$$

Since $\mathbb{Q}_f = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$ any $\sigma \in G_f$ is determined by what it does on α_i hence the above morphism is injective. **Answer 1 : The above morphism defines an isomorphism**

$$G_f \simeq \{\sigma \in \mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\} \text{ s.t. } \forall g \in \mathbb{Q}[X_0, X_1, X_2]\,, g(\alpha_0, \alpha_1, \alpha_2) = 0 \Rightarrow g(\sigma(\alpha_0), \sigma(\alpha_1), \sigma(\alpha_2)) = 0\}$$

in other words, G_f is the permutations of roots of f which preserves all algebraic relations over $\mathbb{Q}$.

Proof. $\mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$ is precisely the image of the evaluation map

$$\mathbb{Q}[X_0, X_1, X_2] \to \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]\,,\; X_i \mapsto \alpha_i$$

[1] Can be checked by Eisenstein's criterion. Alternatively, a cubic over $\mathbb{Q}$ is reducible iff it has a root in $\mathbb{Q}$. This can be checked to be impossible by brute force.

It follows that $\mathbb{Q}[\alpha_0, \alpha_1, \alpha_2] \simeq \mathbb{Q}[X_0, X_1, X_2]/I$ where I is the set of polynomials $g(X_0, X_1, X_2)$ with $g(\alpha_0, \alpha_1, \alpha_2)$. From this, it is clear that G_f lands inside the RHS. Now given $\tilde{\sigma}$ in RHS, one can evaluate

$$\mathbb{Q}[X_0, X_1, X_2] \to \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]\,,\ X_i \mapsto \tilde{\sigma}(\alpha_i)$$

Then by definition I is in the kernel of this evaluation map so it factors through the quotient by I to give an automorphism of $\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ preserving $\mathbb{Q}$. □

Let us now compute G_f. We have the following

$$\mathbb{Q}_f = \mathbb{Q}[\alpha_0, \omega] = \mathbb{Q}[\alpha_0][\omega] \simeq \frac{\mathbb{Q}[\alpha_0][Y]}{(Y^2 + Y + 1)} \simeq \frac{\mathbb{Q}[X][Y]/(X^3 - 2)}{(X^3 - 2, Y^2 + Y + 1)/(X^3 - 2)} \simeq \frac{\mathbb{Q}[X, Y]}{(X^3 - 2, Y^2 + Y + 1)}$$

where the last isomorphism is the 3rd isomorphism theorem of rings. Consider the 3-cycle $\sigma := (\alpha_0\ \alpha_1\ \alpha_2)$. Knowing $\omega = \alpha_1/\alpha_0$ we send $X \mapsto \alpha_1, Y \mapsto \omega$.

$$\begin{tikzcd}
\mathbb{Q}[X, Y] \arrow[r, "\substack{X\mapsto\alpha_1 \\ Y\mapsto\omega}"] \arrow[d, "\substack{X\mapsto\alpha_0 \\ Y\mapsto\omega}"'] & \mathbb{Q}[\alpha_0, \omega] \\
\mathbb{Q}[\alpha_0, \omega] \arrow[ur, dashed, "\simeq"'] &
\end{tikzcd}$$

We get the factoring because $\alpha_1^3 - 2 = 0 = \omega^2 + \omega + 1$ and so $\sigma \in G_f$. Now consider $\tau := (\alpha_0\ \alpha_1)$. Again, since $\omega = \alpha_1/\alpha_0$ we know τ should send $\omega \mapsto 1/\omega = \omega^2$ so we send $X \mapsto \alpha_0, Y \mapsto \omega^2$.

$$\begin{tikzcd}
\mathbb{Q}[X, Y] \arrow[r, "\substack{X\mapsto\alpha_1 \\ Y\mapsto\omega^2}"] \arrow[d, "\substack{X\mapsto\alpha_0 \\ Y\mapsto\omega}"'] & \mathbb{Q}[\alpha_0, \omega] \\
\mathbb{Q}[\alpha_0, \omega] \arrow[ur, dashed, "\simeq"'] &
\end{tikzcd}$$

Again $\alpha_1^3 - 2 = 0 = (\omega^2)^2 + \omega^2 + 1$ gives the above factoring and hence $\tau \in G_f$. It follows that G_f is the whole of $\mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\}$.

Symmetry means "changes that cannot be observed". The symmetries of a triangle are the ways you can change the triangle such that you cannot tell the difference between before and after. In the same way, G_f are the ways you can swap of roots of f such that as far as $\mathbb{Q}$ can tell, nothing has changed. In this example, there is nothing special about α_0; the whole argument works starting with α_1 or α_2. The roots are equally ambiguous, which is reflected in the quantitative fact that $G_f \simeq S_3$. An example of less ambiguity is $T^3 - 1$. The roots are $1, \omega, \omega^2$. The Galois group of $T^3 - 1$ is cyclic order two generated by $\omega \mapsto \omega^2$. This reflects the fact that 1 is more special than ω, ω^2 whilst the latter cannot be distinguished from each other. Indeed if one writes $\mu := \omega^2$ then $\omega = \mu^2$.

