Definition 0.1. Extension Splitting a Polynomial.

Let $\iota : K \to L$ be a field extension, f a polynomial over K. Then (L, ι) **splits** f when there exists degree 1 polynomials $(r_i)_{i \in \deg f} \in L[X]$ such that

$$\bar{\iota} f = \prod_{i \in \deg f} r_i$$

Equivalently, there exists elements $(a_i)_{i \in \deg f} \in L, \lambda \in K$ such that

$$\bar{\iota} f = \iota(\lambda) \prod_{i \in \deg f} (X - a_i)$$

If the extension is clear, we just say L splits f or L contains all the roots of f.

Exercise. Degree Bounds Number of Roots.

Let f be a polynomial over a field K. Show that an element $a \in K$ is a root if and only if $(X - a) \mid f$. Let $S_f := \{a \in K \mid f(a) = 0\}$ be the set of roots of f. Hence show that $|S_f| \leq \deg f$.

This shows that for the definition of a polynomial splitting, we did not have to assume it factorises into exactly $\deg f$ *many degree 1 polynomials.*

Lemma 0.2. *Splitting Minimal Polynomials Lifts up.*

Let $K \overset{\iota_0}{\to} L \overset{\iota_1}{\to} M$ be field extensions, $a \in M$ algebraic over K. Then M splits $\min(a, K)$ *implies M splits* $\min(a, L)$.

Proof. We have the following situation.

$$\begin{tikzcd}
K[X] \arrow[r, "\bar{\iota}_0"] & L[X] \arrow[r, "\bar{\iota}_1"] & M[X] \arrow[d, "ev_a"] \\
K \arrow[r, "\iota_0"] & L \arrow[r, "\iota_1"] & M
\end{tikzcd}$$

By definition, $0 = \bar{\iota}_1(\bar{\iota}_0 \min(a, K))(a)$ i.e. $\bar{\iota}_0 \min(a, K)$ is a polynomial over L that has a as a root. So $\min(a, L) \mid \bar{\iota}_0 \min(a, K)$, which implies $\bar{\iota}_1 \min(a, L) \mid \bar{\iota}_1(\bar{\iota}_0 \min(a, K))$. Since M splits $\min(a, K)$,

$$\bar{\iota}_1(\bar{\iota}_0 \min(a, K)) = \prod_{i \in \deg(\min(a,K))} r_i$$

where $r_i \in M[X]$ are polynomials of degree 1. So there exists a polynomial f over M such that

$$f \bar{\iota}_1 \min(a, L) = \prod_{i \in \deg(\min(a,K))} r_i$$

Clearly, the degree 1 polynomials r_i are irreducible. So by unique factorisation, there is a subset $I \subseteq \deg(\min(a, K))$ such that

$$\bar{\iota}_1 \min(a, L) = \prod_{i \in I} r_i$$

where the r_i may have been reordered and scaled by units. Clearly, the r_i are still degree 1. To see that $|I| = \deg f$, note that I is finite and apply degree of product is sum of degrees. □

Remark. Previously, we showed that for an extension $\iota : K \to L$ with $a \in L$ algebraic over K, $K(a) \cong K[X]/(\min(a, K))$ where $\min(a, K)$ is irreducible. This assumed the existence of a larger field L inside which a sits. We now do the reverse: Given a (monic) irreducible polynomial f over K, we will create a larger field in which we have an element a which has f as its minimal polynomial.

Lemma 0.3. *Quotienting by an Irreducible Element gives a Field.*

Let f be a irreducible polynomial over K. Then the quotient $K[X]/(f)$ is a field and hence a finite extension of K.

For $g \in K[X]$, let $\bar{g}$ denote the image of g in the quotient. Then $f = \lambda \min(\bar{X}, K)$ where $\lambda \in K^\times$. In particular, if f was monic, it would be the minimal polynomial of $\bar{X}$.

Proof. Let $\bar{g} \in K[X]/(f)$. Then by irreducibility of f, $f \mid g$ or $(f, g) = 1$. If $f \mid g$, then $g \in (f)$ and hence $\bar{g} = \bar{0}$ in the quotient. If $(f, g) = 1$, then there exists polynomials $\alpha, \beta \in K[X]$ such that $\alpha f + \beta g = 1$. Thus by projecting to the quotient, $\bar{\beta}\bar{g} = \bar{1}$, i.e. $\bar{g}$ is a unit in the quotient. We just showed all elements in the quotient is either zero or a unit. So $K[X]/(f)$ is a field. By the division algorithm, $\{\bar{1}, \bar{X}, \ldots, \bar{X}^{\deg f - 1}\}$ is a basis of $K[X]/(f)$ as a K-vector space so this is a finite extension of K.

