Corollary: If K is a field and S is a set of polynomials of positive degree in $K[x]$, then there exists a splitting field of S over K.

Proof: Let X be the set of all roots of elements of S, note X is a subset of the algebraic closure F of K. Then $K(X)$ is the splitting field of S over K.

Splitting fields and algebraic closures are unique.

Theorem: Suppose K, L are fields, $S \subset K[x]$, $\sigma : K \longrightarrow L$ an isomorphism and $\sigma S \subset L[x]$ the image of S. If F is the splitting field of S over K and M is the splitting field of σS over L, then σ extends to an isomorphism $F \simeq M$.

Proof: Let us suppose that S is finite, in which case we can assume that $S = \{f\}$ where $f(x) \in K[x]$. We will proceed by induction on $[F:K] = n$.

If $n=1$ then $F = K$ and f splits over K, and therefore σf splits over L, and hence $L = M$. Thus $\sigma : K \to L$ is the homomorphism we need to conclude in this case.

If $n > 1$, then f must have at least one irreducible factor g with $\deg g > 1$. Let $u \in F$ be a root of g. Since $\sigma : K \longrightarrow L$ is an isomorphism, σg is irreducible in $L[x]$.

Now if v is a root of σg in M, then $\sigma : K \to L$ will extend to an isomorphism

$$\sigma : K(u) \longrightarrow L(v)$$

with $\sigma(u) = v$ (recall the isomorphism is $h(u) \longmapsto \sigma h(v)$).

Then as $[K(u):K] = \deg g > 1$, $[F : K(u)] < n$. Now apply the induction hypothesis:

One can check that F is a splitting field of f over $K(u)$ and that M is a splitting field of σf over $L(v)$, so by the induction hypothesis $\sigma : K(u) \xrightarrow{\sim} L(v)$ extends to $\sigma : F \xrightarrow{\sim} M$ (an isomorphism)

If S is infinite, one can use either Zorn's lemma or transfinite induction to set up a proof.

Corollary: If K is a field and $S \subset K[x]$, then any two splitting fields of S over K are K-isomorphic. In particular, any two algebraic closures are isomorphic.

Proof: Apply the previous theorem with $\sigma = id_K$. The uniqueness of algebraic closures follows from the characterization of the algebraic closure as the splitting field over K of

$$S = \{ f \in K[x] \mid f \text{ is irreducible} \}.$$

In order to address fields in complete generality, we have to now split our considerations into two cases: characteristic zero and characteristic $p>0$.

Recall: The characteristic of a field is the integer $p>0$ such that

$$\underbrace{1+1+\dots+1}_{p \text{ summands}} = 0 \qquad (p \text{ prime, it turns out}).$$

or we say the characteristic is zero if no such p exists.

Definition: Let K be a field and $f\in K[x]$ irreducible. Then f is said to be separable if in some splitting field of f over K every root of f is a simple root (no repeated roots).

If $K\subseteq F$ fields and $u\in F\setminus K$, then u is called separable ~~of~~ over K if its minimal poly is separable. If every $u\in F$ is separable over K, F is called a separable extension.

Remarks: • There is a theorem:

Theorem: An irreducible polynomial $f\in K[x]$ is separable iff its derivative is nonzero.

Proof: Suppose f is not separable, so $f(x)=(x-c)^m g(x)$ where $m>1$. Then

$$f'(x) = m(x-c)^{m-1}g(x) + (x-c)^m g'(x)$$

So we observe that $f'(c)=0$ whenever $f(c)$ is not a simple root. We will use this shortly.

Now suppose $f' \neq 0$, and let u be a root of f in the splitting field for f over K. Then up to scalars, f is the minimal polynomial for u over K so $\deg f' < \deg f$ $\Rightarrow f'(u) \neq 0$ (f' is not the minimal poly). So u is a simple root of f, and f is separable.

On the other hand suppose f is separable, it's easy by direct calculation to show $f' \neq 0$.

Something that may make the previous theorem seem funny is if you are thinking only of fields of characteristic zero. E.g. if char $K=0$ then every irreducible polynomial has nonzero derivative so every irreducible polynomial is separable.

It is "hard" to cook up inseparable irreducible polynomials:

Example: (Char $K=3$).

Let $K = \mathbb{Z}_3(t)$. Then $K/(t) \simeq \mathbb{Z}_3$, so (t) is maximal, hence prime, so t is prime.

So Eisenstein $\Rightarrow f(x) = x^6 + tx^3 + 2t$ is irreducible in $K[x]$.

Yet one can show that f splits as $f(x) = (x-\alpha)^3(x-\beta)^3$; and indeed $f'(x) = 6x^5 + 3tx^2 = 0$ in $\mathbb{Z}_3(t)[x]$.

Remark: · Our definition of separability of extensions requires that the extension be algebraic, this is not true in general (other books do not require this).

Our goal in stating the next theorem is to characterize Galois extensions in terms of separability. We will state the theorem in full generality, but only prove it fully in the case when $[F:K]$ is finite.

