Fields and Galois Theory

David Rufino

May 24, 2020

Contents

1 Fields and Galois Theory

Some concise notes on fields and galois theory for algebraic extensions K/k. Mainly follows LangAlgebra72 by characterizing key properties in terms of embeddings in the algebraic closure $\bar{k}$. There are a few changes

- Start with more intuitive definitions of Normal and Separable
- Don't assume that algebraic extensions are subsets of an algebraic closure, just that they have a non-canonical embedding.
- Make use of category of algebraic extensions to simplify exposition
- Include Artin's independence argument for proving key lemma $[K : K^H] \leq \#H$. This is taken largely from JMilne.

1.1 Category of field extensions

A field extension K/k is a pair $(K,\ i_{kK})$ where $i_{kK} : k \to K$ is an injective ring homomorphism (embedding). Note every field is an extension over its prime subfield ($k = \mathbb{Q}$ or $\mathbb{F}_p$) by inclusion, so we lose no generality by always considering field extensions. Then a morphism $\sigma : K/k \to L/k$ of field extensions is simply a ring homomorphism which commutes i.e. $\sigma \circ i_{kK} = i_{kL}$. This constitutes a category $\mathbf{Field}_k$. As with any category we can consider the set of morphisms

$$\mathrm{Mor}_k(K, L) := \mathrm{Mor}(K/k, L/k)$$

and the set of self-isomorphisms (automorphisms)

$$\mathrm{Aut}(K/k) \subset \mathrm{Mor}_k(K, K)\,.$$

It's easy to show that every field morphism is automatically injective

Proposition 1.1
Every element $\sigma \in \mathrm{Mor}_k(K, L)$ is automatically injective and therefore an isomorphism onto its image.

In particular $\sigma \in \mathrm{Mor}_k(K, L)$ is an isomorphism if and only if it is surjective.

Moreover for any morphisms $f : F \to K$ and $g : L \to M$ there are natural maps

$$\begin{aligned} \mathrm{Mor}_k(K, g) : \mathrm{Mor}_k(K, L) &\to \mathrm{Mor}_k(K, M) \\ \sigma &\to g \circ \sigma \end{aligned}$$

and

$$\begin{aligned} \mathrm{Mor}_k(f,L) : \mathrm{Mor}_k(K,L) &\to \mathrm{Mor}_k(F,L) \\ \sigma &\to \sigma \circ f \end{aligned}$$

When f is just inclusion, then the latter corresponds to restriction of functions. In fancy terminology $\mathrm{Mor}(-,-)$ is a bifunctor covariant in second argument and contravariant in the first.
We may also consider a "tower" of extensions

$$K_n/\ldots/K_0 = k$$

with embeddings $i_{K_iK_{i+1}} : K_i \to K_{i+1}$, with the picture that these usually correspond to inclusions. Typically if we have a family of morphisms

$$\sigma_i : K_i \to M$$

they would commute with these embeddings. In particular we may abuse notation by defining $\sigma_i|_{K_j} = \sigma_i \circ i_{K_{i-1}K_i} \circ \ldots \circ i_{K_jK_{j+1}}$.

Observe every extension K/k may be viewed as a k-vector space with $\lambda \cdot \alpha = i_{kK}(\lambda)\alpha$.

Definition 1.1
A field extension K/k is said to be finite if it has finite dimension as a k-vector space. In this case denote its dimension by $[K:k]$

In many circumstances they are also surjective, by using counting arguments.

Proposition 1.2
Let K/k be a finite field extension, then every k-embedding $\sigma : K \to K$ is automatically surjective and therefore an isomorphism.

$$\mathrm{Mor}_k(K,K) = \mathrm{Aut}(K/k)$$

Proof. This follows from results on finite vector spaces. □

1.2 Polynomials over a field

Proposition 1.3
The ring $k[X]$ is a principal ideal domain, that is every ideal has the form

$$\mathfrak{a} = (f)$$

Moreover we may choose f to be monic, and in this case it is unique.

Corollary 1.4 (UFD)
$k[X]$ is a unique factorization domain (UFD). More precisely every non-zero polynomial may be decomposed uniquely as follows

$$f = c(f)\prod_{i\in I} p_i^{v_{p_i}(f)}$$

where the p_i run over all distinct monic irreducible polynomials, $0 \neq c(f) \in k$ is the leading coefficient of f and $v_{p_i}(f)$ are non-negative integers with only finitely many non-zero so that the product is well-defined.

Proof. The fact that $k[X]$ is a UFD follows from standard results about PIDs. Note that the units of $k[X]$ are precisely the constant polynomials, so f, g are associates iff $f = \lambda g$, and every irreducible polynomial is associated to precisely one monic irreducible polynomial. Therefore we're able to determine a unique decomposition as above. □

Remark 1.2
The polynomials $(X - \alpha)$ are irreducible.

Note by uniqueness v_p satisfies

$$v_p(fg) = v_p(f) + v_p(g)$$

and furthermore

$$\deg(f) = \sum_i \deg(p_i)v_{p_i}(f)$$

The support of f is the set of irreducible polynomials for which $v_p(f)$ is non-zero.

Lemma 1.5 (Divisibility)
f divides g iff $v_p(f) \leq v_p(g)\ \forall p$ iff $(g) \subseteq (f)$

Lemma 1.6 (Roots and Multiplicity)
For $f \in k[X]$ a non-constant polynomial and $\alpha \in k$ we have

$$f(\alpha) = 0 \iff (X-\alpha) \mid f \iff v_{(X-\alpha)}(f) > 0$$

In this case $r := v_{(X-\alpha)}(f)$ is the multiplicity of the root α, and observe

$$f(X) = c(X-a)^r g(X)$$

with $g(\alpha) \neq 0$ (equivalently $v_{(X-\alpha)}(g) = 0$).

Proof. The right to left implication is obvious. Conversely by the division algorithm we may write

$$f(X) = f(\alpha) + (X-\alpha)Q(X)$$

Then if $f(\alpha) = 0$ we clearly have $v_{(X-\alpha)}(f) > 0$. Finally we may construct

$$g(X) = \prod_{p \neq (X-\alpha)} p^{v_p(f)}$$

It's clear that for every p appearing in the product $p(\alpha) \neq 0$ because otherwise we would have $(X-\alpha) \mid p$ and by irreducibility $(X-\alpha) = p$. Therefore $g(\alpha) \neq 0$ as required. □

Definition 1.3
Let $\sigma : K \to L$ be a field morphism and $f \in K[X]$ such that

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n$$

then define $f^\sigma \in L[X]$ by

$$f^\sigma(X) := \sigma(a_0) + \sigma(a_1)X + \ldots + \sigma(a_n)X^n$$

Note this has the property that

$$f^\sigma(\sigma(\alpha)) = \sigma(f(\alpha)) \quad \forall \alpha \in K$$

In the case of a field extension K/k we may abuse notation by writing $f^{i_{kK}}$ as simply f.