Back to T^3-2. Observe that $\mathbb{Q} \subseteq \mathbb{Q}_f^{G_f}$:= the set of elements in $\mathbb{Q}_f$ fixed by G_f. **Claim :** $\mathbb{Q} = \mathbb{Q}_f^{G_f}$**.** Let $x \in \mathbb{Q}_f$ be fixed by G_f. We approach $\mathbb{Q}_f$ this time by adding ω first then α_0. Since $\mathbb{Q}_f = \mathbb{Q}[\omega][\alpha_0]$ we can write

$$x = \lambda_0 + \lambda_1\alpha_0 + \lambda_2\alpha_0^2$$

for $\lambda_i \in \mathbb{Q}(\omega)$. Then since $\sigma(\omega) = \omega$ we have

$$x = \sigma(x) = \lambda_0 + \lambda_1\omega\alpha_0 + \lambda_2\omega^2\alpha_0^2$$

Since $1, \alpha_0, \alpha_0^2$ are a $\mathbb{Q}(\omega)$-basis for $\mathbb{Q}_f$, we can compare coefficients to get $\lambda_1 = \lambda_1\omega$ and $\lambda_2 = \lambda_2\omega^2$ This implies $\lambda_1 = 0 = \lambda_2$ and so $x \in \mathbb{Q}(\omega)$. Now $x = \mu_0 + \mu_1\omega$ for $\mu_i \in \mathbb{Q}$. Then

$$x = \tau(x) = \mu_0 + \mu_1\omega^2 = (\mu_0 - \mu_1) - \mu_1\omega$$

which implies $\mu_1 = -\mu_1$ and so $\mu_1 = 0$. We find that $x \in \mathbb{Q}$. More generally, given any subgroup H of G_f we can compute the *fixed subfield* $\mathbb{Q}_f^H$. Here is a diagram of all the subgroups of G_f and their corresponding fixed subfields.

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) & & \\
\mathbb{Q}(\omega) \arrow[ur] & \mathbb{Q}(\alpha_0) \arrow[u] & \mathbb{Q}(\alpha_1) \arrow[ul] & \mathbb{Q}(\alpha_2) \arrow[ull] \\
 & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & 1 \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle(\alpha_0\ \alpha_1\ \alpha_2)\rangle \arrow[dr] & \langle(\alpha_1\ \alpha_2)\rangle \arrow[d] & \langle(\alpha_0\ \alpha_2)\rangle \arrow[dl] & \langle(\alpha_0\ \alpha_1)\rangle \arrow[dll] \\
 & G_f & &
\end{tikzcd}$$

The fundamental theorem of Galois theory says this is all of them. To be more precise, we make some definitions.

> **Definition – Galois extension**
>
> Let $K \to L$ be an extension of fields. We often identify K with its image in L. We call it *Galois* when there is a finite group $G \subseteq \operatorname{Aut}_K L$ such that $K = L^G$.

The extension earlier $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ was an example of a Galois extension.

> **Proposition – Fundamental theorem of Galois theory**
>
> Let $K \to L$ be a Galois extension of fields and let $G := \operatorname{Aut}_K L$. Consider the following two constructions :
>
> - Given a subgroup $H \subseteq G$, define L^H as the set of fixed points of L by H. This defines a field containing the image of K.
> - Given a subfield $M \subseteq L$ containing K, define $\operatorname{Aut}_M L$ as the subgroup of G acting trivially on M.
>
> Then we have an order reversing bijection
>
> $$\begin{tikzcd} \{\text{subextensions } M \subseteq L\} \arrow[r, shift left=1.5, "\mathrm{Aut\_}L"] \arrow[r, phantom, "\simeq"] & \{\text{subgroups of } \operatorname{Aut}_K L\} \arrow[l, shift left=1.5, "L^{-}"] \end{tikzcd}$$

∎

The Galois extension $\mathbb{Q}_f/\mathbb{Q}$ is an example of a *solvable* extension.

> **Definition**
> Let $K \to L$ be a field extensions. We say it is *radical* when there exists a chain of extensions
>
> $$K = L_0 \to L_1 \to \cdots \to L_{n-1} \to L_n = L$$
>
> such that each $L_{i+1} = L_i(\alpha_i)$ for some α_i with $\alpha_i^{d_i} \in L_i$ for some $d_i > 0$.
>
> We say a polynomial $f \in K[T]$ is *solvable by radicals* when K_f/K is radical.

Notice that in the example, that the sequence of groups

$$1 \to \langle(\alpha_0\ \alpha_1\ \alpha_2)\rangle \to G_f$$

is such that one subgroup is normal in the next and furthermore that the factor groups are cyclic. This is an example of a *solvable group*.

> **Definition**
> Let G be a finite group. Then G is called solvable when there exists a chain
>
> $$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{n-1} \triangleleft H_n = G$$
>
> such that H_{n+1}/H_n is cyclic.

We will show the following by the end of the course.

> **Proposition – Characteristization of solvable polynomials**
> Let K be a field of characteristic zero and $f \in K[T]$. Then f is solvable by radicals iff G_f is solvable.

> **Proposition**
> The polynomial $T^5 - T - 1 \in \mathbb{Q}[T]$ has Galois group S_5 and hence is not solvable by radicals.