Theorem: If $K \subseteq F$ are fields, then TFAE:

(i) F is algebraic and Galois over K

(ii) F is separable over K and F is the splitting field of some set $S \subset K[x]$ of polynomials

(iii) F is the splitting field of a set $S \subset K[x]$ of separable polynomials.

Proof:

Assuming (i), we can proceed (verbatim) as in the proof of

$$E/K \text{ Galois + algebraic} \Longrightarrow E \text{ stable}$$

in order to show that every $u \in F \setminus K$ has a minimal polynomial with distinct roots in F. Thus every $u \in F$ is separable.

If $\{v_i\}_{i \in I}$ is a basis for F over K, then writing f_i for the minimal polynomial of v_i over K we can take $S = \{f_i\}_{i \in I}$. Then f is the splitting field of S over K, proving (i) $\Rightarrow$ (ii).

Assume (ii). To show (iii), suppose $f \in S$ and let $g \in K[x]$ be a monic irreducible factor of f.

Since f splits in $F[x]$, g must be the minimal polynomial of some $u \in F$. Since F is separable, so is g. It follows that F is the splitting field over K of the following set:

$$S' = \{\text{monic irreducible factors of polynomials in } S\}$$

which, as we just saw, consists only of separable polynomials.

Now we show (iii) $\Rightarrow$ (i), which is true in general, but we restrict to $[F:K] < \infty$. Say $S = \{g_1, \dots, g_t\}$. We will prove $[F:K] = |\mathrm{Aut}_K F|$, by induction on $[F:K] = n$. The case of $n = 1$ is trivial, so assume $n > 1$. Then $\exists i$ such that $\deg g_i = s > 1$, say $i = 1$ for simplicity.

Then if u is a root of g_1, $[K(u):K] = \deg g_1 = s$ and g_1 has s distinct roots (it's separable). Set $H = \mathrm{Aut}_{K(u)} F$. We saw in a previous proof that the map

$$\begin{tikzcd}
\left\{\begin{matrix}\text{cosets of } H \\ \text{in } \mathrm{Aut}_K F\end{matrix}\right\} \arrow[r] & \left\{\begin{matrix}\text{roots of } g_1 \\ \text{in } F\end{matrix}\right\} \\
\sigma H \arrow[r, mapsto] & \sigma(u)
\end{tikzcd}$$

is injective, so

$$|\mathrm{Aut}_K F : H| \leq s.$$

In this case, however, the map is also <u>surjective</u>!

To see this:

Now suppose $v \in F$ is another root of g_1. There is an isomorphism $\tau : K(u) \longrightarrow K(v)$ with $\tau(u) = v$ and $\tau(k) = k \ \forall k \in K$. Since F is the splitting field of $\{g_1, \dots, g_t\}$ considered as polynomials over $K(u)$ or $K(v)$, τ extends to an automorphism $\tau : F \longrightarrow F$ with $\tau(u) = v$ (by a theorem from last day). This means that $\tau \in \text{Aut}_K F$ gives a coset τH such that $\tau H \longmapsto \tau(u) = v$, so we have surjectivity. Thus $|\text{Aut}_K F : H| = s$.

Now we finish by invoking the induction hypothesis:

F is the splitting field over $K(u)$ of all irreducible factors $h_j \in K(u)[x]$ of the g_i's, and the h_j's are all separable since they divide the g_i's. Then as $[F : K(u)] = n/s < n$, by induction $[F : K(u)]$

$$= |\text{Aut}_{K(u)} F| = |H|.$$

So we can calculate:

$$\begin{aligned} [F : K] = [F : K(u)][K(u) : K] &= |H| \cdot s \\ &= |H| \cdot |\text{Aut}_K F : H| \\ &= |\text{Aut}_K F|. \end{aligned}$$

So the extension is Galois, and (i) holds.

Remark: If we assume $[F:K]<\infty$ in the statement of the theorem, then we can replace our characterization of Galois extensions with something simpler:

Instead of saying that every Galois extension is the splitting field of some collection of separable polynomials, (iii) becomes: It is the splitting field of a single ~~separable polynomial~~ polynomial whose irreducible factors are separable.

Our next goal: Remove the reference to splitting fields in our characterization of Galois extensions, by directly referencing the essential property of splitting fields that we need. This property is as follows:

Definition: An algebraic extension F is normal over K (or is a normal extension) if every irreducible polynomial having at least one root in F actually splits in $F[x]$.

E.g. - Every splitting field of a polynomial turns out to be normal

- Algebraic closures are clearly normal
- The extension $\mathbb{Q}(2^{1/4})$ of $\mathbb{Q}$ is not normal: The polynomial x^4-2 is irreducible over $\mathbb{Q}$, but $\mathbb{Q}(2^{1/4})$ contains only real numbers so does not contain the roots $\pm 2^{1/4} i$ of x^4-2.

Theorem 3.14: If F is an algebraic extension of K, TFAE:

(i) F is normal over K,

(ii) F is the splitting field over K of some set of polynomials in $K[x]$.

(iii) If $\overline{K}$ is any algebraic closure of K containing F, then for any injective $\sigma : F \longrightarrow \overline{K}$ with $\sigma(k) = k \; \forall k \in K$ we have $\operatorname{im}\sigma = F$, so σ is actually an automorphism of F fixing K.