Definition 1.4 (Splitting Polynomial)
Let K/k be a field extension and $f \in k[X]$. We say a polynomial f splits completely in K if the irreducible decomposition of f^i in $K[X]$ is

$$f^i(X) = c(f^i)\prod_{i=1}^{n}(X-\alpha_i)^{r_i}$$

where α_i are the distinct roots of $f(X)$ in K and $r_i := v_{(X-\alpha_i)}(f^i)$ are the multiplicities. Equivalently f splits in K if

$$p \in K[X] \text{ irreducible } \wedge \deg(p) > 1 \implies v_p(f^i) = 0 \tag{1}$$

Observe that the number of roots counting multiplicities is $\deg(f)$

$$\deg(f) = \sum_{i=1}^{n} v_{(X-\alpha_i)}(f^i)$$

1.2.1 Separable Polynomials

NB in this section we abuse notation by identifying $f \in k[X]$ and $f^{i_{kK}} \in K[X]$

We are interested in characterizing polynomials $f \in k[X]$ which do not have multiple roots in any extension field K/k. This may be achieved by considering the formal derivative $f'(X)$ as follows

Proposition 1.7 (Criteria for Multiple Roots)
Let $f(X) \in k[X]$ be a polynomial and either $char(k) = 0$ or $r < char(k)$. Then $\alpha \in K$ is a root of multiplicity r precisely when

$$f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(r-1)}(\alpha) = 0$$

and $f^{(r)}(\alpha) \neq 0$.
Therefore the multiple roots are precisely the common roots of $f(X)$ and $f'(X)$ (irrespective of the characteristic).

Proof. Note that by Lemma 1.6

$$f^{(1)}(X) = (X-\alpha)^{r-1}[rg(X) + (X-\alpha)g'(X)]$$

with $g(\alpha) \neq 0$ and r the multiplicity of the root. If $r = 1$, then $f^{(1)}(\alpha) = g(\alpha) \neq 0$ as required. If $r > 1$, then $f^{(1)}(X)$ has α as a root of multiplicity $r-1$, so it follows by induction.
The second statement is simply the case $r = 1$. □

Definition 1.5 (Coprime)
We say two elements x, y of a ring are coprime if $(x, y) = (1) \iff ax + by = 1$ for some a, b

Definition 1.6
A polynomial $f \in k[X]$ is separable if f and f' are coprime.

Proposition 1.8 (Separable Polynomial)
A separable polynomial $f \in k[X]$ has no multiple roots in any extension field K/k

Proof. Since $(f, f') = 1$ we have $af + bf' = 1$. Clearly f and f' have no common roots, and therefore f has no multiple roots by Proposition 1.7. □

We can provide a partial converse by working in a large enough extension field

Proposition 1.9 (Separability)
Let K/k be a field extension and $f \in k[X]$ a polynomial which splits completely in K. Then TFAE

1. *f is separable*
2. *f has no multiple roots in K*
3. *f has $\deg(f)$ distinct roots in K*

Proof. Using the formula

$$\deg(f) = \sum_{i=1}^{n} v_{(X-\alpha_i)}(f)$$

we see easily that $3 \iff 2$. The previous Proposition shows that $1 \implies 2$.

Conversely suppose f is not separable, then by Lemma 1.10 f and f' must have a non-trivial common divisor h. Using 1.5 and (1) we see that h splits in K. Any root of h is a common root of f and f' in K, which by Proposition 1.7 is a multiple root of f in K. □

We used the following

Lemma 1.10 (Co-prime elements in a PID)
Let A be a PID, then x, y are co-prime if and only if they have no non-trivial common divisors.

Proof. First suppose $(x, y) = 1$, then $ax + by = 1$ and any common divisor d must divide 1 and therefore be invertible.

Conversely suppose $(x, y) \neq (1)$, since A is a PID it must equal (d) for some non-invertible d, which by definition is a non-trivial common divisor. □

We will need the following

Lemma 1.11
If $f \mid g$ and g is separable then f is separable

Proof. By assumption we have $g = hf$ and $ag + bg' = 1$ (see). By the product rule we have $g' = h'f + hf'$. Therefore $1 = (ah)f + b(h'f + hf') = (ah + bh')f + bhf'$, so f and f' are coprime as required. □

1.3 Algebraic Extensions

Definition 1.7 (Algebraic element and Minimal Polynomial)
If K/k is a field extension we say that $\alpha \in K$ is algebraic (over k) if it satisfies

$$f^i(\alpha) = 0$$

for some polynomial $f \in k[X]$, or equivalently if the evaluation morphism

$$\phi_\alpha : k[X] \to K$$

has a non-zero kernel. There is a unique monic polynomial $m_{\alpha,k}(X)$ such that $(m_{\alpha,k}) = \ker(\phi_\alpha)$, which we call the minimal polynomial. This is irreducible. It is the unique monic polynomial such that

$$f^i(\alpha) = 0 \iff m_{\alpha,k} \mid f$$

Proof. Note that $k[X]/\ker(\phi_\alpha)$ is isomorphic to $\mathrm{im}(\phi_\alpha)$. As the image is an integral domain, being a subring of a field, the kernel must be prime. This means that $m_{\alpha,k}$ is irreducible. □

Definition 1.8 (Algebraic Extension)
A field extension K/k is algebraic if every element $\alpha \in K$ is algebraic.

A field extension K/k is simple if $K = i(k)(\alpha)$ for α algebraic.

Proposition 1.12 (f.g. algebraic $\implies$ finite)
A simple extension $K = k(\alpha)$ is finite of dimension $\deg(m_\alpha, k)$.
More generally a finitely generated algebraic extension $K = k(\alpha_1, \ldots, \alpha_n)$ is finite over k.

Proof. The first part follows from an isomorphism with $k[\alpha] = k[X]/(m_\alpha)$.
The second part follows by induction and taking simple extensions. □

This allows us to prove a stronger version of Proposition 1.2

Proposition 1.13
Let K/k be an algebraic extension then any k-embedding to itself is surjective and therefore an isomorphism. In other words

$$\mathrm{Mor}_k(K, K) = \mathrm{Aut}(K/k)$$

Proof. □

We prove the first lifting theorem

Proposition 1.14 (Lifting to simple extensions)
Let $K(\alpha)/K$ be a simple algebraic extension, and $\sigma : K \to L$ a field embedding such that $m^\sigma_{\alpha,K}$ has a root in L. Then there exists a lifting $\sigma : K(\alpha) \to L$.