2 Finite extensions and the embedding theorem

We saw in the previous section that $\omega \in \mathbb{Q}(\alpha_0)$ precisely when there is a solution to $T^2 + T + 1$ inside $\mathbb{Q}(\alpha_0)$. Accordingly, there is no copy of $\mathbb{Q}(\omega)$ inside $\mathbb{Q}(\alpha_0)$. This section investigates this phenomenon. We didn't formally define field extensions last time.

> **Definition**
> A field extension is a ring morphism $\iota : K \to L$ between fields.
>
> Since fields have no non-trivial ideals, any field extension $\iota : K \to L$ must be injective. When it is clear, we often identify K with its image ιK.

> *Example.*
> *Here is an example of a field extension from a field to itself. Let* $\mathbb{Q}(T) := \operatorname{Frac}\mathbb{Q}[T]$. *Define* $\mathbb{Q}[T] \to \mathbb{Q}[T], T \mapsto T^2$. *Then this induces a field extension* $\mathbb{Q}(T) \to \mathbb{Q}(T)$ *where the image of the first copy is* $\mathbb{Q}(T^2)$.

A basic invariant of a field extension is its degree.

> **Definition – Degree of an extension**
>
> Let $K \to L$ be a field extension. Define its *degree* as $[L : K] := \dim_K L$. It is called finite when $[L : K] < \infty$.

When proving things about a finite extension $K \to L$, we will often do so by inducting on $[L : K]$. The following is useful.

> **Proposition – Tower law**
>
> Let $K \to L \to N$ be extensions of fields. Then $[N : K] = [N : L][L : K]$. In particular, a sequence of finite extensions is finite.

The following argument works for infinite extensions, though we will mostly be interested in finite extensions.

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. □

> *Example.*
> *Now we can show* $\omega \notin \mathbb{Q}(\alpha_0)$ *from the previous section. We have* $3 = [\mathbb{Q}(\alpha_0) : \mathbb{Q}] = [\mathbb{Q}(\alpha_0) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha_0) : \mathbb{Q}(\omega)]2$ *which is a contradiction because 2 does not divide 3.*

> **Definition**
>
> Let $K \to L$ be a field extension. For $A \subseteq L$, define $K(A) \subseteq L$ as the smallest subfield of L containing the image of K and A. We say $K \to L$ is finite type when there exists finite $A \subseteq L$ with $L = K(A)$. In the case of $A = \{a\}$, we write $K(a)$. We call extensions of the form $K \to K(a)$ simple.

> Given $a \in L$, one can consider the evaluation ring morphism
>
> $$\mathrm{ev}_a : K[T] \to L, f(T) \mapsto f(a)$$
>
> We say a is *algebraic over* K when there exists a non-zero f with $f(a) = 0$, i.e. $0 \neq \ker \mathrm{ev}_a$.
>
> We say $K \to L$ is algebraic when all $a \in L$ is algebraic over K.

> **Proposition – Characteristization of finite simple extensions**
> Let $K \to L$ be an extension and $a \in L$. Then the following are equivalent :
>
> 1. a is algebraic over K
> 2. $[K(a) : K]$ is finite
> 3. $K \to K(a)$ is algebraic.

Proof. $(1 \Rightarrow 2)$ We saw in section 1 how to compute $K(a)$. Specifically, consider the evaluation map $K[T] \to L, f \mapsto f(a)$ and let $K[a]$ be its image. By assumption, there exists non-zero $f \in K[T]$ with $f(a) = 0$. WLOG $\deg f = N \geq 0$. Then $1, a, \ldots, a^{N-1}$ is a K-spanning set for $K[a]$. This implies $K[a]$ is a finite dimensional K-vector space and hence a field and hence $K[a] = K(a)$.

$(2 \Rightarrow 3)$ Let $b \in K(a)$. Since $[K(a) : K]$ is finite, there exists a non-trivial linear combination $0 = \sum_{n \geq 0} \lambda_n b^n$ with $\lambda_n \in K$, which implies b is algebraic over K.

$(3 \Rightarrow 1)$ trivial. □

> **Proposition – Characteristization of finite extensions**
> Let $K \to L$ be an extension. The following are equivalent :
>
> 1. $[L : K]$ is finite
> 2. $K \to L$ is finite type and algebraic
> 3. There exists finite $A \subseteq L$ such that $L = K(A)$ and all $a \in A$ are algebraic.

Proof. $(1 \Rightarrow 2)$ Take a K-basis and use the characterization of finite simple extensions . $(2 \Rightarrow 3)$ Clear. $(3 \Rightarrow 1)$ Induct on the size of A and use the characterization of finite simple extensions .

□

We are now ready for the main result of this section.

