2

Galois theory of Grothendieck

This chapter does not present the Galois theory of Grothendieck in its full generality, that is in the context of schemes: this would require a long technical introduction. But the spirit of Grothendieck's approach is applied to the context of Galois theory for fields.

Convention *In this chapter, all fields, rings and algebras we consider are commutative and have a unit.*

2.1 Algebras on a field

Let us recall that an algebra A on a field K is a vector space A on K provided with a multiplication which makes it a ring and which satisfies $k(aa') = (ka)a'$ for all elements $k \in K$ and $a, a' \in A$. Let us emphasize the fact that all rings we consider are commutative and have a unit.

A typical example of a K-algebra is the ring $K[X]$ of polynomials with coefficients in K. Observe that given such a polynomial

$$p(X) = k_n X^n + \cdots + k_0$$

and a K-algebra A, we get at once a polynomial function

$$p\colon A \longrightarrow A, \quad a \mapsto p(a) = k_n a^n + \cdots + k_0 \cdot \mathbf{1}$$

where $\mathbf{1}$ is the unit of A. It is well known that distinct polynomials can give rise to the same polynomial function, for example the polynomials X and X^2 on the field of integers modulo 2.

Another immediate example of a K-algebra is the power K^n, where all operations are defined componentwise.

An ideal $I \subseteq A$ of a K-algebra A is an ideal I of the ring A; it is in particular a vector subspace of A. The quotient A/I is then again a

K-algebra. On the other hand the kernel of a K-algebra homomorphism $f\colon A \longrightarrow B$ is an ideal of the K-algebra A.

Proposition 2.1.1 *Let K be a field and A a K-algebra. The following conditions are equivalent:*

(i) *A is a field;*
(ii) *A has only trivial ideals.*

Proof (i) $\Rightarrow$ (ii) was already observed at the beginning of section 1.1. Conversely, if $0 \neq a \in A$, then aA is an ideal of A as K-algebra. Since $0 \neq a = a \cdot 1 \in aA$, we get $aA = A$, from which we get $a' \in A$ with $aa' = 1$. □

Corollary 2.1.2 *Let K be a field and $f\colon A \longrightarrow B$ a surjective homomorphism of K-algebras. If B is a field, then the kernel of f is a maximal ideal of A.*

Proof We have $B \cong A/\mathsf{Ker}\, f$. If $\mathsf{Ker}\, f \subseteq I$, with I an ideal, we get a corresponding quotient $q\colon A/\mathsf{Ker}\, f \longrightarrow A/I$. The kernel of q is then an ideal of the field $B = A/\mathsf{Ker}\, f$, thus is trivial. If $\mathsf{Ker}\, q = (0)$, then $\mathsf{Ker}\, f = I$. If $\mathsf{Ker}\, q = A/\mathsf{Ker}\, f$, then $A/I = (0)$ by surjectivity of q and $A = I$. □

Proposition 2.1.3 *Let K be a field. Every ideal of the K-algebra $K[X]$ is principal.*

Proof Let $I \subseteq K[X]$ be a non zero ideal and $p(X)$ a non zero polynomial in I, whose degree is minimal in I. For every polynomial $q(X) \in K[X]$ let us perform the euclidean division

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

Since $p(X)$ and $q(X)$ are in the ideal I, we get $\beta(X) \in I$ and by minimality of the degree of $p(X)$, it follows that $\beta(X) = 0$. Therefore $p(X)$ divides $q(X)$ and I is the principal ideal generated by $p(X)$. □

Proposition 2.1.4 *Let K be a field and $p(X) \in K[X]$. The following conditions are equivalent:*

(i) *the polynomial $p(X)$ is irreducible;*
(ii) *the ideal $\langle p(X) \rangle$ generated by $p(X)$ is maximal;*
(iii) *the K-algebra $K[X]/\langle p(X) \rangle$ is a field.*

Proof (i) $\Rightarrow$ (ii) Let $\langle p(X)\rangle \subseteq I$ with I an ideal; by 2.1.3 $I = \langle s(X)\rangle$ for some polynomial $s(X)$. Thus $p(X) \in \langle s(X)\rangle$, from which follows the existence of $r(X)$ such that $p(X) = r(X) \cdot s(X)$. If $s(X)$ is a non zero constant, then $\langle s(X)\rangle = K[X]$. Otherwise, $r(X)$ is a non zero constant since $p(X)$ is irreducible, from which $\langle p(X)\rangle = \langle s(X)\rangle$.

