Fields and Galois Theory

David Rufino

Apr 2020

Contents

1 Fields and Galois Theory **1**
1.1 Field extensions . . . 1
1.2 Polynomials over a field . . . 2
1.2.1 Separable Polynomials . . . 3
1.3 Algebraic Extensions . . . 4
1.4 Algebraic Closure . . . 5
1.5 Splitting Fields . . . 6
1.6 Separable Extensions . . . 6
1.7 Perfect Fields . . . 7
1.8 Normal Extensions . . . 7
1.9 Galois Correspondence . . . 8

1 Fields and Galois Theory

Some concise notes on fields and galois theory for algebraic extensions K/k. Mainly follows LangAlgebra72, with a couple of changes. The definition of separable extension is the more obvious and general one. The proof of key lemma $[K : K^H] \leq \#H$ uses independence argument rather than Primitive Element Theorem. This is taken from JMilne and Garling.

1.1 Field extensions

A field extension K/k is simply an inclusion of fields $k \subset K$. Note every field is an extension over its prime subfield, so we lose no generality by always considering field extensions. Then a morphism $\sigma : K \to L$ of field extensions is simply a ring homomorphism which is the identity on k. Note every field morphism is injective so we refer to this as a k-embedding, and it is automatically an isomorphism onto its image.
Note every extension K/k may be viewed as a k-vector space.

Definition 1.1
An extension K/k is finite if it has finite dimension as a k-vector space. In this case denote its dimension as $[K : k]$

Field homomorphisms are automatically injective

Proposition 1.1
Let $\sigma : K \to L$ be a k-algebra homomorphism of fields, then σ is injective. Therefore we refer to it as a k-embedding
We write the set of such maps as

$$\mathrm{Mor}_k(K, L)$$

Proof. Recall that for a ring homomorphism σ is injective iff $\ker(\sigma) = (0)$. Suppose that $x \neq 0$, then $1 = f(1) = f(xx^{-1}) = f(x)f(x)^{-1}$, hence $f(x) \neq 0$. Therefore σ is injective.
Alternatively since a field has no non-trivial ideals, so $\ker(\sigma) = (0)$ or 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 (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 in $K[X]$ is

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

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

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

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

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

1.2.1 Separable Polynomials

We are interested 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 $r = 1$. □

We say two elements x, y of a ring are co-prime if $(x, y) = (1)$.

Definition 1.4
A polynomial $f \in k[X]$ is separable if f and f' are co-prime.

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. □

1.3 Algebraic Extensions

Definition 1.5 (Algebraic element and Minimal Polynomial)
If K/k is a field extension we say that $x \in$ is algebraic (over k)if it satisfies

$$f(x) = 0$$

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

$$\phi_x : k[X] \to K$$

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

$$f(x) = 0 \iff m_{x,k} \mid f$$

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

Definition 1.6 (Algebraic Extension)
A field extension K/k is algebraic if every element $x \in K$ is algebraic.

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

Proposition 1.11 (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 1.12
Let K/k be an algebraic extension then any k-embedding to itself is surjective and therefore an isomorphism. In other words

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

Proof. □

We prove the first lifting theorem

Proposition 1.13 (Lifting to simple extensions)
Let $K(\alpha)/K$ be a simple algebraic extension, and $\sigma : K \to L$ a field embedding such that $m_{\alpha,K}$ 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 $m_{\alpha,K}$ in L.

In particular if $m_{\alpha,K}$ 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 $i(K)(\alpha')$ are both isomorphic to the quotient ring $K[X]/(m_{\alpha,K})$. □

Corollary 1.14
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 inclusion $K \subset K(\beta)$ 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 Algebraic Closure

The theory is somewhat easier to develop if one may assume the existence of a maximal algebraic extension, so we develop this first.

Definition 1.7 (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 1.8 (Algebraic Closure)
Finally $\bar{k}$ is an algebraic closure of k if it is algebraic over k and algebraically closed.

Proposition 1.15 (Algebraic extensions embed in Algebraic Closure)
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

$$\mathrm{Mor}_k(L, M) \to \mathrm{Mor}_k(K, M)$$

$$\sigma \to \sigma|_K$$

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 1.13 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 1.16 (Unique up to isomorphism)
An algebraic closure $\bar{k}$ of k is unique up to (non-unique) isomorphism.