More precisely the number of extensions is equal to the number of distinct roots of $m^\sigma_{\alpha,K}$ in L.

In particular if $m^\sigma_{\alpha,K}$ is separable and splits completely in L then there are precisely $\deg(m_\alpha) = [K(\alpha) : K]$ *such extensions.*

Proof. Essentially we just need that $K(\alpha)$ and $\sigma(K)(\alpha')$ are both isomorphic to the quotient ring $K[X]/(m_{\alpha,K})$. The last statement follows from Proposition 1.9. □

Corollary 1.15
Let $K(\alpha)/K$ and $K(\beta)/K$ be two simple extensions such that

$$m_{\alpha,K} = m_{\beta,K}$$

Then there exists a unique K-isomorphism

$$\sigma : K(\alpha) \to K(\beta)$$

such that

$$\sigma(\alpha) = \beta$$

Proof. The embedding $K \to K(\beta)$ extends by the previous proposition to a K-embedding $K(\alpha) \to K(\beta)$. The image is a field containing β and therefore clearly surjective. □

1.4 Galois Theory Summary

Definition 1.9 (Separable, Normal and Galois)
Let K/k be an algebraic extension. We say that K/k is

- Normal *if every minimal polynomial $m_{\alpha,k} \in k[X]$ splits completely in K*
- Separable *if every minimal polynomial $m_{\alpha,k} \in k[X]$ is separable.*
- Galois *if it is both normal and separable (iff $m_{\alpha,k}$ has* $\deg(m_{\alpha,k})$ *distinct roots in K, see Proposition 1.9).*

In the case of a Galois extension we denote the group of automorphisms by $\mathrm{Gal}(K/k)$.

To summarize the main results

1. The group of automorphism of a normal extension K/k acts transitively on the roots of a given irreducible polynomial.
2. For K/k finite we have $\#\,\mathrm{Aut}(K/k) \leq [K : k]$ with equality if and only if K/k is Galois.

3. An algebraic extension K/k is automatically separable whenever either $\text{char}(k) = 0$ or k is finite.

4. When K/k is finite and Galois then we have an order-reversing bijection between subfields and subgroups

$$\begin{aligned} \{H \leq \text{Gal}(K/k)\} &\longleftrightarrow \{F \subseteq K\} \\ \phi : H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \psi : \text{Gal}(K/F) &\longleftarrow F \end{aligned}$$

We follow the approach in Lang72 and rephrase the concepts of "Normal" and "Separable" in terms of morphisms into an algebraic closure, i.e. the set $\text{Mor}_k(K, \bar{k})$. The first requires some work to set up the algebraic closure $\bar{k}$.

1.5 Algebraic Closure

Definition 1.10 (Algebraically Closed)
A field M is algebraically closed if one of the following equivalent conditions holds

- *Every algebraic extension M'/M is trivial*
- *Every non-constant polynomial in $M[X]$ has a root in M*
- *Every non-constant polynomial in $M[X]$ splits in M*

If M is an extension field of k, then we say it is algebraically closed over k.

Definition 1.11 (Algebraic Closure)
An algebraic closure $\bar{k}$ of k is a field extension $\bar{k}/k$ which is algebraic and for which $\bar{k}$ is algebraically closed.

Proposition 1.16 (Existence of Algebraic Closure)
Given a field k there exists an algebraic closure $\bar{k}/k$

Proposition 1.17 (Generic Lifting Theorem)
Let K/k be a field extension. Suppose L/K is an algebraic extension and $\sigma : K \to M$ a k-embedding into an algebraically closed field. Then there exists an extension $\tilde{\sigma} : L \to M$. In other words there is a surjection

$$\text{Mor}_k(i_{KL}, M) : \text{Mor}_k(L, M) \to \text{Mor}_k(K, M)$$

Proof. Broadly speaking consider the poset of extensions to subfields of L ordered under consistency and take a maximal element by Zorn's Lemma. Apply Proposition 1.14 to show that this maximal element must be an extension to L.

If $[L : K] < \infty$, then we may simply proceed by induction on dimension. □

Corollary 1.18 (Unique up to isomorphism)
An algebraic closure $\bar{k}$ of k is unique up to (non-unique) isomorphism.

Remark 1.12
Note if K/k is an algebraic extension then the Proposition shows that we may consider construct an embedding $K \to \bar{k}$ commuting with $k \to \bar{k}$.

In general given a tower of algebraic extensions

$$K = k_n/\ldots/k_0 = k$$

we will assume the existence of compatible embeddings $i_{k_i} : k_i \to \bar{k}$ such that $i_{k_{i+1}} \circ i_{k_i,k_{i+1}} = i_{k_i}$.

1.6 Separability

The concept of separable extensions is important, as illustrated by Proposition 1.14. So we develop this theory further, and reinterpret it in terms of $\text{Mor}_k(k, \bar{k})$.

Proposition 1.19
Let $K/F/k$ be a tower of extensions, then K/k is separable $\iff$ K/F, F/k separable.

Proof. Suppose K/k is separable. Clearly F/k is separable. Furthermore $m_{\alpha,F} | m_{\alpha,k}$ by definition, and so the former is separable by Lemma 1.11.
Conversely TODO □

Proposition 1.20
$K = k(\alpha_1, \ldots, \alpha_n)$ is separable over k if and only if each α_i is separable over k.