It is easy to show that f is a constant multiple of the minimal polynomial of $\bar{X} \in K[X]/(f)$. □

Exercise. Alternative Proof.

Let f be a irreducible polynomial over K, (f) the ideal generated by f. Show that for any ideal I that contains (f), $I = (f)$ or $I = K[X]$. Hence deduce from the 3rd isomorphism theorem that $K[X]/(f)$ is a field.

*In general, ideals such that the only ideals containing it are itself and the entire ring are called **maximal ideals**. These are precisely the ideals whose quotient ring are fields.*

Example 0.4. The polynomial $X^2 + 1$ is irreducible over $\mathbb{R}$. Taking the quotient ring, let i denote $\bar{X}$ in $\mathbb{R}[X]/(X^2 + 1)$. Then the quotient is what we call $\mathbb{C}$.

Remark. The above lemma is an example of how quotients are used to "set things to zero", forcing desired properties. Specifically, we took a polynomial f which previously is not equal to zero, and we set it to zero, thus making "X" a root of f.

Remark. We now show that for any polynomial, there is an extension where it splits.

Theorem 0.5. *Existence of Finite Extensions Splitting any Polynomial.*

Let f be a polynomial over a field K. Then there exists a finite extension $\iota : K \to L$ that splits f.

Proof. The idea is to repeatedly apply our previous lemma. We proceed by induction on the degree of f. Assume the theorem is true for polynomials with degree less than n. Let $\deg f = n$. By unique factorisation, there exists irreducible polynomials $r_1, \ldots, r_m$ over K such that $f = r_1 \cdots r_m$. By applying the previous lemma on r_1, there exists a finite extension $\iota_0 : K \to L$ such that there is a root of r_1, a_1. In other words, $(X - a_1) \mid \bar{\iota} r_1$, which gives $(X - a_1) \mid \bar{\iota}_0 f$, i.e.

$$\bar{\iota}_0 f = (X - a_1) g$$

Clearly, $\deg g < n$. So by assumption, there exists a finite extension $\iota_1 : L \to M$ such that M splits g. Then M splits f and is a finite extension by the Tower Law. This completes the induction. □

Definition 0.6. Splitting Field of a Polynomial.

Let f be a polynomial over a field K. A K-extension $\iota : K \to L$ is called a **splitting field of** f when L splits f and L is generated by the roots of f.

Note that splitting fields are automatically finite extensions.

Example 0.7. Let $f = X^2 - 2$ the polynomial over $\mathbb{Q}$. Then the extension $\mathbb{Q} \to \mathbb{R}$ is *not* a splitting field of f whilst the extension $\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ is.

Remark. We will now proceed to show that a splitting field of a polynomial is in a sense the *smallest* field that splits that polynomial.

Definition 0.8. Galois Conjugates.

Let $\iota_L : K \to L, \iota_M : K \to M$ be K-extensions and $a \in L, b \in M$ be elements algebraic over K. Then a, b are called **galois conjugates** when any of the following equivalent statements are true:

1. b is a root of $\min(a, K)$.
2. $\min(a, K) = \min(b, K)$.

This forms an equivalence relation on algebraic elements in K-extensions.

Example 0.9.

1. Let $\mathbb{R} \to \mathbb{C}$ be the usual extension. Then i and $-i$ are galois conjugates.
2. Let $\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ be the usual extension. Then $\sqrt{2}$ and $-\sqrt{2}$ are conjugates.
3. Let $\mathbb{Q} \to \mathbb{Q}(\omega)$ where $\omega = \exp(2\pi i/3)$. Then 1 and ω are *not* galois conjugates even though both are roots of $X^3 - 1$. The mistake is that $X^3 - 1$ is not the minimal polynomial of ω, it is $X^2 + X + 1$.

Lemma 0.10. *Embedding Simple Extensions via Conjugates.* [*]

Let $\iota : K \to K(a)$ be a simple K-extension where a is algebraic over K. Let $\iota_M : K \to M$ be another K-extension. Then for any K-extension morphism $f : K(a) \to M$, $f(a)$ is a galois conjugate of a. Hence the map $f \mapsto f(a)$ gives a bijection between the K-extension morphisms $K(a) \to M$ and the galois conjugates of a in M.

$$\{f : K(a) \to M \mid f \ K\text{-extension morphism}\} \leftrightarrow \{b \in M \mid b \text{ galois conjugate to } a\}$$

In particular, the number of such morphisms equals $\deg \min(a, K) = [K(a) : K]$ if and only if M contains all the roots of $\min(a, K)$ and they are distinct.

