1
Classical Galois theory

Convention *In this chapter, all fields we consider are commutative.*

This chapter develops the basic aspects of Galois theory for fields. We study first the notions of algebraic, separable, normal and Galois field extensions, before exhibiting the Galois correspondence between Galois extensions and field automorphisms.

1.1 Algebraic extensions

Given a field extension $K \subseteq L$, the composite

$$\begin{tikzcd} K \times L \arrow[r, tail] & L \times L \arrow[r, "\times"] & L \end{tikzcd}$$

provides L with the structure of a vector space on K, thus also of a K-algebra. We write $[L : K]$ or $\mathsf{dim}\,[L : K]$ for the dimension of L as a K-vector space.

Let us recall that every proper ideal $I \subsetneq L$ of a field L is necessarily trivial. Indeed, if I contains a non zero element i, then $l = ii^{-1}l \in I$ for every $l \in L$, thus $I = L$. Since the kernel of a field homomorphism is an ideal not containing 1, this ideal must be zero, proving that every field homorphism is injective.

We write $K[X]$ for the ring of polynomials with coefficients in the field K.

Definition 1.1.1 Let $K \subseteq L$ be a field extension. An element $l \in L$ is algebraic over K when there exists a non-zero polynomial $p(X) \in K[X]$ such that $p(l) = 0$. The extension $K \subseteq L$ is algebraic when all elements of L are algebraic over K.

Proposition 1.1.2 *Every finite dimensional field extension is algebraic.*

Proof Given $l \in L$, the sequence of elements $1, l, l^2, l^3, \dots, l^n, \dots$ necessarily yields a dependence relation

$$a_n l^n + a_{n-1} l^{n-1} + \cdots + a_2 l^2 + a_1 l + a_0 = 0, \quad a_i \in K,$$

since $[L : K]$ is finite. Putting

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$$

yields $p(l) = 0$. □

Proposition 1.1.3 *Let $K \subseteq L$ be a field extension and $l \in L$ an element which is algebraic over K. There exists a unique polynomial $p(X) \in K[X]$ such that*

(i) *the leading coefficient of $p(X)$ is 1,*
(ii) *$p(l) = 0$,*
(iii) *the degree of $p(X)$ is minimal among the polynomials $q(X) \in K[X]$ satisfying $q(l) = 0$.*

This polynomial $p(X)$ is irreducible and is called the minimal polynomial of l. When $q(X) \in K[X]$ and $q(l) = 0$, $p(X)$ divides $q(X)$.

Proof By 1.1.1, we choose a polynomial $p(X) \in K[X]$ of minimal degree among those satisfying $p(l) = 0$; there is of course no restriction in assuming that its leading coefficient is 1. If $p(X)$ could be decomposed as the product of two polynomials in $K[X]$, then l would be a root of one of these; the minimality of the degree of $p(X)$ implies therefore that $p(X)$ is irreducible in $K[X]$.

If $q(X)$ is a polynomial as in the statement, we consider the euclidean division of $q(X)$ by $p(X)$, yielding

$$q(X) = p(X)\alpha(X) + r(X), \quad \text{degree of } r(X) < \text{degree of } p(X).$$

Since $q(l) = p(l) = 0$, it follows that $r(l) = 0$ and by minimality of the degree of $p(X)$, we get $r(X) = 0$.

The uniqueness of $p(X)$ satisfying those conditions follows at once from the last statement and condition (i). □

Proposition 1.1.4 *In the conditions of proposition 1.1.3, the smallest subfield $K(l)$ of L containing K and l is isomorphic to the quotient $K[X]/\langle p(X)\rangle$, where $\langle p(X)\rangle \subseteq K[X]$ is the principal ideal generated by $p(X)$. Moreover, the dimension $[K(l) : K]$ of the extension $K(l)$ equals the degree of the minimal polynomial $p(X)$ of l.*

Proof Writing

$$p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_o$$

it follows at once that we have an isomorphism

$$\frac{K[X]}{\langle p(X)\rangle} \cong \{k_{n-1}X^{n-1} + \cdots + k_1X + k_0 \,|\, k_i \in K\}$$

where the operations on the right hand side are defined modulo the relation

$$X^n = -a_{n-1}X^{n-1} - \cdots - a_1X - a_0.$$

Observe that the dimension of $K[X]$ over K is indeed n, the degree of $p(X)$.