> **Proposition – Embedding theorem for finite simple extensions**
> Let $K \to L$ be an extension and $a \in L$ algebraic over K. The ideal $\ker \mathrm{ev}_a \subseteq K[T]$ is generated by a unique monic polynomial. We call it the *minimal polynomial of a over K*, denoted $\min(a, K)$. Let $K \to N$ be another extension. Then we have a bijection
>
> $$\mathrm{Emb}_K(K(a), N) \simeq \{b \in N \text{ s.t. } \min(a, K) = \min(b, K)\}, \varphi \mapsto \varphi(a)$$

> In particular, $|\mathrm{Emb}_K(K(a), N)| \leq [K(a) : K]$. Elements $b \in N$ with $\min(b, K) = \min(a, K)$ are called *Galois conjugates of a.*

Proof. We saw $K(a) = K[a] \simeq K[T]/(\min(a, K))$. Given $\varphi : K(a) \to N$ a K-embedding, the composition $K[T] \to K(a) \to N$ is $\mathrm{ev}_{\varphi(a)}$. Since $K(a) \to N$ is injective, we have $\ker \mathrm{ev}_{\varphi(a)} = \ker \mathrm{ev}_a$. It follows that $\min(\varphi(a), K) = \min(a, K)$. Conversely, given $b \in N$ a Galois conjugate of a we can define the K-embedding $K(a) \simeq K[T]/(\min(a, K)) = K[T]/(\min(b, K)) \simeq K(b) \subseteq N$. □

We will now generalise the above to general finite extensions. For this, we need to know how embeddings from subextensions interact with the whole extension.

> **Proposition – Subextensions partition embeddings**
>
> Let $K \to L \to M$ and $K \to N$ be extensions. Then we have a bijection
>
> $$\bigsqcup_{\iota \in \mathrm{Emb}_K(L,N)} \mathrm{Emb}_L(M, N) \xrightarrow{\sim} \mathrm{Emb}_K(M, N)$$
>
> by sending $(L \to N \in \mathrm{Emb}_K(L, N), M \to N \in \mathrm{Emb}_L(M, N))$ to $M \to N$ viewed as a K-embedding.

Proof. The point is that we have a map $\mathrm{Emb}_K(M, N) \to \mathrm{Emb}_K(L, N)$ and the fibers over each $\iota : L \to N$ is precisely the set of L-embeddings $M \to N$ where N is viewed as an L-extension by $\iota : L \to N$. □

> **Proposition – Embedding theorem for finite extensions**
>
> Let $K \to L$ be an extension and $A \subseteq L$ finite set of algebraic generators for L over K. Let $K \to N$ be another extension and assume that for all $a \in A$ the minimal polynomial $\min(a, K)$ splits into linear factors in $N[T]$. Then
>
> $$0 < |\mathrm{Emb}_K(L, N)| \leq [L : K]$$
>
> and we have equality if for all $a \in A$ the polynomial $\min(a, K)$ has no *repeated* roots in N.

Proof. Induct on the cardinality of A. $A = \varnothing$ is trivial so let $a_0 \in A$ and $M := K(A \setminus \{a_0\})$ and assume inductively $0 < \mathrm{Emb}_K(M, N) \leq [M : K]$ with equality if all for all $a_1 \in A \setminus \{a_0\}$ we have $\min(a_1, K)$ with no repeated roots in N. Then $L = M(a_0)$. We have $\min(a_0, M)$ divides $\min(a_0, K)$ in $M[T]$, so $\min(a_0, M)$ also splits into linear factors in $N[T]$. It follows from the characterization of finite simple extensions and the tower law that

$$0 < |\mathrm{Emb}_K(L, N)| = \sum_{\mathrm{Emb}_K(M,N)} |\mathrm{Emb}_M(L, N)| \leq \sum_{\mathrm{Emb}_K(M,N)} [L : M] \leq [L : M][M : K] = [L : K]$$

Now assume all $\min(a, K)$ for $a \in A$ split into linear factors in N. This implies $\min(a_0, M)$ splits into linear factors in N so $|\mathrm{Emb}_M(L, N)| = [L : M]$. Then the first $\leq$ is an equality and the second is also by the induction hypothesis on M.

□

3 Normal and separable extensions

Given an extension $K \to L = K(a_1, \dots, a_n)$ with a_i algebraic over K, the embedding theorem for finite extensions tells us how to construct automorphisms of L over K. For the main theorem of Galois theory to hold true, we need to have the maximum number of automorphisms, i.e. $|\mathrm{Aut}_K L| = [L : K]$. The embedding theorem indicates two ways in which this can fail :

1. the polynomials $\min(a_i, K)$ do not split into linear factors in $L[X]$
2. there exists some a_i such that $\min(a_i, K)$ has a repeated root in L.

These two phenomena are respectively called normality and separability. Let us illustrate the failure of normality by focusing on the extension $\mathbb{Q} \to \mathbb{Q}(\alpha_0)$ from the first section. Using the embedding theorem for finite simple extensions, we see that $\sigma \in \mathrm{Emb}_{\mathbb{Q}}(\mathbb{Q}(\alpha_0), \mathbb{Q}(\alpha_0))$ correspond to solutions of $T^3 - 2$ in $\mathbb{Q}(\alpha_0)$. There is only α_0: If there is another root $\tilde{\alpha_1}$ then $\tilde{\omega} := \tilde{\alpha_1}/\alpha_0$ would be a primitive cube root of unity and $[\mathbb{Q}(\tilde{\omega}) : \mathbb{Q}] = 2$ which we cannot have as we saw before. From this, we can see the problem is that $\mathbb{Q}(\alpha_0)/\mathbb{Q}$ does not contain *all* the roots of the polynomial $T^3 - 2$. More precisely, $T^3 - 2$ does not factorise into linear factors in $\mathbb{Q}(\alpha_0)[T]$. We can also see this phenomenon in the following way : there are three ways of $\mathbb{Q}$-embedding $\mathbb{Q}(\alpha_0)$ inside $\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ corresponding to each $\mathbb{Q}(\alpha_i)$ and their images are *different*.