Proof: (i) $\Rightarrow$ (ii).

Suppose F is normal over K, and let $\{u_i\}_{i\in I}$ be a basis of F over K. Let f_i be the minimal polynomial of u_i $\forall i \in I$, and observe that F is the splitting field of $\{f_i\}_{i\in I}$ over K.

(ii) $\Rightarrow$ (iii). Suppose F is the splitting field over K of $\{f_i\}_{i\in I}$. Let $\sigma : F \longrightarrow \overline{K}$ be as in the statement of (iii).

Observe that if $u \in F$ is a root of some f_j, then so is $\sigma(u)$ since σ fixes the elements of K (and thus the coefficients of f_j). Since f_j splits in F, we may suppose

$$f = c\,(x-u_1)\cdots(x-u_n) \text{ where } c \in K \text{ and } u_i \in F.$$

Since $\overline{K}[x]$ is a UFD, $\sigma(u_j)$ must be equal to one of $u_1, \ldots, u_n$ for each i. Since σ is injective, σ must therefore permute the u_i.

As this holds for all polynomials f_j in our collection $\{f_i\}_{i \in I}$, and since F is the splitting field of $\{f_i\}_{i \in I}$ we know F is generated over K by the roots of the f_i's. Since σ permutes this collection of roots, $\sigma(F) = F$ and so $\sigma \in \mathrm{Aut}_K F$.

(iii) $\Rightarrow$ (i).

Suppose (iii) holds, and let $f \in K[x]$ be irreducible and $u \in F$ a root of $f(x)$. Then $\overline{K}$ contains all the roots of f, and if $v \in \overline{K}$ is any other root then there's a K-isomorphism $K(u) \cong K(v)$ with $u \mapsto v$. Call this isomorphism $\sigma : K(u) \longrightarrow K(v)$.

By a previous theorem (proved on Monday), σ extends to an automorphism $\sigma : \overline{K} \longrightarrow \overline{K}$. Then $\sigma|_F : F \longrightarrow \overline{K}$ is injective, and so our assumptions (we're assuming (iii) holds) give $\sigma(F) = F$. But then $u \in F \Rightarrow \sigma(u) = v \in F$.

As this holds for any other root $v \in \overline{K}$, in fact f must split in $F[x]$. So F is normal over K.

Corollary: Suppose F is algebraic over K. Then:

F is Galois over $K \iff F$ normal and separable over K.

If $\operatorname{char} K = 0$, then this gives:

F is Galois over $K \iff F$ is normal over K.

Proof: Combine the two previous theorems. We saw

Galois over K $\iff$ F separable over K and F is a splitting field of some $S \subset K[x]$

and the underlined condition is equivalent to normality.

When $\operatorname{char} K = 0$, every irreducible polynomial in $K[x]$ is separable. Thus F algebraic over $K \Rightarrow F$ is separable, since for every $u \in F$ the minimal polynomial of u over K is irreducible $\Rightarrow$ separable.

§5.4 Galois group of a polynomial.

Our goal now is to analyze the Galois groups, their subgroups, and the intermediate fields that arise from splitting fields of separable polynomials.

Definition: The Galois group of $f \in K[x]$ is the group $\mathrm{Aut}_K F$ where F is a splitting field of f over K.

We will use the following terminology in the next theorem: A subgroup H of the symmetric group S_n is said to be transitive if for every pair of distinct integers i, j with $1 \leq i, j \leq n$ there exists $\sigma \in H$ with $\sigma(i) = j$.

Theorem: Suppose that $f \in K[x]$ has Galois group G. Then:

(i) G is isomorphic to a subgroup of S_n for some n

(ii) If f is irreducible and separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Remark: Part (i) of this theorem really says nothing, since every finite group is isomorphic to a subgroup of S_n for some n and we know $|G| < \infty$. The interesting thing behind (i) is how we arrive at the conclusion that $G \cong H < S_n$.

Proof.

(i) Suppose f has distinct roots $\{u_1, \dots, u_n\}$ in some splitting field. Then every $\sigma \in \mathrm{Aut}_F K$ induces a permutation of $\{u_1, \dots, u_n\}$, and the action of σ on this set completely determines the action of σ on the splitting field $K(u_1, \dots, u_n)$. Thus if S_n is the group of permutations of $\{u_1, \dots, u_n\}$, this gives an injective homomorphism $G \longrightarrow S_n$.

(ii) From our setup, F is Galois over K, and if u_1 is a root of f then $[K(u_1) : K] = n = \deg f$ since f is the minimal poly of u_1 over K. But the fundamental theorem of Galois theory then says $[K(u_1) : K] = |\mathrm{Aut}_K F : K(u_1)'| = n$, so $n \mid |G|$. Next, For any two roots u_i, u_j there's an isomorphism $\sigma : K(u_i) \longrightarrow K(u_j)$ s.t. $\sigma(u_i) = u_j$ and this extends to an automorphism of F. Thus the correspondence $G \longrightarrow S_n$ of (i) gives a transitive subgroup of S_n.