The subalgebra $K(l) \subseteq L$ generated by K and l is clearly given by

$$K(l) = \{q(l) \,|\, q(X) \in K[X]\}.$$

Using the minimal polynomial of l, every occurrence of l^n can be replaced by terms of lower degree, thus

$$K(l) = \{k_{n-1}l^{n-1} + \cdots + k_0 \,|\, k_i \in K\}.$$

This is a K-vector space of dimension at most n. Multiplying by $a \in K(l) \subseteq L$, $a \neq 0$, is a K-linear endomorphism of $K(l)$, which is injective since L is a field. By finiteness of the dimension of $K(l)$, this endomorphism is a linear isomorphism, proving that a is invertible in $K(l)$. Thus the subalgebra $K(l) \subseteq L$ is in fact the subfield $K(l) \subseteq L$ generated by K and l.

Next we consider the ring homomorphism

$$\gamma\colon \frac{K[X]}{\langle p(X)\rangle} \longrightarrow K(l), \quad q(X) \mapsto q(l), \quad \text{degree}\, q(X) < n.$$

This K-linear map is injective since $q(l) = 0$ implies $q(X) = 0$, because the degree of $q(X)$ is stricly less than the degree of the minimal polynomial $p(X)$ (see 1.1.3). Therefore it is bijective, because the first space has dimension n and the second has dimension at most n. Thus γ is an isomorphism. □

Definition 1.1.5 Let $K \subseteq L$ be a field extension. Two elements $l_1, l_2 \in L$ are conjugate over K when they are algebraic over K and have the same minimal polynomial.

A link with the usual notion of conjugate complex numbers should certainly be exhibited. This is the object of the following example.

Example 1.1.6 Consider the field extension $\mathbb{R} \subseteq \mathbb{C}$. For every complex number $l = a + b\,\mathsf{i}$ which is not already a real, that is $b \neq 0$, one gets at once

$$p(X) = \big(X - (a + b\,\mathsf{i})\big)\big(X - (a - b\,\mathsf{i})\big) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$$

which is an irreducible polynomial over $\mathbb{R}$, since it is a product of linear polynomials not in $\mathbb{R}[X]$. The degree 2 of $p(X)$ is certainly minimal in $\mathbb{R}[X]$ for allowing $p(a + b\,\mathsf{i}) = 0$, since $a + b\,\mathsf{i}$ is not a real. Therefore $p(X)$ is the minimal polynomial of $a + b\,\mathsf{i}$ (see 1.1.3) and $a + b\,\mathsf{i}$, $a - b\,\mathsf{i}$ are conjugate complex numbers over the reals.

Definition 1.1.7 Let $K \subseteq L$ be a field extension. A field homomorphism $f\colon L \longrightarrow L$ is called a K-homomorphism when it fixes all elements of K, that is, $f(k) = k$ for every element $k \in K$.

Proposition 1.1.8 *Let $K \subseteq L$ be an algebraic field extension. Then every K-endomorphism of L is necessarily an automorphism. We shall write $\mathsf{Aut}_K(L)$ for the group of K-automorphisms of L.*

Proof Consider $l \in L$ with minimal polynomial $p(X)$ over K. For every K-endomorphism f of L, one has

$$p\big(f(l)\big) = f\big(p(l)\big) = f(0) = 0$$

which proves that $f(l)$ is conjugate to l over K. Therefore f induces a map

$$f_l\colon \{l' \in L | p(l') = 0\} \longrightarrow \{l' \in L | p(l') = 0\}, \quad l' \mapsto f(l').$$

The set on which f_l acts is finite, as the set of roots of $p(X)$ in L. Since f is injective as a field homomorphism, f_l is injective as well and thus surjective, because it acts on a finite set. In particular $l = f_l(l') = f(l')$ for some conjugate l' of l, which proves the surjectivity of f. □

1.2 Separable extensions

Let us recall that the derivative of a polynomial

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$$

in $K[X]$ is the polynomial

$$p'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2X + a_1.$$

The classical formulæ for the derivative of a sum and a product are valid for polynomials over an arbitrary field.