Proof. □

Proposition 1.21 (Separability degree)
The cardinality of $\mathrm{Mor}_k(K, (\bar{k}, i_k))$ *is independent of the choice of embedding* $i_k : k \to \bar{k}$*. We write this as* $[K : k]_s$

Proof. Essentially if L/k and M/k are isomorphic then so are $\mathrm{Mor}_k(K, L)$ and $\mathrm{Mor}_k(K, M)$, since $\mathrm{Mor}_k(K, -)$ is a covariant functor. If L/k and M/k are two algebraic closures of k, then we have seen they are isomorphic and the result follows. □

From Proposition 1.14 we've seen that $[k(\alpha) : k]_s \leq [k(\alpha) : k]$ with equality iff α is separable iff $k(\alpha)$ is separable. We may show this more generally

Proposition 1.22 (Multiplicativity of separability degree)
If $L/K/k$ *is a tower of finite extensions then*

$$[L : k]_s = [L : K]_s [K : k]_s \,.$$

Proof. We assume compatible embeddings in $\bar{k}$. The restriction map

$$\psi := \mathrm{Mor}_k(i_{KL}, \bar{k}) : \mathrm{Mor}_k(L, \bar{k}) \to \mathrm{Mor}_k(K, \bar{k})$$

is surjective by Proposition 1.17. Consider $\sigma \in \mathrm{Mor}_k(K, \bar{k})$ then the fibre $\psi^{-1}(\sigma)$ is equal to $\mathrm{Mor}_K(L, (\bar{k}, \sigma))$. As we've noted in Proposition 1.21 the cardinality does not depend on the embedding σ, and is equal to $\#\,\mathrm{Mor}_K(L, \bar{k}) = [K : k]_s$ for all σ. As $\mathrm{Mor}_k(L, \bar{k})$ is equal to the disjoint union of all the fibres, then the result follows. □

Proposition 1.23 (Bounds on $\mathrm{Mor}_k(K, \bar{k})$)
Let K/k *be a finite extension then* $[K : k]_s \leq [K : k]$ *with equality if and only if* K/k *is separable.*

Proof. For a general finite extension we may obtain a tower of simple extensions

$$K = k_n / \ldots / k_0 = k$$

with $k_i = k_{i-1}(\alpha_i)$. We have by Proposition 1.22

$$[K : k]_s = \prod_{i=1}^{n} [k_i : k_{i-1}]_s$$

and from Proposition 1.14 that $[k_i : k_{i-1}]_s \leq [k_i : k_{i-1}] = \deg(m_{\alpha_i, k_{i-1}})$. The inequality follows from multiplicativity of extension and separability degrees.

When K/k is separable then Proposition 1.19 together with Proposition 1.14 also shows that $[k_i : k_{i-1}]_s = [k_i : k_{i-1}]$ and again we have equality by multiplicity of both degrees.

Conversely if $[K : k]_s = [K : k]$ then we must have equality at each stage, which implies α_i is separable over k_{i-1}. The choice of α_1 was arbitrary, so we see that every element of K is separable over k in this case, as required. □

Definition 1.13 (Bounds on $\mathrm{Aut}(K/k)$)
Let K/k *be an algebraic extension and* $i_K : K \to \bar{k}$ *a fixed* k*-embedding. Then there is a natural injection*

$$\begin{aligned} \mathrm{Mor}_k(K, i_K) : \mathrm{Aut}(K/k) &\to \mathrm{Mor}_k(K, \bar{k}) \\ \sigma &\to i_K \circ \sigma \end{aligned}$$

In particular in the finite case

$$\#\,\mathrm{Aut}(K/k) \leq [K : k]_s \leq [K : k] < \infty$$

If i_K *is inclusion, then we may regard* $\mathrm{Aut}(K/k)$ *as a subset of* $\mathrm{Mor}_k(K, \bar{k})$

Corollary 1.24 (Extension to algebraic closure II)
Let K/k *be an algebraic extension and* $i_K : K \to \bar{k}$ *a* k*-embedding. Then every* $\sigma : K \to \bar{k}$ *lifts to* $\sigma : \bar{k} \to \bar{k}$*. i.e. there is a canonical surjection by restriction*

$$\begin{aligned} \mathrm{Mor}_k(i_K, \bar{k}) : \mathrm{Aut}(\bar{k}/k) &\longrightarrow \mathrm{Mor}_k(K, \bar{k}) \\ \sigma &\longrightarrow \sigma \circ i_K \end{aligned}$$

When i *is inclusion then this is simply the restriction to* K*.*

Proof. Given $\sigma \in \mathrm{Mor}_k(K, \bar{k})$ there exists an extension $\tilde{\sigma} \in \mathrm{Mor}_k(\bar{k}, \bar{k})$ by Proposition 1.17 with $L = M = \bar{k}$. This is automatically an automorphism as required.

□

Corollary 1.25 (Conjugate elements)
We say $\alpha, \beta \in \bar{k}$ are conjugate if they have the same minimal polynomial.
This is the case if and only if there is an element $\sigma \in \mathrm{Aut}(\bar{k}/k)$ such that $\sigma(\alpha) = \beta$.

Proof. By Corollary 1.15 there is an isomorphism $k(\alpha) \to k(\beta)$. Corollary 1.24 gives the required automorphism. The converse is easy. □

As an application of the concept of separability degree we prove

Proposition 1.26 (Primitive Element Theorem)
Let K/k be a finite separable extension of k then $K = k(\alpha)$ is simple.

Proof. We only prove the case k is infinite. The finite case can be proven separately by showing that the $K^\star$ is cyclic.

Consider the set $\mathrm{Mor}_k(K, \bar{k}) = \{\sigma_1, \ldots, \sigma_n\}$ which by Proposition 1.23 has order $n = [K : k]$. By induction we can assume that $K = k(\alpha, \beta)$. We claim that there exists $0 \neq c \in k$ such that $\sigma_i(\alpha + c\beta)$ are all distinct. In this case we clearly have $\#\,\mathrm{Mor}_k(k(\alpha + c\beta), \bar{k}) \geq n$ so by the same result $[k(\alpha + c\beta) : k] \geq n$ whence $k(\alpha + c\beta) = K$.

We have $\sigma_i(\alpha + c\beta) = \sigma_j(\alpha + c\beta) \iff c(\sigma_i(\beta) - \sigma_j(\beta)) = (\sigma_i(\alpha) - \sigma_j(\alpha))$. Therefore consider the polynomial

$$f(X) = \prod_{i \neq j} (X(\sigma_i(\beta) - \sigma_j(\beta)) - (\sigma_i(\alpha) - \sigma_j(\alpha)))$$

Then the embeddings are distinct precisely when $f(c) \neq 0$. Since $f(X)$ has at most finitely many roots and k is infinite, there must exist such a c. □

1.7 Splitting Fields

Definition 1.14 (Splitting Field)
A field extension K/k is a splitting field for $f \in k[X]$ if f splits in K and does not in any proper subfield. Equivalently

$$K = k(\alpha_1, \ldots, \alpha_n)\,.$$

where α_i are the roots of f^i in K. Similarly K is said to be a splitting field for a family of polynomials $\{f_i\}$ if it splits every polynomial and no proper subfield does so.

A splitting field always exists

Proposition 1.27 (Existence of Splitting Fields)
Every family of polynomials has a splitting field. Moreover any two such splitting fields are k-isomorphic.