Proof. Let $f : K(a) \to M$ be a K-extension morphism. Then the fact that $f(a)$ is a galois conjugate of a just comes from the property of the evaluation morphism,

$$\bar{\iota}_M \min(a, K)(f(a)) = ev_{f(a)}(\bar{\iota}_M \min(a, K)) = ev_{f(a)}(\bar{f}(\bar{\iota} \min(a, K))) = ev_a(\bar{\iota} \min(a, K)) = 0$$

So the function $f \mapsto f(a)$ is well-defined.

To prove injectivity, note that $K(a)$ being a simple extension with a algebraic implies $\{a^i\}_{i \in \deg \min(a,K)}$ is a basis of $K(a)$. $f : K(a) \to M$ is K-extension morphism implies it is a K-vector space morphism. Hence f is determined by its image on the basis elements. What's more, since f is a ring morphism, $f(a^i) = f(a)^i$ implies f is determined entirely by $f(a)$. This proves injectivity.

Surjectivity is a consequence of the form of $K(a)$. Let $b \in M$ be a galois conjugate of a. Then $\min(b, K) = \min(a, K)$ implies

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

This composition of ring isomorphisms is a K-extension morphism $f : K(a) \to K(b) \subseteq M$ that maps a to b. ∎

Remark. We extend the previous result to finite extensions.

Theorem 0.11. *Embedding Finite Extensions via Conjugates.*

Let $\iota_L : K \to L$ be a finite extension, i.e. (by picking a basis) there exists finitely many elements $a_1, \ldots, a_n \in L$ such that $L = K(a_1, \ldots, a_n)$. Let $\iota_M : K \to M$ be another extension, such that for all a_i generators of L, M splits $\min(a_i, K)$. Then there exists a K-extension morphism $\iota : L \to M$. Furthermore, the number of such K-extension morphisms is less than equal to $[L : K]$ and is equal when for all generators a_i, $\min(a_i, K)$ has distinct roots in M.

Proof. For $1 \le i \le n$, let K_i denote $K(a_1, \ldots, a_i)$. The following diagram is the idea of the proof.

$$\begin{tikzcd}
K \arrow[r, "\iota_1 = \iota_L"] \arrow[d, "\iota_M"] & K(a_1) = K_1 \arrow[r, "\iota_2 = \subseteq"] \arrow[dl] & \cdots \arrow[r, "\iota_{n-1} = \subseteq"] & K_{n-1} \arrow[r, "\iota_n = \subseteq"] \arrow[dlll, "\iota_{M,n-1}"'] & K_{n-1}(a_n) = K_n = L \arrow[dllll, "\iota"] \\
M
\end{tikzcd}$$

[*] The word "embedding" is synonymous to injecting/injection.

Since $K_{i-1}(a_i) = K_i$, we can break the extension $\iota_L : K \to L$ into a chain of simple extensions and proceed by induction on the number of generators. The base case of one generator, i.e. a simple extension, is covered by the previous lemma.

Assume the theorem is true for $n-1$ generators. Let $\iota_{M,n-1}$ be one of the K-extension morphisms from K_{n-1} to M. Since M splits $\min(a_n, K)$, it also splits $\min(a_n, K_{n-1})$. So by applying the previous lemma to the simple extension $\iota_n : K_{n-1} \to K_n$, we obtain a K_{n-1}-extension morphism $\iota : K_n \to M$. ι is clearly a K-extension morphism and there are less than or equal $[K_n : K_{n-1}]$ of ι's, equal if $\min(a_n, K_{n-1})$ has distinct roots in M. Since we had at most $[K_{n-1} : K]$ many $\iota_{M,n-1}$ to choose from, by the Tower Law, we have at most

$$[K_n : K_{n-1}][K_{n-1} : K] = [K_n : K]$$

many morphisms ι arising in this way.

We show that all K-extension morphisms from K_n to M arise from applying the previous lemma to $K_{n-1} \to K_n$. Let $\iota : K_n \to M$ be a K-extension morphism. This gives a K_{n-1}-extension $\iota\big|_{K_{n-1}} : K_{n-1} \to M$ by restricting to the subfield K_{n-1}. So the restriction $\iota\big|_{K_{n-1}}$ must be one of the at most $[K_{n-1} : K]$ many morphisms of K-extensions and ι becomes one of the at most $[K_n : K_{n-1}]$ many morphisms of K_{n-1}-extensions from $\iota_n : K_{n-1} \to K_n$ to $\iota\big|_{K_{n-1}} : K_{n-1} \to M$. Thus it must be one of the at most $[K_n : K]$ many morphisms we already have.