Definition 1.9 (Separability degree)
The cardinality of $\mathrm{Mor}_k(K, \bar{k})$ is independent of the choice of $\bar{k}$. We write this as $[K : k]_s$

Definition 1.10 (Automorphisms are embeddings into $\bar{k}$)
Let K/k be an algebraic extension and $\bar{k}$ an algebraic closure of k. Then there exists at least one k-embedding $i : K \to \bar{k}$. Given any such embedding there is an embedding

$$i^{\#} : \mathrm{Aut}(K/k) \to \mathrm{Mor}_k(K, \bar{k})$$

In particular when the right hand side is finite

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

When i is inclusion, then this may be regarded as inclusion also.

Corollary 1.17 (Extension to algebraic closure)
If $k \subset K \subset \bar{k}$, then every $\sigma : K \to \bar{k}$ lifts to $\tilde{\sigma} : \bar{k} \to \bar{k}$. That is to say, there is a canonical surjection

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

Proof. Take $L = M = \bar{k}$ in Proposition 1.15, then any $\sigma \in \mathrm{Mor}_k(K, \bar{k})$ lifts to a $\tilde{\sigma} \in \mathrm{Mor}_k(\bar{k}, \bar{k})$. Proposition 1.12 shows this is an element of $\mathrm{Aut}(\bar{k}/k)$. □

Corollary 1.18 (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. First suppose that $m_\alpha = m_\beta$. Then there is an isomorphism $\sigma : k(\alpha) \to k(\beta) \subset \bar{k}$. Applying the previous corollary gives the required lift to $\tilde{\sigma} : \bar{k} \to \bar{k}$.
Conversely $m_\alpha(\beta) = m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0$. Therefore $m_\beta \mid m_\alpha$. Similarly by considering σ^{-1}, we see that $m_\alpha \mid m_\beta$. □

1.5 Splitting Fields

Definition 1.11 (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

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

where α_i are the roots of f 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 1.19 (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.

Uniqueness (up to non-unique isomorphism!) requires an extension theorem and a rigidity theorem... □

1.6 Separable Extensions

The concept of separable extensions is important, as illustrated by Proposition 1.13.

Definition 1.12 (Separability)
An algebraic element $x \in K$ is separable over k if its minimal polynomial is separable.

Definition 1.13 (Separable Extension)
An algebraic extension K/k is separable if every element is separable.

Remark 1.14
Lang72 initially only defines separability for finite field extensions by $[K : k]_s = [K : k]$. Then defines for algebraic extensions for f.g. (i.e. finite) sub-extensions.

We may show another characterization of separability

Proposition 1.20
If K/k is separable and $K' \subset K$, then K/K' and K'/k are separable.

Proof. The second is obvious. For the first embed K in $\bar{k}$, and consider any $\alpha \in K$. Then we have $m_{\alpha,K'} | m_{\alpha,k}$ by definition. We may show directly that if $f \mid g$ and g separable then f is separable. For by Lemma 1.10 $1 = ag + bg'$. Since $g = fh$, then $g' = fh' + f'h$, and $1 = afh + b(fh' + f'h) = (ah + bh')f + bhf'$, whence f is separable. □

Proposition 1.21
$K = k(\alpha_1, \dots, \alpha_n)$ is separable over k if and only if each α_i are separable.

Proof. □

From Proposition 1.13 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 (Criterion for separability)
Let K/k be a finite extension then

$$[K : k]_s \leq [K : k]$$

with equality if and only if K/k is separable.

Artin Theorem 4.6

Proposition 1.23 (Primitive Element Theorem)
Let K/k be a finite separable extension of an infinite field k then $K = k(\alpha)$ is simple.

Proof. Consider the set $\mathrm{Mor}_k(K, \bar{k}) = \{\sigma_1, \dots, \sigma_n\}$ which by Proposition 1.22 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 Perfect Fields

For large classes of base fields all extensions are separable :

Proposition 1.24 (Perfect field)
TFAE

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

In this case we say k is perfect.

Proposition 1.25 (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.

1.8 Normal Extensions

A normal extension is an algebraic extension in which every minimal polynomial splits completely. In some sense it is "closed" because automorphisms over the algebraic closure map the field into itself . In what follows it is more convenient to work with an algebraic closure, but strictly speaking that is not necessary (see Garling). First we prove a trivial Lemma.

Lemma 1.26
Let K/k, L/k be field extensions and $i : K \to L$ a k-embedding. Suppose that $f \in k[X]$ is a polynomial, then α is a root of f if and only if $i(\alpha)$ is a root of f.
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 1.27 (Normal Extension)
Let K/k be an algebraic extension and a given algebraic closure $\bar{k}$, then the following are equivalent

1. *For any two k-embedding of $\sigma, \tau \in \mathrm{Mor}_k(K, \bar{k})$ we have $\sigma(K) = \tau(K)$.*
2. *K is the splitting field of some family of polynomials $f_i \in k[X]$.*
3. *Every irreducible polynomial in $k[X]$ with at least one root in K splits in K.*

This is called a normal extension.