Proof. This easiest way is to assume the existence of an algebraic closure and take the smallest field under which the polynomials split. Alternatively if the family of polynomials is finite we may proceed by induction on the total degree and adjoin roots as simple extensions. This gives a bound on the total degree of the extension.

□

1.8 Perfect Fields

For large classes of base fields all algebraic extensions are separable :

Proposition 1.28 (Perfect field)
Let k be a field. Then TFAE

- *Every irreducible polynomial in $k[X]$ is separable*
- *Every algebraic extension K/k is separable*
- *$\bar{k}$ is separable*

In this case we say k is perfect.

Proposition 1.29 (Criteria for perfectness)
k is perfect if and only if one of the following holds

- *k has characteristic 0*
- *k has characteristic p and every element is a p-th power*

In particular finite fields are perfect.

1.9 Normal Extensions

We characterize normal extensions in terms of morphisms $\mathrm{Mor}_k(K, \bar{k})$. First we prove a trivial Lemma.

Lemma 1.30
Let K/k, L/k be field extensions and $\sigma : K \to L$ a k-embedding. Suppose that $f \in k[X]$ is a polynomial, then α is a root of f if and only if $\sigma(\alpha)$ is a root of f^σ.
If f splits in K, then it splits in L and i induces a bijection between the roots of f in K and L preserving multiplicity.

Proposition 1.31 (Normal Criteria)
Let K/k be an algebraic extension and $\bar{k}$ a given algebraic closure, then the following are equivalent

NOR1 *For any two k-embeddings $\sigma, \tau \in \mathrm{Mor}_k(K, \bar{k})$ we have $\sigma(K) = \tau(K)$.*

NOR2 *K is the splitting field of some family of polynomials $f_i \in k[X]$.*

NOR3 *K/k is normal (i.e. every minimal polynomial in $k[X]$ splits completely in K)*

Proof. Clearly 3 $\implies$ 2, for K is the splitting field of all the minimal polynomials of elements in K.

We show 2 $\implies$ 1. Define $T_j = \{\alpha \in K \mid f_j(\alpha) = 0\}$ and $T'_j = \{\alpha \in \bar{k} \mid f_j(\alpha) = 0\}$. By hypothesis $K = k(\cup_j T_j)$, and we claim that for any such σ we have $\sigma(K) = k(\cup_j T'_= j) =: K' \subset \bar{k}$. By Lemma 1.30 that any σ induces a bijection between T_j and T'_j. Therefore $\bigcup_j T'_j \subseteq \sigma(K) \implies K' \subseteq \sigma(K)$. Furthermore $\sigma(K) \subseteq k(\sigma(\bigcup_j T_j)) \subseteq k(\bigcup_j T'_j) = K'$ **NB last step is not entirely trivial**.

Finally we show 1 $\implies$ 3. Wlog assume $k \subset K \subset \bar{k}$. Suppose $f(X)$ is an irreducible polynomial with root $\alpha_1, \ldots, \alpha_n \in \bar{k}$ and $\alpha_1 \in K$. By Corollary 1.25 there is a morphism $\phi \in \mathrm{Aut}(\bar{k}/k)$ such that $\phi(\alpha_1) = \alpha_j$. Therefore the inclusion map i and the composite map $\phi \circ i$ must have the same image, K. Therefore $\alpha_j \in K$ as required. □

We provide some more straight-forward criteria based on a specific embedding $K \subset \bar{k}$.

Proposition 1.32 (Normal Criteria II)
Let K/k be an algebraic extension and $i_K : K \to \bar{k}$ a given k-embedding then the following are equivalent

1. *K/k is normal*
2. *Every $\sigma \in \mathrm{Mor}_k(K, \bar{k})$ has image $i_K(K)$*
3. *The embedding $\mathrm{Mor}_k(K, i_K) : \mathrm{Aut}(K/k) \to \mathrm{Mor}_k(K, \bar{k})$ (1.13) is a bijection*

When K/k is finite it's necessary and sufficient that $\#\,\mathrm{Aut}(K/k) = [K : k]_s$

Proof. 1 $\iff$ 2). This is clear by NOR1.

2 $\implies$ 3). Given $\sigma \in \mathrm{Mor}_k(K, \bar{k})$, by hypothesis it has image $i_K(K)$, so we may define $\tau(x) = i_K^{-1}(\sigma(x))$ and $\tau \in \mathrm{Aut}(K/k)$.

3 $\implies$ 2). Conversely given $\sigma \in \mathrm{Mor}_k(K, \bar{k})$, by hypothesis $\sigma = i_K \circ \tau$, and so has image $i_K(K)$.

For the final statement if K/k is finite, then we've shown in Proposition 1.23 that $[K : k]_s < \infty$. So the embedding $\mathrm{Mor}_k(K, i_K)$ is bijective if and only if $\#\,\mathrm{Aut}(K/k) = [K : k]_s$ as required. □

Corollary 1.33 (Galois Criteria)
Let K/k be a finite extension. Then

$$\#\,\mathrm{Aut}\,K/k \leq [K : k]_s \leq [K : k]$$

with equalities if and only if K/k is Galois.

Proof. We've seen the inequalities (Definition 1.13)

$$\#\,\mathrm{Aut}(K/k) \leq [K : k]_s \leq [K : k] < \infty$$

with equality if and only if K/k is both normal (Proposition 1.32) and separable (Proposition 1.23) □

Corollary 1.34 (Subfield is Normal)
Let K/k be a normal extension and $F \subset K$ a subfield, then K/F is normal.

Proof. We assume the tower F/k has compatible embeddings into $\bar{k}$, then we have

$$\mathrm{Mor}_F(K, \bar{k}) \subset \mathrm{Mor}_k(K, \bar{k})$$

and the result follows from NOR1 . □

Proposition 1.35 (Automorphisms of Normal Extension)
Let K/k be a normal extension with compatible embeddings in $\bar{k}$. There is a canonical isomorphism of groups

$$\begin{aligned} \operatorname{Aut}(\bar{k}/k)/\operatorname{Aut}(\bar{k}/K) &\to \operatorname{Aut}(K/k)\,. \\ \sigma &\to i_K^{-1}\circ\sigma\circ i_K \end{aligned}$$

When $K\subset\bar{k}$ then this map is simply restriction to K.