> **Definition – Normal Extension**
>
> Let $K \to L$ be an extension and $f \in K[X]$. Then we say L *splits* f when f factorises into linear factors in $L[X]$.
>
> Suppose L/K 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 $\min(a, K)$.

> **Proposition – Splitting Polynomials**
>
> Let K be a field and $f \in K[X] \setminus K$. Then there exists an extension $K \to L$ 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. □

> **Proposition – Characterisation of Finite Normal Extensions**
>
> Let $K \to L$ be a finite extension. Then the following are equivalent :
>
> 1. (Contains all Galois K-Conjugates) $K \to L$ normal.
> 2. (Contains all Galois K-Conjugates of Generators) There exists $A \subseteq L$ a finite set of generators of $K \to L$ 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 extensions $K \to N$ 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-embeddings. Let $f(X) = \prod_{k=1}^{\deg f}(X - a_k) \in L[X]$. where $a_k \in L$. Then $f(X) = \prod_{k=1}^{\deg f}(X - \iota_0(a_k)) \in N[X]$ For all a_l, since ι_1 fixes K we get

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

so 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 $\iota_1 L \subseteq \iota_0 L$ and by symmetry $\iota_0 L \subseteq \iota_1 L$ 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 extension $L \to M$ such that M splits $\min(a, K)$. We seek to show that all Galois K-conjugates of a in M are actually in (the image of) L already. 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 $\iota_1 \in \mathrm{Emb}_{K(a)}(L, \phi_\alpha)$. □

Now let us discuss separability. As we will see, existence of inseparable irreducible polynomials is linked with the *characteristic* of the base field K. This implies that in terms of finding an insolvable quintic over $\mathbb{Q}$, the problem of inseparable minimal polynomials never happens.

> **Definition – Separable Polynomial, Separable extension**
>
> 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*. An algebraic extension $K \to L$ is called separable when for all $a \in L$, the polynomial $\min(a, K)$ is separable.

> **Proposition – Characterization of separable polymomials using differentials**
>
> Let K be a field and $f = \sum_{0 \le n} f_n X^n \in K[X]$. The *formal derivative of* f is defined to be $f' = \sum_{0<n} n f_n X^{n-1}$. Then f is separable iff $(f, f') = 1$.

Proof. We will prove f is inseparable iff $(f, f') \neq 1$. Assume f is inseparable. Suppose $(f, f') = 1$. Then by the Euclidean algorithm there exists $\lambda, \mu \in K[X]$ such that $\lambda f + \mu f' = 1$. Let $K \to L$ be an extension where f has a repeated root a. By factoring $f(X) = (X - a)^2 g(X)$ in $L[X]$ and the product rule for formal differentiation (which can be proved by induction), we see a contradiction

$$1 = \lambda(a) f(a) + \mu(a) f'(a) = 0 + 0 = 0$$

Now assume $(f, f') \neq 1$. Let $h \in K[X]$ be the GCD of f and f', which is non-constant by assumption. Let $K \to L$ be any extension that splits f. It also splits h. Let $a \in L$ with $h(a) = 0$. We can write $f(X) = (X - a)^d g(X)$ in $L[X]$ for some $d \geq 0$ and $g(a) \neq 0$. Since h divides f we have $f(a) = 0$ so $d \geq 1$. Suppose $d = 1$. We also have h divides f' yielding a contradiction

$$0 = f'(a) = g(a) \neq 0$$

□

To give an example of an inseparable extension, we need to discuss the notion of the characteristic of a field.

> **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 $\mathrm{Char} K$.
>
> More generally, the characteristic of any integral domain A is defined in the same way.

> *Example.*
> *All fields K of characteristic 0 have a unique extension map $\mathbb{Q} \to K$. Similarly, all fields K of characteristic $p > 0$ have a unique extension map $\mathbb{F}_p \to K$.*

The following is the root of all interesting phenomena in positive characteristic.

> **Proposition – Freshman's dream**
>
> Let A be an integral domain of characteristic $p > 0$ and $a, b \in A$. Then $(a + b)^p = a^p + b^p$

Proof. The point is that the binomial coefficient $\binom{p}{k}$ for $0 < k < p$ is divisible by p. □

> *Example.*
> *Consider $K = \mathbb{F}_p(T) := \mathrm{Frac}\, \mathbb{F}_p[T]$ and the polynomial $f(X) = X^p - T \in K[X]$. Then by Eisenstein's criterion f is irreducible. Let $L := K[X]/(f)$ and $T^{1/p}$ the image of X in L. Then in $L[X]$ we have by Freshman's dream*
>
> $$f(X) = X^p - T = X^p - (T^{1/p})^p = (X - T^{1/p})^p$$
>
> *So f is inseparable. Notice in that $f' = 0$ so indeed $(f, f') \neq 1$.*

In fact, we cannot have inseparable extensions in characteristic zero.