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 $T_i = \{\alpha \mid f_i(\alpha) = 0\}$ and $T_i' = \{\alpha \in \bar{k} \mid f_i(\alpha) = 0\}$. By hypothesis $K = k(\cup_i T_i)$, and we claim that for any such σ we have $\sigma(K) = k(\cup_i T_i') =: K' \subset \bar{k}$. By Lemma 1.26 that any σ induces a bijection between T_i and T_i'. Therefore $\bigcup_i T_i' \subseteq \sigma(K) \implies K' \subseteq \sigma(K)$. Furthermore $\sigma(K) \subseteq k(\sigma(\bigcup_i T_i)) \subseteq k(\bigcup_i T_i') = K'$.

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 1.18 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 another criterion

Proposition 1.28
Let K/k be an algebraic extension and $i : K \to \bar{k}$ a given embedding then the following are equivalent

- *K/k is normal*
- *The embedding $i^{\#} : \mathrm{Aut}(K/k) \to \mathrm{Mor}_k(K, \bar{k})$ (1.10) is a bijection*

When $K \subset \bar{k}$ it's necessary and sufficient that every $\sigma \in \mathrm{Mor}_k(K, \bar{k})$ has image K.

When K/k is finite it's necessary and sufficient that

$$\# \mathrm{Aut}(K/k) = [K : k]_s$$

Proof. If K/k is normal, then given $\sigma' \in \mathrm{Mor}_k(K, \bar{k})$ by hypothesis the image of i and σ' is the same. Therefore we can define $\sigma(x) = i^{-1}(\sigma'(x))$.
Conversely any $\sigma' \in \mathrm{Mor}_k(K, \bar{k})$ can be written as $i \circ \sigma$ for σ invertible, so must have image $i(K)$. As this is true for every such σ' then K/k must be normal.
Clearly if K/k is finite, then we've shown in Proposition 1.22 that $[K : k]_s < \infty$. So the embedding $i^{\#}$ is bijective if and only if $\# \mathrm{Aut}(K/k) = [K : k]_s$ as required. □

Corollary 1.29 (Subfield is Normal)
Let K/k be a normal extension and $K' \subset K$ a subfield, then K/K' is normal.

Proof. This is clear from the first criterion in Proposition 1.27 since $\mathrm{Mor}_{K'}(K, \bar{k}) \subset \mathrm{Mor}_k(K, \bar{k})$. □

Proposition 1.30 (Automorphisms of Normal Extension)
For K/k an normal extension and $K \subset \bar{k}$. Then $\mathrm{Aut}(\bar{k}/K)$ is a normal subgroup of $\mathrm{Aut}(\bar{k}/k)$ and there is a canonical isomorphism of groups

$$\mathrm{Aut}(\bar{k}/k)/\,\mathrm{Aut}(\bar{k}/K) \to \mathrm{Aut}(K/k)\,.$$

Proof. By Corollary 1.17 the canonical map $\mathrm{Aut}(\bar{k}/k) \to \mathrm{Aut}(K/k)$ is surjective, and it's clear the kernel $\mathrm{Aut}(\bar{k}/K)$ so the result follows. □

In fact we can replace $\bar{k}$ with a normal overfield and obtain results corresponding to Corollary 1.17 and Proposition 1.28 respectively.

Corollary 1.31 (Extension to normal overfield)
Let L/k be a normal extension and $K \subset L$ then there is a canonical surjective monoid morphism

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

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

Proof. Without loss of generality assume that $L \subset \bar{k}$.
Consider $\sigma \in \mathrm{Mor}_k(K, L)$, then by Corollary 1.17 there exists an extension $\tilde{\sigma} : \bar{k} \to \bar{k}$. By Proposition 1.28 the morphism $\tilde{\sigma}|_L$ has image L and therefore by Proposition 1.12 is an element of $\mathrm{Aut}(L/k)$.