Proof. By NOR1 $(\sigma\circ i_K)(K) = i_K(K)$ so this is well-defined and by Corollary 1.24 it's surjective. It's clear the kernel is $\operatorname{Aut}(\bar{k}/K)$ so the result follows. □

In fact we can replace $\bar{k}$ with a normal overfield and obtain results corresponding to Corollary 1.24 and Proposition 1.32 respectively. Due to the explicit embeddings in $\bar{k}$ the arguments become slightly awkward.

Corollary 1.36 (Extension to normal overfield)
Let L/k be a normal extension such that $K\subset L$ then there is a canonical surjective monoid morphism

$$\operatorname{Aut}(L/k)\to \operatorname{Mor}_k(K,L)$$

by restriction. The kernel is $\operatorname{Aut}(L/K)$.

Proof. Assume an embedding $i_L : L\to\bar{k}$.
Consider $\sigma\in\operatorname{Mor}_k(K,L)$, then by Corollary 1.24 there exists an extension $\tilde{\sigma}\in\operatorname{Aut}(\bar{k}/k)$ such that $i_L\circ\sigma = \tilde{\sigma}\circ i_K$. As in the previous Proposition there exists $\hat{\sigma}\in\operatorname{Aut}(L/k)$ such that $\tilde{\sigma}\circ i_L = i_L\circ\hat{\sigma}$. Therefore $i_L\circ\sigma = i_L\circ\hat{\sigma}|_K$ which implies $\sigma = \hat{\sigma}|_K$ as required.

□

Corollary 1.37 (Automorphisms of Normal subextension)
Let L/k be a normal extension and $K\subset L$, then the following are equivalent

1. *K/k is normal*
2. *$\operatorname{Mor}_k(K,L) = \operatorname{Aut}(K/k)$, i.e. every k-embedding $\sigma : K\to L$ has $\sigma(K) = K$.*
3. *For every $\sigma\in\operatorname{Aut}(L/k)$ we have $\sigma(K) = K$*

In this case $\operatorname{Aut}(L/K)\triangleleft\operatorname{Aut}(L/k)$ is normal and we have a canonical group isomorphism

$$\operatorname{Aut}(L/k)/\operatorname{Aut}(L/K)\to\operatorname{Aut}(K/k)$$

Proof. 1 $\implies$ 2). Given $\sigma\in\operatorname{Mor}_k(K,L)$, then by definition we have $(i_L\circ\sigma)(K) = (i_L)(K)$, which means $\sigma(K) = K$
2 $\implies$ 1). Given any $\sigma\in\operatorname{Mor}_k(K,\bar{k})$, this extends to $\tilde{\sigma}\in\operatorname{Mor}_k(L,\bar{k})$. Since L is normal $\tilde{\sigma}(L) = i_L(L)$, we see $\hat{\sigma} := i_L^{-1}\circ\tilde{\sigma}\in\operatorname{Aut}(L/k)$. By hypothesis $\hat{\sigma}(K) = K$. Furthermore $\sigma(K) = \tilde{\sigma}(K) = i_L(\hat{\sigma}(K)) = i_L(K)$. Since σ is arbitrary then it shows K is normal.
2 $\implies$ 3). This is clear
3 $\implies$ 2). Given $\sigma\in\operatorname{Mor}_k(K,L)$ by the previous Corollary we can extend to $\operatorname{Aut}(L/k)$ and the result follows easily. By the previous corollary the canonical map given is surjective, which yields the isomorphism. □

The following is straight-forward

Corollary 1.38 (Conjugate Elements)
Let K/k be a normal extension and two elements $\alpha,\beta\in K$ be two elements with the same minimal polynomial. Then there exists $\sigma\in\operatorname{Aut}(K/k)$ such that $\sigma(\alpha) = \beta$.

Proof. By Corollary 1.15 there is an isomorphism $k(\alpha)\to k(\beta)$. Corollary 1.36 gives the required extension. □

1.10 Finite Fields

A finite field K necessarily has positive characteristic p, and therefore the prime subfield is isomorphic to the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Proposition 1.39 (Properties of finite fields)
Every finite field K is a finite-dimensional vector space over its prime subfield $\mathbb{F}_p$. Define $n = [K:\mathbb{F}_p]$.

- *$\#K = p^n$*
- *K is a splitting field for $X^{p^n} - X\in\mathbb{F}_p[X]$, and indeed is equal to the set of roots*
- *The multiplicative group of units $K^\star$ is cyclic.*

Proof. Since $K/\mathbb{F}_p$ is a finite-dimensional vector space it must have order p^n.

The group of units has order $p^n - 1$, so by Lagrange's theorem every non-zero element satisfies $X^{p^n-1} - 1 = 0$, so therefore every element satisfies $X^{p^n} - X = 0$. Since this polynomial can have at most p^n roots it shows that the roots are exactly all the elements of K.

We note that $X^d - 1$ as at most d roots. The proof that $K^\star$ is cyclic is delayed to Section 1.10.1 and Proposition 1.45. □

Proposition 1.40 (Frobenius morphism)
Given any field $K/\mathbb{F}_p$ the Frobenius map

$$\phi : x \to x^p$$

is an injective field homomorphism. In particular when K is finite it is an automorphism.

Proposition 1.41 (Existence and uniqueness of finite fields)
Consider the algebraic closure $\overline{\mathbb{F}_p}$ and let $\mathbb{F}_{p^n}$ denote the splitting field of $f(X) = X^{p^n} - X$ in $\overline{\mathbb{F}_p}$. Then

- *$\mathbb{F}_{p^n}$ is equal to the set of roots of $X^{p^n} - X$*
- *It is the unique subfield of order p^n and every finite field of order p^n is isomorphic to this.*
- *$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$*

Proof. First we show that the set of roots of $f(X)$ forms a subfield of $\overline{\mathbb{F}_p}$. This follows from the previous Proposition. We see that $f(X)$ has at most $\deg(f) = p^n$ roots, and in fact p^n distinct roots because $f'(X) = -1$ (and ...). Therefore the splitting field of $f(X)$ is exactly the set of roots.

Furthermore every subfield of order p^n must satisfy this polynomial, so it is the unique such subfield.

Since every algebraic extension of $\mathbb{F}_p$ is isomorphic to a subfield of $\overline{\mathbb{F}_p}$ it's also the unique algebraic extension of order p^n up to isomorphism.

Clearly if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ we see that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p]$, so we must have $m \mid n$. Conversely if $\alpha \in \mathbb{F}_{p^m}$ then $\alpha^{p^m} = \alpha \implies \alpha^{p^{rm}} = \alpha$ for all $r > 0$, so $\alpha \in \mathbb{F}_{p^n}$. □

It is usually most convenient to work in $\overline{F_p}$ and consider the finite fields of the form $\mathbb{F}_{p^n}$ as in the Proposition. We've seen in Proposition 1.29 that every finite field $\mathbb{F}_q := \mathbb{F}_{p^n}$ is perfect and therefore every algebraic extension is separable. In fact we may show that every finite extension is Galois.