> **Proposition**
> Let K be characteristic zero. Then any irreducible $f \in K[T]$ is separable.

Proof. f' is either zero or has degree strictly less than f. WLOG f is monic. Then $0 = f'$ implies by looking at the leading coefficient, $0 = \deg f$ as elements of K, contradicting the characteristic of K being zero. So $f' \neq 0$. But then we must have $(f, f') = 1$ because $\deg f' < \deg f$ implies f cannot divide f'. □

4 Galois extensions and the fundamental theorem

> **Definition**
> An extension $K \to L$ is called Galois when there exists a finite subgroup $G \subseteq \operatorname{Aut}_K L$ such that $K = L^G$.

> **Proposition – Characterization of Galois extensions**
> Let $K \to L$ be an extension. Then $K \to L$ is finite, normal, separable iff $K \to L$ is Galois. In this case the finite subgroup G such that $K = L^G$ must be $\operatorname{Aut}_K L$.

Proof. Slogan : *set of Galois conjugates = orbit*.

$(1 \Rightarrow 2)$ By the embedding theorem, $|\operatorname{Aut}_K L| \leq [L : K]$. We claim that $G := \operatorname{Aut}_K L$ works. Let $a \in L^G$. Goal : $a \in K$. It suffices to show $\min(a, K)$ is linear. Since $K \to L$ is normal, $\min(a, K)$ splits in L. Since $K \to L$ is separable, it suffices to show that for any Galois K-conjugate α of a we have $\alpha = a$. Let $\alpha \in L$ with $\min(a, K)(\alpha) = 0$. Since $a \in L^G$ is suffices to give $\sigma \in \operatorname{Aut}_K L$ which $\sigma(a) = \alpha$. By the embedding theorem applied to $K(a) \to L$, we can extend $K(a) \simeq K(\alpha) \to L$ to an automorphism $\sigma : L \to L$ preserving K. This maps a to α as desired.

$(2 \Rightarrow 1)$ Let G be a finite subgroup of $\operatorname{Aut}_K L$ such that $K = L^G$. For $a \in L$ we claim that

$$\min(a, K)(T) = \prod_{\alpha \in Ga} (T - \alpha) \in L[T]$$

where Ga denotes the G-orbit of a. This proves that L/K is normal and separable. Let $f \in L[T]$ be the above product. The claim is equivalent to showing $f \in L^G[T] = K[T]$ and f is irreducible in $K[T]$. Let $\sigma \in G$. Then

$$\sigma f(T) = \sigma \prod_{\alpha \in Ga} (T - \alpha) = \prod_{\alpha \in Ga} (T - \sigma(\alpha)) = \prod_{\tilde{\alpha} \in Ga} (T - \tilde{\alpha}) = f(T)$$

Therefore $f \in K[T]$. For irreducibility, if $f = gh$ is a non-trivial factoring in $K[T]$ then one of g or h has a as a root. Say it's g, then by applying $\sigma \in G$ to the equation $0 = g(a)$ we get that g has all $\alpha \in Ga$ as roots, i.e. f divides g, a contradiction.

Now we show L/K is finite. We are expecting $G = \operatorname{Aut}_K L$ which should have size $[L : K]$. So we will bound $[L : K] \leq |G|$. Magic claim : $\dim_K L = \dim_L L[G] = |G|$ where $L[G]$ is the set of functions from G to L. It will suffice for us to show that any K-linearly independent set gives rise to a L-linearly independent set in $L[G]$ with the same cardinality. Let $A \subseteq L$ be a finite K-linearly independent set. Define $\tilde{A} := \{\mathrm{ev}_a\}_{a \in A} \subseteq L[G]$. Then $\mathrm{ev}_\_ : A \to \tilde{A}$ is a bijection because $\mathrm{ev}_a = \mathrm{ev}_{a_1}$ implies $a = \mathrm{ev}_a(e) = \mathrm{ev}_{a_1}(e) = a_1$ and surjectivity is by definition. Claim : $\tilde{A}$ is a L-linearly independent set in $L[G]$. We induct on $|A|$. Let $\sum_{x \in X_0} \lambda_x ev_x = 0$ with

$\lambda_x \in L$. Suppose for a contradiction that there exists $a_0 \in A$ such that $\lambda_{a_0} \neq 0$. It suffices to show for all $a \in A$ we have $\lambda_a \in L^G = K$, for then by evaluating at $e \in G$ gives $0 = \sum_{a \in A} \lambda_a a$, implying all $\lambda_a = 0$. So let $\sigma \in G$ with the goal of showing $\sigma(\lambda_a) = \lambda_a$ for all $a \in A$. By rescaling, WLOG $\lambda_{a_0} = 1$. By induction it suffices to show

$$\sum_{x \in X_0 \backslash \{x_0\}} (\lambda_x - \sigma(\lambda_x)) ev_x = 0 \in L[G]$$