(ii) $\Rightarrow$ (iii) Consider the quotient $q\colon K[X] \longrightarrow K[X]/\langle p(X)\rangle$. Every ideal $I \subseteq K[X]/\langle p(X)\rangle$ induces an ideal $q^{-1}(I) \supseteq \langle p(X)\rangle$. Since $\langle p(X)\rangle$ is maximal, $q^{-1}(I) = \langle p(X)\rangle$ or $q^{-1}(I) = K[X]$, that is, $I = qq^{-1}(I) = (0)$ or $I = qq^{-1}(I) = K[X]/\langle p(X)\rangle$. Thus the ideals of $K[X]/\langle p(X)\rangle$ are trivial and it is a field by proposition 2.1.1.

(iii) $\Rightarrow$ (i) Let $p(X) = s(X) \cdot r(X)$ be a factorization of $p(X)$. It follows that $\langle p(X)\rangle \subseteq \langle s(X)\rangle$, from which $\langle s(X)\rangle/\langle p(X)\rangle$ is an ideal of $K[X]/\langle p(X)\rangle$. If this ideal is (0), then $\langle s(X)\rangle = \langle p(X)\rangle$ and $p(X)$ divides $s(X)$, thus $r(X)$ is a constant. If this ideal is $K[X]/\langle p(X)\rangle$, then the constant polynomial 1 is in $\langle s(X)\rangle$ up to a polynomial in $\langle p(x)\rangle$, that is

$$1 = u(X) \cdot s(X) + v(X) \cdot p(X) = s(X) \cdot \big(u(X) + v(X) \cdot r(X)\big).$$

This implies that $s(X)$ is a constant. □

Let us now study the algebraic elements of a K-algebra and their minimal polynomials.

Definition 2.1.5 Let K be a field and A a K-algebra. An element $a \in A$ is algebraic when there exists a polynomial $p(X) \in K[X]$ with $p(a) = 0$. The K-algebra A itself is called "algebraic" when all its elements are algebraic.

Proposition 2.1.6 *Let K be a field. Every finite dimensional K-algebra is algebraic.*

Proof As for proposition 1.1.2. □

Proposition 2.1.7 *Let K be a field, A a K-algebra and $0 \neq a \in A$ an algebraic element. There exists a unique polynomial $p(X) \in K[X]$ such that*

(i) *the leading coefficient of $p(X)$ is 1,*
(ii) *$p(a) = 0$,*
(iii) *if $q(X) \in K[X]$ with $q(a) = 0$, then $p(X)$ divides $q(X)$.*

This polynomial $p(X)$ is called the minimal polynomial of a.

Proof As for proposition 1.1.3. Observe that the irreducibility of $p(X)$ is not asserted (see example 2.1.9). And of course there is a trivial reason for this, since $A = K[X]/\langle p(X)\rangle$, with $p(X)$ any reducible polynomial, is a possible situation to which this proposition applies. □

Corollary 2.1.8 *Let K be a field, A a K-algebra and $0 \neq a \in A$ an algebraic element. When the algebra A is an integral domain, the minimal polynomial of a is irreducible.*

Proof Write $p(X)$ for the minimal polynomial of a. If $p(X) = r(X) \times s(X)$, then $0 = s(a) \times r(a)$, from which $s(a) = 0$ or $r(a) = 0$ since A is an integral domain. By minimality of the degree of $p(X)$, it follows that $r(X)$ or $s(X)$ is constant. □

Example 2.1.9 (A reducible minimal polynomial) Let us consider a field K and the K-algebra K^2, of dimension 2 over K. Given $k \in K$, the only root of the first degree polynomial $X - k$ in K^2 is $k \cdot \mathbf{1}$, where $\mathbf{1} = (1,1)$ is the unit of K^2. In particular the minimal polynomial of the element $(1,0) \in K^2$ has not degree 1. But since $(1,0)^2 = (1,0)$, this element is a root in K^2 of $X^2 - X$, which is thus its minimal polynomial. Observe that this polynomial is reducible: $X^2 - X = X(X-1)$.