Remark 1.2.1 With the previous notation, when $a_n \neq 0$, $p(X)$ has degree n. The corresponding coefficient na_n of the derivative vanishes when $n = 0$ in K, that is, when the characteristic of the field K divides n. Thus $p'(X)$ has degree $n-1$ if and only if the characteristic of K does not divide n. This is the place to recall that the exponents of a polynomial in $K[X]$ are natural numbers, not elements of K; when computing a derivative, the exponent n which is a natural number enters the coefficients of the derivative in the form $1 + \cdots + 1$ (n times), $1 \in K$, which is an element of K, possibly 0.

Proposition 1.2.2 *Consider a field K, an element $a \in K$ and a polynomial $p(X) \in K[X]$. The following conditions are equivalent:*

(i) *a is a multiple root of $p(X)$;*
(ii) *$p(a) = 0$ and $p'(a) = 0$.*

Proof Assuming (i), we can write $p(X) = (X-a)^k q(X)$ with $k \geq 2$. Therefore

$$p'(X) = k(X-a)^{k-1}q(X) + (X-a)^k q'(X).$$

Since $k - 1 \geq 1$, this implies $p'(a) = 0$.

Conversely, $p(X) = (X-a)q(X)$ since a is a root of $p(X)$, thus

$$p'(X) = q(X) + (X-a)q'(X).$$

Putting $X = a$, there remains $q(a) = 0$ since $p'(a) = 0$. This implies $q(X) = (X-a)s(X)$ and thus $p(X) = (X-a)^2 s(X)$. □

Definition 1.2.3 A field extension $K \subseteq L$ is separable when

(i) the extension is algebraic,
(ii) the roots of the minimal polynomial of every $l \in L$ are all simple.

Proposition 1.2.4 *Let $K \subseteq L$ be a field extension in characteristic zero. If $l \in L$ is algebraic over K, all roots of the minimal polynomial of l over K are simple.*

Proof Write $p(X)$ for the minimal polynomial of l; it suffices to verify that l is a simple root of $p(X)$. If l is a multiple root of $p(X)$, then $p(X)$ has degree at least 2 and $p'(l) = 0$ (see 1.2.2), with $p'(X)$ a polynomial of degree at least 1 (see remark 1.2.1). This contradicts the minimality condition in 1.1.3. □

Corollary 1.2.5 *In characteristic zero, every algebraic extension is separable.* □

Proposition 1.2.6 *Let $K \subseteq M \subseteq L$ be field extensions. If $K \subseteq L$ is separable, then $M \subseteq L$ is separable as well.*

Proof Every $l \in L$ has a minimal polynomial $p(X) \in K[X]$. Since $K[X] \subseteq M[X]$, the extension $M \subseteq L$ is algebraic. The minimal polynomial $q(X) \in M[X]$ of l is a factor of $p(X)$ in $M[X]$, thus all its roots in L are distinct. □

1.3 Normal extensions

Definition 1.3.1 A field extension $K \subseteq L$ is normal when

(i) the extension is algebraic,
(ii) for every element $l \in L$, the minimal polynomial of l over K factors entirely in $L[X]$ in polynomials of degree 1.

An algebraic field extension $K \subseteq L$ with L algebraically closed is thus necessarily normal.

Proposition 1.3.2 *Let $K \subseteq M \subseteq L$ be field extensions. If $K \subseteq L$ is normal, then $M \subseteq L$ is normal as well.*

Proof Every $l \in L$ has a minimal polynomial $p(X) \in K[X]$. Since $K[X] \subseteq M[X]$, the extension $M \subseteq L$ is algebraic. The minimal polynomial $q(X) \in M[X]$ of l divides $p(X)$ in $M[X]$, thus factors in $L[X]$ into polynomials of degree 1, since so does $p(X)$. □

Proposition 1.3.3 *Let $K \subseteq L$ be a normal, finite dimensional field extension. For every intermediate field extension $K \subseteq M \subseteq L$, every K-homomorphism $M \longrightarrow L$ extends to a K-automorphism of L.*

Proof Consider the situation

$$\begin{tikzcd}
K \arrow[r, tail] \arrow[d, equal] & N \arrow[r, tail] \arrow[d, "f"] & L \\
K \arrow[r, tail] & L \arrow[r, equal] & L
\end{tikzcd}$$

where f is a K-homomorphism between arbitrary field extensions; we want to prove that f can be extended to $N(l)$, for an arbitrary element $l \in L$. If $N = L$, we are done; otherwise choose $l \in L$, $l \notin N$, with minimal polynomial $p(X) \in K[X]$. Since $[L : N]$ is finite, the extension $N \subseteq L$ is algebraic (see 1.1.2). Let $q(X) \in N(X)$ be the minimal polynomial of l over N. It follows by 1.1.3 that $q(X)$ divides $p(X)$ in $N[X]$ and thus, since $p(X)$ decomposes in $L[X]$ into linear factors, so does $q(X)$.