Proposition 1.42
The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle$$

cyclic of order n generated by the Frobenius automorphism.

Proof. Let $G = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. We've observed that $\phi \in G$. We claim that it has order n. Certainly by Lagrange's theorem $\phi^n = 1$, whence the order d divides n. By definition every $\alpha \in \mathbb{F}_{p^n}$ satisfies $X^{p^d} - X = 0$. This has at most p^d roots whence $d = n$. Clearly ϕ generates a cyclic subgroup of order n. However by Corollary 1.33 G has at most order n, whence $G = \langle \phi \rangle$ as required. Furthermore by the same result $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. □

Proposition 1.43 (Subfields of $\mathbb{F}_{p^n}$)
Consider the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. Then it has a unique subfield of order p^m if and only if $m \mid n$. In this case $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois and

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \phi^m \rangle$$

and in particular has order n/m.

Proof. We've already shown that it has a unique subfield of order p^m, by assuming an embedding in $\overline{\mathbb{F}_p}$. Let $H = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$. This is a subgroup of the cyclic group G, so by Lemma 1.44 it's of the form $\langle \phi^r \rangle$ for $r \mid n$. By a similar argument as before $r \geq m$. Clearly $\phi^m \in H$, so $r \mid m$, whence $r = m$. This subgroup has order n/m, so the extension is Galois. □

By Lemma 1.44 the cyclic group of order n has a unique subgroup of order n/m if and only if $m \mid n$. So we have shown that there is a correspondence between subfields of $\mathbb{F}_{p^n}$ and subgroups of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. This holds more generally as described in Section 1.11.

1.10.1 $\mathbb{F}_q^\star$ is cyclic

This proof is adapted from this stackexchange answer.

First we show some simple properties of cyclic groups in general

Lemma 1.44
Let G be a cyclic group of order n with generator g. Then

- *An element $h = g^r$ has order $\frac{n}{(n,r)}$. In particular there are $\phi(n)$ generators.*
- *For every $m \mid n$ there is a unique subgroup of order m, which is cyclic and generated by $g^{n/m}$*
- *When $d \mid n$ there are precisely $\phi(n/d)$ elements of order d*
- *Similarly there are d elements of order dividing d*

In particular

$$n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$$

Proof. Let d be the order of $h = g^r$ for $0 \leq r < n$. Firstly $h^{\frac{n}{(n,r)}} = g^{\frac{r}{(n,r)}n} = 1$, whence $d \mid \frac{n}{(n,r)}$. Conversely $h^d = g^{rd} = 1 \implies n \mid rd \implies \frac{n}{(n,r)} \mid \frac{r}{(n,r)}d \implies \frac{n}{(n,r)} \mid d$. Therefore the result follows. Note h is a generator if and only if $(n, r) = 1$.

Clearly if $m \mid n$ then $H = \langle g^{n/m} \rangle$ is a cyclic subgroup of order m. Suppose H is an arbitrary subgroup. Let r be the minimal integer such that $g^r \in H$. By Euclid's Algorithm $ar + bn = (r, n)$, therefore $g^{(r,n)} \in H$, whence by minimality $r = (r, n) \implies r \mid n$. Let $m = n/r$ then $H = \langle g^{n/m} \rangle$ as required.

There are $\phi(n)$ elements of order n. Every element of order d generates the unique cyclic subgroup of order d, therefore there are $\phi(n/d)$ of them.

Any element of order dividing d generates a cyclic subgroup of order dividing d, which must be contained in the unique cyclic subgroup of order d. □

For any group G define

$$G[d] = \{x \in G \mid x^d = 1\}$$

For a cyclic group we have shown that $\#G[d] = d$. We show that if $\#G[d] \leq d$ then G is cyclic.

Proposition 1.45
Let G be a finite group. Suppose $\#G[d] \leq d$ for all $d \mid n$ then G is cyclic.

Proof. Let G_d denote the set of elements of order exactly d. It's enough to show that G_n is non-empty, we actually show $G_d = \phi(d)$ for all $d \mid n$.

Suppose G_d is non-empty and $y \in G_d$, then $\langle y \rangle \subseteq G[d]$ and by hypothesis $\langle y \rangle = G[d]$ is cyclic of order d. Clearly $G_d \subset G[d]$ is the set of generators of $\langle y \rangle$, and therefore has order $\phi(d)$. Therefore G_d is either empty or has order $\phi(d)$ by the previous Lemma. Counting we have

$$n = \#G = \sum_{d|n} \#G_d \leq \sum_{d|n} \phi(d) = n$$

where the last equality follows from the previous Lemma. Since we have equality $\#G_d = \phi(d)$ for every $d \mid n$ as required. □

1.11 Galois Correspondence

We've seen that for K/k a finite extension

$$\#\operatorname{Aut}(K/k) \leq [K : k]_s \leq [K : k]$$

with equality if and only if K/k is Galois, by Corollary 1.33.

Remark 1.15
If k is perfect then $\bar{k}/k$ is Galois.

The main result of Galois Theory is that in the finite case there is an order-reversing bijection between subgroups and subfields

$$\begin{aligned} \{H \leq \mathrm{Gal}(K/k)\} &\longleftrightarrow \{F \subseteq K\} \\ \phi : H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \psi : \mathrm{Gal}(K/F) &\longleftarrow F \end{aligned}$$

Such an order reversing map is usually called an (antitone) Galois connection, as the first such type arose from Galois Theory. Note it is well-defined because of the following proposition.

Proposition 1.46
If K/k is Galois and $F \subset K$ then K/F is Galois.

Proof. This follows from Corollary 1.34 and 1.19 □

We need to show that $\phi \circ \psi = \mathrm{id}$ and $\psi \circ \phi = \mathrm{id}$. The first is marginally easier, and follows purely from the definition of Galois without making any finiteness assumptions.

Proposition 1.47 (Fixed field of Galois group)
If K/k is Galois and $F \subset K$ then

$$K^{\mathrm{Gal(K/F)}} = F$$

or in other words $\phi \circ \psi = \mathrm{id}$, and in particular ϕ is injective.