Proposition 2.1.10 *Let K be a field, A a K-algebra and $0 \neq a \in A$ an algebraic element with minimal polynomial $p(X)$ of degree n. The K-subalgebra $K(a) \subseteq A$ generated by a is isomorphic to*

$$K(a) \cong \frac{K[X]}{\langle p(X)\rangle} \cong \{k_0 + k_1 X + \cdots + k_{n-1}X^{n-1} \mid k_i \in K\}$$

where, in this last expression, the operations are defined modulo $p(X)$.

Proof One has trivially

$$K(a) \cong \big\{q(a)\big|q(X) \in K[X]\big\}.$$

The map

$$\{k_0 + k_1 X + \cdots + k_{n-1}X^{n-1} | k_i \in K\} \longrightarrow K(a), \quad r(X) \mapsto r(a)$$

is surjective. Indeed, every polynomial $q(X)$ can be written as $q(X) = p(X)s(X) + r(X)$ where $r(X)$ has degree at most $n-1$ and, of course, $q(a) = r(a)$. This map is also injective. Indeed, given $r(X)$ and $s(X)$ of degrees at most $n-1$, $r(a) = s(a)$ implies $(r-s)(a) = 0$ with $(r-s)(X)$ of

degree at most $n-1$; by minimality of the degree of $p(X)$, $(r-s)(X)=0$ and $r(X)=s(X)$. □

Corollary 2.1.11 *Let K be a field and A a K-algebra. If A is an integral domain, every non-zero algebraic element of A is invertible.*

Proof By corollary 2.1.8 and propositions 2.1.10 and 2.1.4. □

Let us conclude this section with two general results on K-algebras.

Proposition 2.1.12 (Chinese lemma) *Let K be a field and*

$$(f_i\colon A \longrightarrow\!\!\!\!\!\rightarrow B_i)_{1\leq i\leq n}$$

a finite family of surjective homomorphisms of K-algebras. If

$$i\neq j \Longrightarrow \mathsf{Ker}\, f_i + \mathsf{Ker}\, f_j = A,$$

then the corresponding factorization $f\colon A \longrightarrow \prod_{1\leq i\leq n} B_i$ is surjective as well.

Proof For every pair $i\neq j$ of indices, let us choose $\alpha_{ij}\in \mathsf{Ker}\, f_i$ and $\beta_{ij}\in \mathsf{Ker}\, f_j$ such that $\alpha_{ij}+\beta_{ij}=1$. It follows that

$$f_j(\alpha_{ij}) = f_j(\alpha_{ij}) + f_j(\beta_{ij}) = f_j(\alpha_{ij}+\beta_{ij}) = f_j(1) = 1.$$

We then put

$$\alpha_j = \prod_{i\neq j} \alpha_{ij}$$

and observe immediately that

$$\begin{cases} f_j(\alpha_j) &= 1, \\ f_k(\alpha_j) &= 0 \quad \text{if } k\neq j. \end{cases}$$

Then fix $b=(b_i)_{1\leq i\leq n}\in \prod_{1\leq i\leq n} B_i$ and for each index i, choose $a_i\in A$ such that $f_i(a_i)=b_i$. The element

$$a = \sum_{1\leq k\leq n} \alpha_k a_k$$

is such that

$$f_j(a) = \sum_{1\leq k\leq n} f_j(\alpha_k) f_j(a_k) = f_j(a_j) = b_j,$$

from which

$$f(a) = \big(f_j(a)\big)_{1\leq j\leq n} = (b_j)_{1\leq j\leq n} = b.$$ □

Proposition 2.1.13 *Let K be a field and $n \in \mathbb{N}$ an integer. Every ideal I of the K-algebra K^n has the form*

$$I = \left\{(k_i)_{1\leq i\leq n} \middle| \forall i \in J \ k_i = 0\right\}$$

where $J \subseteq \{1, \ldots, n\}$ is an arbitrary subset of indices.