Let $\rho \in G$. Then we have as desired

$$\begin{aligned} \sum_{a \in A \backslash \{a_0\}} (\lambda_a - \sigma(\lambda_a)) ev_a(\rho) &= \sum_{x \in X_0} \lambda_x ev_x(\rho) - \sum_{a \in A} \sigma(\lambda_a) \rho(a) \\ &= -\sigma\left(\sum_{a \in A} \lambda_a \sigma^{-1} \rho(a)\right) = -\sigma\left(\left(\sum_{a \in A} \lambda_a \, \mathrm{ev}_a\right) \sigma^{-1} \rho\right) = 0 \end{aligned}$$

□

> **Proposition – Fundamental theorem of Galois theory**
> Let $K \to L$ be a Galois extension of fields and let $G := \operatorname{Aut}_K L$. Then we have an order reversing bijection
>
> $$\begin{tikzcd} \{K\text{-subextensions } E \subseteq L\} \arrow[r, shift left=1.5ex, "\mathrm{Aut\_}L"] \arrow[r, phantom, "\simeq"] & \{\text{subgroups of } \mathrm{Aut}_K L\} \arrow[l, shift left=1.5ex, "L^{-}"] \end{tikzcd}$$
>
> Furthermore, for $E \subseteq L$ a K-subextension we have the following :
>
> 1. (Degree equals Index) $[E : K] = [\operatorname{Aut}_K L : \operatorname{Aut}_E L]$.
> 2. (Group Action) For all $\sigma \in \operatorname{Aut}_K L$, $\operatorname{Aut}_{\sigma E} L = \sigma \operatorname{Aut}_E L \sigma^{-1}$.
> 3. (Normality) 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. We need a lemma.

> *Lemma. Let $K \to E \to L$ be a sequence of extensions.*
>
> 1. *If $K \to L$ is finite normal, then $E \to L$ is finite normal.*
> 2. *If $K \to L$ is finite separable, then $E \to L$ is finite separable.*
>
> *Proof.* Exercise. ■

(Surjectivity) Let $H \subseteq \operatorname{Aut}_K L$ be a subgroup. Then $\operatorname{Aut}_{L^H} L = H$ by the characterisation of Galois extensions. Now let $E \subseteq L$ be a K-subextension. Then by the above lemma, L/E is Galois so $E = L^{\operatorname{Aut}_E L}$.

(Injectivity) This actually does not use any Galois theory and is true for any partially ordered set. Here is the statement.

> *Lemma. Let I, J be partially ordered sets, $F : I \to J$ and $G : J \to I$ be order reversing functions satisfying:*
>
> - *(Adjunction) For all $x \in I$ and $y \in J$, $x \leq G(y)$ iff $y \leq G(x)$.*
>
> *Then $FGF = F$ and $GFG = G$. In particular, F and G induce a bijection on the images FI, GJ.*
>
> *Proof.* Exercise. ■

(Degree equals index) Use the above lemma and the characterisation of Galois extensions.

(Group action) Exercise.

(Normality) If E/K is normal, then image-invariance of normal extensions we get a well-defined morphism of groups by restriction

$$\operatorname{Aut}_K L \to \operatorname{Aut}_K E$$

The kernel is by definition $\operatorname{Aut}_E L$ so it is normal.

If $\operatorname{Aut}_E L$ is normal, then for any $\sigma \in \operatorname{Aut}_K L$ we have

$$\sigma E = L^{\operatorname{Aut}_{\sigma E} L} = L^{\sigma \operatorname{Aut}_E L \sigma^{-1}} = L^{\operatorname{Aut}_E L} = E$$

so restriction gives a well-defined morphism of groups $\operatorname{Aut}_K L \to \operatorname{Aut}_K E$. Let G be the image. Then $E^G = E \cap L^{\operatorname{Aut}_K L} = E \cap L^G = E \cap K = K$ so E/K is Galois and hence normal. By the characterisation of Galois extensions, G must be all of $\operatorname{Aut}_K E$ and hence by the first isomorphism theorem of groups we have $\operatorname{Aut}_K E \simeq \operatorname{Aut}_K L / \operatorname{Aut}_E L$.