On the other hand f induces a ring homomorphism

$$\overline{f}\colon N[X] \longrightarrow L[X]$$

obtained by applying f to the coefficients of every polynomial. Since $q(X)$ divides $p(X)$ in $N[X]$ and $\overline{f}$ is a ring homomorphism, $\overline{f}\big(q(X)\big)$ divides $\overline{f}\big(p(X)\big)$ in $L[X]$. But $\overline{f}\big(p(X)\big) = p(X)$ since f is a K-homomorphism. Again since $p(X)$ factors in L into polynomials of degree 1, the same conclusion applies to $\overline{f}\big(q(X)\big)$. We choose a root l' of $\overline{f}\big(q(X)\big)$ in L. Thus $\overline{f}\big(q(X)\big)$ is in the ideal of $L[X]$ generated by $X - l'$. Therefore, combining with 1.1.4, we get a K-homomorphism

$$N(l) \cong \frac{N[X]}{\langle q(X)\rangle} \xrightarrow{\tilde{f}} \frac{L[X]}{\langle X - l'\rangle} \cong L(l') \cong L$$

extending f.

Coming back to the situation in the statement, we put first $N = M$, from which we get a K-extension $M(l) \longrightarrow L$. One repeats the process with $N = M(l)$, and so on. We must reach $N = L$ after finitely many steps, because $[L : K]$ is finite. □

Proposition 1.3.4 *Let $K \subseteq L$ be a finite dimensional normal extension. The following conditions are equivalent:*

(i) *the elements l_1, l_2 of L are conjugate over K;*

(ii) *there exists a K-automorphism $f\colon L \longrightarrow L$ such that $f(l_1) = l_2$.*

Proof Assuming condition (i), we consider the minimal polynomial $p(X)$ of l_1, l_2. Applying 1.1.4 twice, we get a K-isomorphism

$$K(l_1) \cong \frac{K[X]}{\langle p(X)\rangle} \cong K(l_2),$$

mapping l_1 onto l_2. By 1.3.3, this extends to a K-automorphism of L still mapping l_1 onto l_2.

Conversely, write $p(X)$ for the minimal polynomial of l_1 over K. Since f is a homomorphism, one gets at once

$$p(l_2) = p\big(f(l_1)\big) = f\big(p(l_1)\big) = f(0) = 0.$$

Since $p(X)$ is irreducible, it is also the minimal polynomial of l_2 and therefore l_1, l_2 are conjugate (see 1.1.5). □

1.4 Galois extensions

Definition 1.4.1 A field extension $K \subseteq L$ is Galois when it is normal and separable. The group $\mathsf{Aut}_K(L)$ of K-automorphisms of L is called the Galois group of this extension and is denoted by $\mathsf{Gal}\,[L : K]$.

Proposition 1.4.2 *Let $K \subseteq M \subseteq L$ be field extensions. If $K \subseteq L$ is a Galois extension, then $M \subseteq L$ is a Galois extension as well.*

Proof By propositions 1.2.6 and 1.3.2. □

Let us now introduce some notation and constructions. Let $K \subseteq L$ be a Galois field extension.

- Given an intermediate field extension $K \subseteq M \subseteq L$, via proposition 1.4.2 we consider the Galois group $\mathsf{Gal}\,[L : M] = \mathsf{Aut}_M(L)$ of those automorphisms of L which fix M.
- Given a subgroup $G \subseteq \mathsf{Gal}\,[L : K]$, we write

  $$\mathsf{Fix}\,(G) = \{l \in L \mid \forall g \in G \;\; g(l) = l\}.$$

  $\mathsf{Fix}\,(G)$ is clearly a subfield of L since each $g \in G$ is a field automorphism, and it contains K since each $g \in G$ is a K-automorphism:

  $$K \subseteq \mathsf{Fix}\,(G) \subseteq L.$$

- $\#X$ indicates as usual the number of elements (the *cardinal*) of the set X.

We now reduce our attention to Galois extensions even if some results, like proposition 1.4.4, are valid more generally.