Suppose for all generators a_m, $\min(a_m, K)$ has distinct roots in M. Clearly, $\min(a_n, K)$ having distinct roots in M implies $\min(a_n, K_{n-1})$ has distinct roots in M, and hence we have exactly $[L : K]$ many ι's. This concludes the induction. □

Theorem 0.12. *Minimal Property of Splitting Field.*

Let f be a polynomial over K and $\iota_L : K \to L$ a splitting field of f. Then L is the smallest *extension splitting f, in the sense that for any K-extension $\iota_M : K \to M$ that splits f, there exists a K-extension morphism $\bar{\iota}_M : L \to M$. Diagrammatically,*

$$\begin{tikzcd}
 & L \arrow[dd, "\bar{\iota}_M"] \\
K \arrow[ur, "\iota_L"] \arrow[dr, "\iota_M"'] & \\
 & M
\end{tikzcd}$$

In particular, we also have uniqueness up to isomorphism, that is if M is also a splitting field of f, then M, L are isomorphic as K-extensions.

Proof. Let $\iota_M : K \to M$ be an extension that splits f. For any a root of f, $\min(a, K) \mid f$ implies M splits $\min(a, K)$. So by embedding finite extensions via conjugates, we get a morphism of K-extensions $\bar{\iota}_M : L \to M$. In particular, $\bar{\iota}_M$ is an injective morphism of K-vector spaces. If M is a splitting field of f, then it is a finite extension. So $\dim_K L \le \dim_K M$. By the same argument on M, $\dim_K M \le \dim_K L$. Hence $\bar{\iota}_M$ must be bijective, implying it is an isomorphism of K-extensions. □

Remark. We conclude with a very special property of splitting fields, which we will further explore in the next section.

Theorem 0.13. *Image Invariance of Splitting Fields.*

Let f be a polynomial over K and $\iota_L : K \to L$ the splitting field of f. Then for all K-extensions $\iota_M : K \to M$ and K-extension morphisms $\phi, \psi : L \to M$, $\phi L = \psi L$.

Proof. Let $\{a_i\}_{i \in \deg f}$ be the roots of f in L. Since L is the splitting field of f, $\{a_i\}_{i \in \deg f}$ generates L, and hence $\{\phi(a_i)\}_{i \in \deg f}$ generates ϕL. By the same argument, $\{\psi(a_i)\}_{i \in \deg f}$ generates ψL. We will show that the two sets of generators are the same.

Since the following argument is completely symmetrical, it suffices to show that for all $i \in \deg f$, there exists $j \in \deg f$ such that $\phi(a_i) = \psi(a_j)$. This is surprisingly just a consequence of the basic properties of the evaluation morphism and induced ring morphisms on polynomial rings. The situation is this,

$$\begin{tikzcd}
& L \arrow[dd, shift right, "\psi"'] \arrow[dd, shift left, "\phi"] & L[X] \arrow[l, "ev_{a_i}"'] \arrow[dd, shift right, "\bar{\phi}"'] \arrow[dd, shift left, "\bar{\psi}"] & \\
K \arrow[ur, "\iota_L"] \arrow[dr, "\iota_M"'] & & & K[X] \arrow[ul, "\bar{\iota}_L"'] \arrow[dl, "\bar{\iota}_M"] \\
& M & M[X] \arrow[l, "ev_{\phi(a_i)}"] &
\end{tikzcd}$$

By definition, L splits f, that is, there exists a $\lambda \in K$ such that

$$\bar{\iota}_L f = \iota_L(\lambda) \prod_{i \in \deg f} (X - a_i)$$

This implies

$$(\overline{\psi \circ \iota})(f) = \bar{\psi}(\bar{\iota}(f)) = \psi(\iota_L \lambda) \prod_{i \in \deg f} (X - \psi(a_i))$$

Now since $\phi \circ ev_{a_i} = ev_{\phi(a_i)} \circ \bar{\phi}$ and a_i is a root of f, we have

$$0 = \phi(0) = \phi(ev_{a_i}(\bar{\iota}_L f)) = ev_{\phi(a_i)}(\bar{\phi}(\bar{\iota}_L(f))) = ev_{\phi(a_i)}((\overline{\phi \circ \iota_L})(f))$$

i.e. $\phi(a_i)$ is a root of f. But of course, since ϕ and ψ are K-extension morphisms, $\phi \circ \iota_L = \iota_M = \psi \circ \iota_L$. And hence,

$$0 = ev_{\phi(a_i)}((\overline{\psi \circ \iota_L})(f)) = ev_{\phi(a_i)}(\psi(\iota_L \lambda) \prod_{i \in \deg f} (X - \psi(a_i))) = \psi(\iota_L \lambda) \prod_{j \in \deg f} (\phi(a_i) - \psi(a_j))$$

which by K being an integral domain gives $\phi(a_i) = \psi(a_j)$ for some j, finishing the proof. $\square$