□

Corollary 1.32 (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. $\mathrm{Mor}_k(K, L) = \mathrm{Aut}(K/k)$*, i.e. every k-embedding $\sigma : K \to L$ has $\sigma(K) = K$.*

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

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

Proof. Without loss of generality assume that $L \subset \bar{k}$.
$1 \implies 2$). This is clear by definition.
$2 \implies 1$). Given $\sigma : K \to L \subset \bar{k}$, this extends to $\tilde{\sigma} \in \mathrm{Mor}_k(L, \bar{k})$. Since L is normal this is actually a member of $\mathrm{Aut}(L/k)$. By hypothesis $\sigma = \tilde{\sigma}|_K$ has image K, so by Proposition 1.28 K/k must be normal.
By the previous corollary the canonical map $\mathrm{Aut}(L/k) \to \mathrm{Aut}(K/k)$ is surjective and the result follows.

□

The following is straight-forward

Corollary 1.33 (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 $\sigma \in \mathrm{Aut}(K/k)$ such that $\sigma(\alpha) = \beta$.

1.9 Galois Correspondence

We've seen that for K/k a finite extension (Definition 1.10 and Proposition 1.22)

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

The first inequality is an equality if and only if K is normal (Proposition 1.28), and the second is an equality if and only if K is separable (Proposition 1.22). Therefore we say a field extension K/k which is normal and separable is Galois, and denote the group of automorphisms by $\mathrm{Gal}(K/k)$, which in the finite case has order $[K : k]$. We have shown

Proposition 1.34 (Order of Galois Group)
A finite extension K/k is Galois if and only if $\#\,\mathrm{Aut}(K/k) = [K : k]$

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

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

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 1.35
If K/k is Galois and $K' \subset K$ then K/K' is Galois.

Proof. This follows from Corollary 1.29 and 1.20 □

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 1.36 (Fixed field of Galois group)
If K/k is Galois and $K' \subset K$ then

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

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

Proof. Clearly $K' \subseteq K^{\mathrm{Gal(K/K')}}$. Conversely given $\alpha \in K \setminus K'$, then $\deg m_{\alpha,K'} > 1$, so must have another root $\beta \in K$. Since α is separable, we must have $\alpha \neq \beta$. By Corollary 1.33 there is an element $\sigma \in \mathrm{Gal}(K/K')$ such that $\sigma(\alpha) = \beta$. In other words $\alpha \notin K^{\mathrm{Gal}(K/K')}$. □

NB Similar to Theorem 1.8 in Lang, but using independence style argument from Garling Theorem 11.2 and JMilne

Proposition 1.37
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 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 1.10 and Proposition 1.22 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 1.38 or Lemma 1.39. Note equality also shows that K/K^H is finite Galois by Proposition 1.34.

□

Lemma 1.38 (Bound degree of fixed field)
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 $H = \{\sigma_1, \dots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}$ and $\alpha_1, \dots, \alpha_m$ a basis for K/K^H.

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

Let $S = \{v \in K^m \mid \sum_{j=1}^m v_j \hat{\alpha}_j = 0\}$, then clearly S is a K-vector space, which we wish to show has dimension 0. First observe that τ acts on S, for suppose $v \in S$ then

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

apply τ to get

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

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

If we have a non-zero $v \in S$, then we may scale it so that the j-th component is exactly equal 1. If $\tau(v) = v$ for all τ, then the coefficients lie in K^H and we have a linear dependence of the basis $\alpha_1, \dots, \alpha_m$ (by just looking at the σ_1 coefficient) a contradiction. Therefore there is $\tau \in H$ such that $\tau(v) \neq v$. Then $\tau(v) - v$ is a non-zero vector with strictly fewer number of non-zero coefficients, since the j-th coefficient is now zero. This shows that there must be an element of S with only one non-zero coefficient, therefore $v_i \sigma(\alpha_i) = 0$ a contradiction. □

Remark 1.15 (Lang approach)
We demonstrate a different approach to Lemma 1.38 by first showing that K/K^H is separable and then resorting to the primitive element theorem.

Lemma 1.39 (Alternative proof of boundedness of fixed field)
Let K/k be a field extension and H a finite subgroup of $\mathrm{Aut}(K/k)$. Then K/K^H is separable, and simple of degree at most $\#H$.

Proof. 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 clearly separable. Furthermore $f^\tau = f$ because τ permutes $H(\alpha)$ (it's injective and hence bijective). Therefore $f \in K^H[X]$ and α has degree at most $\#H$. Proposition 1.9 shows it is separable. Therefore K/K^H is separable as required.

Let $K^H(\alpha)$ be a simple subfield of K of maximal degree, which exists since the degree of α must be bounded 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 1.23, contradicting maximality. Finally the degree of $[K : K^H]$ is the degree of α, which we've seen is bounded above by $\#H$. □

References