Definition 1.4.3 A Galois connection between two posets A, B consists in two order reversing maps

$$f\colon A \longrightarrow B, \quad g\colon B \longrightarrow A$$

with the property

$$a \leq gf(a), \quad b \leq fg(b)$$

for all elements $a \in A$ and $b \in B$.

The reader familiar with category theory will observe that viewing A and B as categories and f, g as contravariant functors, this is just the usual definition of two adjoint functors. Indeed, viewing f, g as covariant functors between A and the dual of B, the conditions for a Galois connection present f as left adjoint to g. The situation is reversed if one works with B and the dual of A.

Proposition 1.4.4 *Let $K \subseteq L$ be a Galois field extension. The maps*

$$\begin{tikzcd}\{M \mid K \subseteq M \subseteq L\} \arrow[r, shift left, "\mathsf{Gal}"] & \{G \mid G \subseteq \mathsf{Gal}\,[L:M]\} \arrow[l, shift left, "\mathsf{Fix}"]\end{tikzcd}$$

defined as above constitute a Galois connection.

Proof Gal and Fix are contravariant functors between posets, so the announced adjunction property reduces to the trivial relations

$$\mathsf{Fix}\,\big(\mathsf{Gal}\,(M)\big) = M \subseteq \mathsf{Fix}\,\big(\mathsf{Gal}\,[L:M]\big), \qquad G \subseteq \mathsf{Gal}\,\big(\mathsf{Fix}\,(G)\big). \qquad \square$$

Theorem 1.4.5 (Galois theorem) *Let $K \subseteq L$ be a finite dimensional Galois extension of fields. In this case, the adjunction in 1.4.4 is a contravariant isomorphism. Moreover, for every intermediate field extension $K \subseteq M \subseteq L$*

$$\mathsf{dim}\,[L:M] = \#\mathsf{Gal}\,[L:M].$$

Proof Let us first prove the last statement, by induction on $\mathsf{dim}\,[L:M]$.

When $\mathsf{dim}\,[L:M] = 1$, $M = L$ and the unique automorphism of L fixing L is the identity.

Let us now assume the result for all extensions $M' \subseteq L'$ of dimension $k < n$ and let us consider $M \subseteq L$ of dimension n. If $l \in L \setminus M$ has minimal polynomial $p(X) \in M[X]$ of degree r, let us consider $M \subseteq$

$M(l) \subseteq L$. Since $l \notin M$, then $M \neq M(l)$ and thus $\dim\big[L : M(l)\big] < n$. But

$$\dim\big[M(l) : M\big] \cdot \dim\big[L : M(l)\big] = \dim\,[L : M]$$

and thus $\dim\big[L : M(l)\big] = \frac{n}{r}$. By inductive assumption, there are exactly $\frac{n}{r}$ $M(l)$-automorphisms

$$f_1, \dots, f_{\frac{n}{r}} \colon L \longrightarrow L.$$

On the other hand, writing $l_1, \dots, l_r$ for the roots of $p(X)$ in L, we get for each index j an M-automorphism $g_j \colon L \longrightarrow L$ such that $g_j(l) = l_j$ (see 1.3.4). Let us define $h_{ij} \colon L \longrightarrow L$ by $h_{ij} = g_j \circ f_i$. This yields n automorphisms h_{ij} of L. We shall prove that they are exactly all the elements of $\mathsf{Gal}\,[L : M]$.

First of all, these h_{ij} are M-automorphisms, thus elements of $\mathsf{Gal}\,[L : M]$. Moreover these elements are distinct, because

$$\begin{array}{llll} h_{ij} = h_{i'j'} & \Rightarrow & g_j f_i(l) = g_{j'} f_{i'}(l) & \\ & \Rightarrow & g_j(l) = g_{j'}(l) & \text{since } f_i,\ f_j \text{ fix } M(l) \\ & \Rightarrow & l_j = l_{j'} & \text{by definition of } g_j,\ g_{j'} \\ & \Rightarrow & j = j' & \text{by separability of } M \subseteq L \\ & & & \text{(see 1.2.6).} \end{array}$$

Thus $g_j = g_{j'}$ and since this is a monomorphism, $f_i = f_{i'}$.