Proof. Clearly $F \subseteq K^{\mathrm{Gal(K/F)}}$. Conversely given $\alpha \in K \setminus F$, then $\deg m_{\alpha,F} > 1$. Since α is separable it must have another root $\beta \in K$. By Corollary 1.38 there is an element $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\alpha) = \beta$. In other words $\alpha \notin K^{\mathrm{Gal}(K/F)}$, which shows the reverse inclusion. □

Proposition 1.48
Let K/k be a field extension and $H \subseteq \mathrm{Aut}(K/k)$ a finite subgroup then K/K^H is finite Galois with

$$H = \mathrm{Gal}(K/K^H)$$

and order equal to $[K : K^H]$. In particular for a finite Galois Extension K/k we have $\psi \circ \phi = \mathrm{id}$.

Proof. Firstly observe that trivially $H \subseteq \mathrm{Aut}(K/K^H)$. If we know that $[K : K^H] < \infty$, then by Definition 1.13 and Proposition 1.23 we have

$$\#H \leq \#\,\mathrm{Aut}(K/K^H) \leq [K : K^H]_s \leq [K : K^H]$$

We can prove equality everywhere if we show that $[K : K^H] \leq \#H$, which is shown either by Lemma 1.49 or Lemma 1.50. Note equality also shows that K/K^H is finite Galois by Corollary 1.33.

□

We present two approaches to showing the inequality $[K : K^H] \leq \#H$. The first uses independence of characters style argument (see Garling, JMilne), and the second which is more straightforward uses the action of H to show that every element has degree at most $\#H$ (Artin).

Lemma 1.49 (Bound degree of fixed field I)
Let K/k be a field extension and $H \subset \mathrm{Aut}(K/k)$ a finite subgroup. Then $[K : K^H] \leq \#H$

Proof. Let $H = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}$ and $\alpha_1, \ldots, \alpha_m$ a K^H-basis for K.

Consider the vector space K^n and the elements $\hat{\alpha}_j = (\sigma_1(\alpha_j), \ldots, \sigma_n(\alpha_j))$ for $j = 1 \ldots m$. It's enough to show that these are linearly independent over K, as that shows $m \leq n$.

Let $S(K) := \{v \in K^m \mid \sum_{j=1}^m v_j \hat{\alpha}_j = 0\}$, we aim to show that $S(K) = \{0\}$. If we also consider $S(K^H)$, any non-zero elements will be a K^H linear-dependence for $\alpha_1, \ldots, \alpha_m$ by considering the first component ($\sigma_1 = \mathrm{id}$). Therefore by assumption $S(K^H) = \{0\}$. Finally we see it's enough to show that $S(K) \neq \{0\} \implies S(K^H) \neq \{0\}$.

First observe that $K^\star$ and H both act on $S(K)$. The first by scaling and the second component-wise. This is well-defined because $v \in S(K)$ if and only if

$$\sum_j v_j \sigma(\alpha_j) = 0 \quad \forall \sigma \in H\,.$$

Apply τ to obtain

$$\sum_j \tau(v_j)(\tau \circ \sigma)(\alpha_j) = 0 \quad \forall \sigma \in H$$

and since multiplication by τ permutes H we see $\tau(v) \in S(K)$ as required.

If there exists $0 \neq v \in S(K)$, consider v with a minimal number of non-zero components. By scaling we can assume λv has at least one component in K^H. The vector $\tau(\lambda v) - \lambda v$ then has at least one fewer non-zero components, so by minimality must be zero. Since τ was arbitrary we see $0 \neq \lambda v \in S(K^H)$ as required.

□

Lemma 1.50 (Bound degree of fixed field II)
Let K/k be a field extension and H a finite subgroup of $\mathrm{Aut}(K/k)$. *Then K/K^H is finite separable, and simple, with* $[K : K^H] \leq \#H$

Proof. We show that K/K^H is separable and every element has degree at most $\#H$. For any $\alpha \in K$, consider the orbit $H(\alpha) = \{\sigma(\alpha) \mid \sigma \in H\}$, which is of order at most $\#H$. Then the polynomial

$$f(X) = \prod_{\beta \in H(\alpha)} (X - \beta)$$

has α as a root and is separable by Proposition 1.9. Furthermore $f^\tau = f$ because τ permutes $H(\alpha)$ (it's injective and hence bijective). Therefore $f \in K^H[X]$ and $m_{\alpha,K^H} \mid f$. We see that α has degree at most $\#H$ and is separable by Lemma 1.11.

If K/k is finite, then a-fortiori K/K^H is finite, so we may apply the Primitive Element Theorem 1.26 directly to show the result.

More generally let $K^H(\alpha)$ be a simple subfield of K of maximal degree. This exists because the degree of α is bounded above by $\#H$. We claim $K^H(\alpha) = K$, for if not then $K^H \subset K^H(\alpha) \subset K^H(\alpha, \beta)$ is a finite separable extension of K^H, whence it must be simple by the Primitive Element Theorem 1.26, contradicting maximality. Finally the degree of $[K : K^H]$ is the degree of α, which we've seen is bounded above by $\#H$. □

Now we may demonstrate straightforward criteria for subfield to be normal

Proposition 1.51
Let K/k be a finite Galois extension and $F \subset K$ a subfield.
Then F/k is Galois if and only if $\mathrm{Gal}(K/F) \triangleleft \mathrm{Gal}(K/k)$ *is normal. In this case we have a canonical isomorphism*

$$\mathrm{Gal}(K/k)/\mathrm{Gal}(K/F) \to \mathrm{Gal}(F/k)$$

Proof. Recall from Corollary 1.37 we have F/k is normal iff $\sigma(F) = F$ for all $\sigma \in \mathrm{Gal}(K/k)$. We also observe that

$$\mathrm{Gal}(K/\sigma(F)) = \sigma \,\mathrm{Gal}(K/F)\sigma^{-1}$$

By the correspondence $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/F') \iff F = F'$.
Therefore

$$\begin{aligned}
F/k \text{ normal} &\iff \sigma(F) = F \quad \forall \sigma \in \mathrm{Gal}(K/k) \\
&\iff \mathrm{Gal}(K/\sigma(F)) = \mathrm{Gal}(K/F) \quad \forall \sigma \in \mathrm{Gal}(K/k) \\
&\iff \sigma \,\mathrm{Gal}(K/F)\sigma^{-1} = \mathrm{Gal}(K/F) \quad \forall \sigma \in \mathrm{Gal}(K/k) \\
&\iff \mathrm{Gal}(K/F) \triangleleft \mathrm{Gal}(K/k)
\end{aligned}$$

Finally the natural restriction map is surjective by Corollary 1.36 and has the required kernel. □

References