□

> *Example.*
> *Let us compute the Galois group of $T^4 - a \in \mathbb{Q}[T]$ over $K = \mathbb{Q}$ where a is a positive integer with no square factors.*
>
> *Let $p > 0$ be a prime that divides a. Then $T^4 - a$ satisfies Eisenstein's criterion and hence is irreducible in $\mathbb{Q}[T]$. Let L/K be a splitting field of $T^4 - a$ and $\alpha \in L$ any root. This is a Galois extension because $\mathbb{Q}$ is characteristic zero. By separability of $T^4 - a$, there exists another root β not equal to $\pm\alpha$. Let $i := \beta/\alpha$. Then $0 = i^4 - 1 = (i-1)(i+1)(i^2+1)$ implies $i^2 + 1 = 0$. So the four roots are $\alpha, \alpha i, \alpha i^2, \alpha i^3$.*
>
> *Let $\sqrt[4]{2} \in \mathbb{R}$ be the unique positive fourth-root of 2. Using the embedding theorem, there exists an embedding $\phi : L \to \mathbb{C}$ such that $\phi(\alpha) = \sqrt[4]{2}$. From this, we deduce $i \notin \mathbb{Q}(\alpha)$ because if it were it would give an element $\phi(i) \in \phi\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ which is not fixed by complex conjugation. It follows that $T^2 + 1$ is irreducible in $\mathbb{Q}(\alpha)[T]$ and hence $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.* [a]
>
> *Using embedding theorem for $L/\mathbb{Q}(\alpha)$, we get $\tau \in \operatorname{Aut}_{\mathbb{Q}} L$ such that*
>
> $$\tau(i) = -i \qquad \tau(\alpha) = \alpha$$
>
> *Since $\deg \min(\alpha, \mathbb{Q}(i)) = [L : \mathbb{Q}(i)] = 4$ by the tower law, we have $\min(\alpha, \mathbb{Q}(i)) = T^4 - 2$. Using embedding theorem again, we have $\sigma \in \operatorname{Aut}_{\mathbb{Q}} L$ such that*
>
> $$\sigma(i) = i \qquad \sigma(\alpha) = \alpha i$$

We have $\sigma^k(\alpha) = \alpha i^k$ so σ has order 4.

$$\tau\sigma\tau^{-1}(i) = \tau\sigma(-i) = \tau(-i) = i$$
$$\tau\sigma\tau^{-1}(\alpha) = \tau\sigma(\alpha) = \tau(\alpha i) = -\alpha i = \sigma^{-1}(\alpha)$$

So $\tau\sigma\tau^{-1} = \sigma^{-1}$ and thus $\operatorname{Aut}_{\mathbb{Q}} L \simeq D_8$. We have the following classification of subgroups of D_8

$$\begin{tikzcd}
 & & \langle 1 \rangle \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle \tau \rangle \arrow[dr] & \langle \tau\sigma^2 \rangle \arrow[d] & \langle \sigma^2 \rangle \arrow[dl] \arrow[d] \arrow[dr] & \langle \tau\sigma \rangle \arrow[d] & \langle \tau\sigma^3 \rangle \arrow[dl] \\
 & \langle \tau, \sigma^2 \rangle \arrow[dr] & \langle \sigma \rangle \arrow[d] & \langle \tau\sigma, \sigma^2 \rangle \arrow[dl] & \\
 & & \langle \sigma, \tau \rangle & &
\end{tikzcd}$$

The corresponding intermediate extensions are :

$$\begin{tikzcd}
 & & \mathbb{Q}(\alpha, i) & & \\
\mathbb{Q}(\alpha) \arrow[urr] & \mathbb{Q}(\alpha i) \arrow[ur] & \mathbb{Q}(i, \alpha^2) \arrow[u] & \mathbb{Q}(\alpha - i\alpha) \arrow[ul] & \mathbb{Q}(\alpha + i\alpha) \arrow[ull] \\
 & \mathbb{Q}(\alpha^2) \arrow[ul] \arrow[u] \arrow[ur] & \mathbb{Q}(i) \arrow[u] & \mathbb{Q}(i\alpha^2) \arrow[ul] \arrow[u] \arrow[ur] & \\
 & & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}$$

To compute fixed subfields L^H of a given subgroup H of $\operatorname{Aut}_{\mathbb{Q}} L$, one can use linear algebra: Choose a $\mathbb{Q}$-basis for L, for each $\sigma \in H$ write the matrix A given by the K-linear map $x \mapsto \sigma(x)$ and compute the kernel of $A - I$ where I is the identity matrix. Alternatively, one can check that it is invariant and then check the degree. For example, $\tau\sigma(\alpha - i\alpha) = \tau(\alpha i + \alpha) = \alpha - \alpha i$ so $\mathbb{Q}(\alpha - i\alpha) \subseteq L^{\langle \tau\sigma \rangle}$.

$$(\alpha - i\alpha)^4 = (-2i\alpha^2)^2 = -4a$$

so $[\mathbb{Q}(\alpha - i\alpha) : \mathbb{Q}] \leq 4$. On the other hand, if $i \in \mathbb{Q}(\alpha - i\alpha)$ then $\alpha = (\alpha - i\alpha + i(\alpha - i\alpha))/2$ implies $L = \mathbb{Q}(\alpha - i\alpha)$ which would imply $8 = [L : \mathbb{Q}] \leq 4$ a contradiction. Therefore $[L : \mathbb{Q}(\alpha - i\alpha)] = 2$ and hence $[\mathbb{Q}(\alpha - i\alpha) : \mathbb{Q}] = 4$. Since $[L^{\langle \tau\sigma \rangle} : \mathbb{Q}] = [\langle \sigma, \tau \rangle : \langle \tau\sigma \rangle] = 4$ we conclude $\mathbb{Q}(\alpha - i\alpha) = L^{\langle \tau\sigma \rangle}$.

[a] There should be a way to do this without using $\mathbb{R}$ but this is probably the easiest way.

5 Cyclotomic extensions, Kummer extensions, Radical extensions

6 Finite fields

7 Frobenius lifts and existence of non-solvable quintic