Finally observe that when an automorphism $f \colon L \longrightarrow L$ fixes M, from $p\big(f(l)\big) = f\big(p(l)\big) = f(0) = 0$, we deduce $f(l) = l_j$ for some j. Therefore $\big(g_j^{-1} \circ f\big)(l) = g_j^{-1}(l_j) = l$ and $g_j^{-1} \circ f$ is an M-automorphism fixing l; it is thus an $M(l)$-automorphism, meaning that $g_j^{-1} \circ f = f_i$ for some i. Therefore $f = g_j \circ f_i = h_{ij}$.

Next let us prove the formula $\dim\big[L : \mathsf{Fix}\,(G)\big] = \#G$ for every subgroup $G \subseteq \mathsf{Gal}\,[L : K]$. It suffices to prove $\dim\big[L : \mathsf{Fix}\,(G)\big] \leq \#G$ since, by the first part of the proof and proposition 1.4.4, this will imply

$$\#G \leq \#\mathsf{Gal}\,\big[L : \mathsf{Fix}\,(G)\big] = \dim\big[L : \mathsf{Fix}\,(G)\big] \leq \#G.$$

On the other hand observe that, again by the first part of the proof,

$$\dim\,[L : K] = \#\mathsf{Gal}\,[L : K]$$

which shows that $\mathsf{Gal}\,[L : K]$ and thus G are finite. Let us say that $\#G = n$; we must prove that $\dim\big[L : \mathsf{Fix}\,(G)\big] \leq n$.

We develop the proof by reduction *ad absurdum*. We thus choose $l_1, \dots, l_{n+1}$ in L, linearly independent over $\mathsf{Fix}\,(G)$. Let us also write

$g_1, \ldots, g_n$ for the n elements of G. Let us consider the homogeneous system of equations

$$\left.\begin{array}{rcl} g_1(l_1)X_1 + \cdots + g_1(l_{n+1})X_{n+1} & = & 0, \\ & \vdots & \\ g_n(l_1)X_1 + \cdots + g_n(l_{n+1})X_{n+1} & = & 0. \end{array}\right\} \quad (1)$$

Since there are more unknowns than equations, there exists a non-zero solution. Let us choose such a non-zero solution which possesses the minimal number of non zero components. There is no restriction in assuming that this solution has the form $(\alpha_0, \ldots, \alpha_r, 0, \ldots, 0)$ with each α_i non-zero. This yields a system

$$\left.\begin{array}{rcl} g_1(l_1)X_1 + \cdots + g_1(l_r)X_r & = & 0, \\ & \vdots & \\ g_n(l_1)X_1 + \cdots + g_n(l_r)X_r & = & 0 \end{array}\right\} \quad (2)$$

admitting a solution all of whose components are non-zero. Let us then fix $g \in G$ and let us apply this g to all equations, evaluated in $\alpha_1, \ldots, \alpha_r$:

$$\left.\begin{array}{rcl} gg_1(l_1)g(\alpha_1) + \cdots + gg_1(l_r)g(\alpha_r) & = & 0, \\ & \vdots & \\ gg_n(l_1)g(\alpha_1) + \cdots + gg_n(l_r)g(\alpha_r) & = & 0. \end{array}\right\} \quad (3)$$

But the elements gg_i are just a permutation of the elements of G, thus the system (3) can be rewritten, up to a permutation of the equations,

$$\left.\begin{array}{rcl} g_1(l_1)g(\alpha_1) + \cdots + g_1(l_r)g(\alpha_r) & = & 0, \\ & \vdots & \\ g_n(l_1)g(\alpha_1) + \cdots + g_n(l_r)g(\alpha_r) & = & 0. \end{array}\right\} \quad (4)$$

Let us multiply system (4) by α_r and system (2), evaluated at the α_i, by $g(\alpha_r)$; let us substract the results. This yields

$$\left.\begin{array}{l} g_1(l_1)\big(\alpha_r g(\alpha_1) - \alpha_1 g(\alpha_r)\big) + \cdots \\ \qquad + g_1(l_{r-1})\big(\alpha_r g(\alpha_{r-1}) - \alpha_{r-1} g(\alpha_r)\big) = 0, \\ \qquad \vdots \\ g_n(l_1)\big(\alpha_r g(\alpha_1) - \alpha_1 g(\alpha_r)\big) + \cdots \\ \qquad + g_n(l_{r-1})\big(\alpha_r g(\alpha_{r-1}) - \alpha_{r-1} g(\alpha_r)\big) = 0 \end{array}\right\} \quad (5)$$

which yields a solution of system (1) with an additional zero component. By choice of the original solution, this one is the zero solution, yielding

Cambridge Books Online © Cambridge University Press, 2010

$\alpha_r g(\alpha_i) = \alpha_i g(\alpha_r)$ for all $i \leq r-1$. This can be rewritten as

$$\alpha_i \alpha_r^{-1} = g(\alpha_i) g(\alpha_r)^{-1} = g(\alpha_i) g(\alpha_r^{-1}) = g(\alpha_i \alpha_r^{-1}).$$

Since $g \in G$ is arbitrary, we get $\alpha_i \alpha_r^{-1} \in \mathsf{Fix}\,(G)$; let us put $m_i = \alpha_i \alpha_r^{-1} \in \mathsf{Fix}\,(G)$. We thus have $\alpha_i = m_i \alpha_r$ with $i < r$ and $m_i \in \mathsf{Fix}\,(G)$; putting $m_r = 1 \in \mathsf{Fix}\,(G)$, we get $\alpha_i = m_i \alpha_r$ for all $i \leq r$. The first equation of system (2) evaluated at the α_i yields

$$\begin{aligned}
0 &= g_1(l_1)\alpha_1 + \cdots + g_1(l_r)\alpha_r \\
&= g_1(l_1) m_1 \alpha_1 + \cdots + g_1(l_r) m_r \alpha_r \\
&= \alpha_r \big(g_1(l_1) m_1 + \cdots + g_1(l_r) m_r \big) \\
&= \alpha_r \big(g_1(l_1) g_1(m_1) + \cdots + g_1(l_r) g_1(m_r) \big) \quad \text{since } m_i \in \mathsf{Fix}\,(G) \\
&= \alpha_r g_1(l_1 m_1 + \cdots + l_r m_r).
\end{aligned}$$

We know that $\alpha_r \neq 0$ and g_1 is injective, from which $l_1 m_1 + \cdots + l_r m_r = 0$, which contradicts the linear independance of the l_i over $\mathsf{Fix}\,(G)$. This concludes the proof that $\dim\,[L : \mathsf{Fix}\,(G)] = \#G$.

The rest is easy. Starting from $K \subseteq M \subseteq L$, we get $M \subseteq \mathsf{Fix}\,(\mathsf{Gal}\,[L : M])$ by proposition 1.4.4. It remains to see that given $l \in L \setminus M$, there exists $f \colon L \longrightarrow L$ fixing M but not l. If $p(X)$ is the minimal polynomial of l over M, then $p(X)$ has not degree 1 since $l \notin M$; thus $p(X)$ has at least two distinct roots in L, since $M \subseteq L$ is a Galois extension by proposition 1.4.2. Let $l' \neq l$ be such a root of $p(X)$; by proposition 1.3.4, there exists an M-automorphism f of L such that $f(l) = l'$.

Choose now $G \subseteq \mathsf{Gal}\,[L : K]$. By proposition 1.4.4 we have $G \subseteq \mathsf{Gal}\,[L : \mathsf{Fix}\,(G)]$. What we have already proved of the present theorem then yields

$$\#G \leq \#\mathsf{Gal}\,[L : \mathsf{Fix}\,(G)] = \dim\,[L : \mathsf{Fix}\,(G)] = \#G.$$

Therefore, since the cardinals are finite, $G = \mathsf{Gal}\,[L : \mathsf{Fix}\,(G)]$. □

The following lemma will help completing the statement of theorem 1.4.5.

Lemma 1.4.6 *Let $K \subseteq M \subseteq L$ be finite dimensional field extensions, with $K \subseteq L$ a Galois extension. For every $f \in \mathsf{Gal}\,[L : K]$,*

$$f \cdot \mathsf{Gal}\,[L : M] \cdot f^{-1} = \mathsf{Gal}\,[L : f(M)].$$

Proof Given $g \in \mathsf{Gal}\,[L : M]$ and $m \in M$,

$$(f \circ g \circ f^{-1})\big(f(m)\big) = (f \circ g)(m) = f(m)$$

since g fixes M. Thus $f \circ g \circ f^{-1}$ fixes $f(M)$, meaning $f \circ g \circ f^{-1} \in \mathsf{Gal}\,\big[L : f(M)\big]$. This already proves

$$f \cdot \mathsf{Gal}\,[L : M] \cdot f^{-1} \subseteq \mathsf{Gal}\,\big[L : f(M)\big].$$

Putting $g = f^{-1}$ and $N = f(M)$, we get in an analogous way

$$f^{-1} \cdot \mathsf{Gal}\big[L : f(M)\big] \cdot f = g \cdot \mathsf{Gal}[L : N] \cdot g^{-1} \subseteq \mathsf{Gal}\big[L : g(N)\big] = \mathsf{Gal}\,[L : M],$$

that is, multiplying on the left by f and on the right by f^{-1},

$$\mathsf{Gal}\,\big[L : f(M)\big] \subseteq f \cdot \mathsf{Gal}\,[L : M] \cdot f^{-1}.$$ □

Theorem 1.4.7 *In the conditions of theorem 1.4.5, the extensions* $K \subseteq M \subseteq L$*, with* $K \subseteq M$ *a normal extension, correspond via the bijection with the normal subgroups* $G \subseteq \mathsf{Gal}\,[L : K]$*. Moreover,*

$$\mathsf{Gal}\,[M : K] \cong \frac{\mathsf{Gal}\,[L : K]}{\mathsf{Gal}\,[L : M]},$$

again when $K \subseteq M$ *is a normal extension.*

Proof Let us begin with $K \subseteq M \subseteq L$ with $K \subseteq M$ normal and prove that $\mathsf{Gal}\,[L : M]$ is normal in $\mathsf{Gal}\,[L : K]$. Given $f \in \mathsf{Gal}\,[L : K]$, let us prove first that $f(M) \subseteq M$. Indeed, if $m \in M$ admits $p(X) \in K[X]$ as minimal polynomial, then $p\big(f(m)\big) = f\big(p(m)\big) = f(0) = 0$, thus $f(m)$ is one of the roots of $p(X)$. Since $K \subseteq M$ is normal, $f(m) \in M$. Moreover since f is injective and dimensions are finite, we have $f(M) = M$. Applying lemma 1.4.6, we then find

$$f \cdot \mathsf{Gal}\,[L : M] \cdot f^{-1} = \mathsf{Gal}\,\big[L : f(M)\big] = \mathsf{Gal}\,[L : M].$$

Let us start now from $K \subseteq M \subseteq L$ with $\mathsf{Gal}\,[L : M] \subseteq \mathsf{Gal}\,[L : K]$ a normal subgroup. Choose $m \in M$ with minimal polynomial $p(X) \in K[X]$; this polynomial $p(X)$ factors in $L[X]$ into distinct factors of degree 1, and we must prove these belong to $M[X]$. If $m \neq l \in L$ is another root of $p(X)$, we get by proposition 1.3.4 the existence of a K-automorphism f of L such that $f(m) = l$. By normality of $\mathsf{Gal}\,[L : M]$,

$$f \cdot \mathsf{Gal}\,[L : M] \cdot f^{-1} = \mathsf{Gal}\,[L : M]$$

while by lemma 1.4.6

$$f \cdot \mathsf{Gal}\,[L : M] \cdot f^{-1} = \mathsf{Gal}\,\big[L : f(M)\big].$$

This yields $\mathsf{Gal}\,[L : M] = \mathsf{Gal}\,\big[L : f(M)\big]$ and thus $M = f(M)$, by the isomorphism of theorem 1.4.5. This proves $l = f(m) \in M$.

It remains to prove the last formula. There is a group homomorphism obtained by taking the restriction to M:

$$\theta\colon \mathsf{Gal}\,[L:K] \longrightarrow \mathsf{Gal}\,[M:K], \quad f \mapsto f\,|_M;$$

indeed, as just observed, the normality of M implies $f(M) = M$. By proposition 1.3.3, this homomorphism θ is surjective. Thus

$$\mathsf{Gal}\,[M:K] \cong \frac{\mathsf{Gal}\,[L:K]}{\mathsf{Ker}\,\theta}$$

and it remains to prove $\mathsf{Ker}\,\theta = \mathsf{Gal}\,[L:M]$. And indeed $f \in \mathsf{Gal}\,[L:K]$ is in $\mathsf{Ker}\,\theta$ when its restriction to M is the identity on M, that is, when $f \in \mathsf{Gal}\,[L:M]$. □