Proof It is obvious that the subsets I as described are ideals of K^n. Conversely, if $I \subseteq K^n$ is an ideal, put

$$J = \left\{j \middle| 1 \leq j \leq n, \ \ \forall (a_i)_{1\leq i\leq n} \in I \ \ a_j = 0\right\}$$

and write

$$I_J = \left\{(a_i)_{1\leq i\leq n} \middle| \forall i \in J \ a_i = 0\right\}.$$

We have $I \subseteq I_J$ by definition of J and it remains to prove the converse inclusion.

For each index $j \notin J$, there exists thus an element $k^j = (k_i^j)_{1\leq i\leq n} \in I$ with $k_j^j \neq 0$. Let us write $e_i \in K^n$ for the element whose ith component is 1, while the other components are 0. One observes at once that when $j \notin J$, $k^j e_j = k_j^j e_j$. Therefore if $x = (x_i)_{1\leq i\leq n} \in I_J$,

$$x = \sum_{1\leq i\leq n} x_i e_i = \sum_{i\notin J} x_i e_i = \sum_{i\notin J} \frac{x_i e_i}{k_i^i} k_i^i = \sum_{i\notin J} \frac{x_i e_i}{k_i^i} k^i,$$

which is an element of I since each k^i is in I. □

2.2 Extension of scalars

In this section, we study the properties of K-algebras in relation with the consideration of a field extension $K \subseteq L$. In section 1.1 we observed that L is a K-vector space; thus it is itself a K-algebra.

Proposition 2.2.1 *Let $K \subseteq L$ be a finite dimensional field extension and $K \subseteq A \subseteq L$ an intermediate K-algebra. In these conditions, the algebra A is itself a field.*

Proof The algebra A is an integral domain since so is L; it is algebraic by finite dimensionality (see proposition 2.1.6). One concludes the proof by corollary 2.1.11. □

Proposition 2.2.2 *Let $K \subseteq L$ be a field extension. Every L-algebra B is trivially a K-algebra, by restriction of the scalar multiplication to the*

elements of K. On the other hand every K-algebra A yields an L-algebra $L \otimes_K A$, where the multiplication of this algebra is determined by

$$(l \otimes a)(l' \otimes a') = (ll') \otimes (aa')$$

and the scalar multiplication by

$$l(l' \otimes a) = (ll') \otimes a,$$

for $l, l' \in L$ and $a, a' \in A$. These constructions extend to functors

$$L\text{-}\mathsf{Alg} \longrightarrow K\text{-}\mathsf{Alg},\ B \mapsto B, \quad K\text{-}\mathsf{Alg} \longrightarrow L\text{-}\mathsf{Alg},\ A \mapsto L \otimes_K A,$$

the second functor being left adjoint to the first one.

Proof Only the adjunction requires a comment. With the previous notation, we must exhibit natural isomorphisms

$$\mathsf{Hom}_L(L \otimes_K A, B) \cong \mathsf{Hom}_K(A, B).$$

Given $f\colon L \otimes_K A \longrightarrow B$, one considers

$$f'\colon A \longrightarrow B, \quad a \mapsto f(1 \otimes a)$$

and given $g\colon A \longrightarrow B$, one constructs

$$g'\colon L \otimes_K A \longrightarrow B, \quad l \otimes a \mapsto lg(a).$$

Notice that $l\big(f(1 \otimes a)\big) = f(l \otimes a)$ by L-linearity of f, from which the result follows at once. □

Corollary 2.2.3 *Let $K \subseteq L$ be a field extension and A a K-algebra. The following isomorphism holds:*

$$\mathsf{Hom}_K(A, L) \cong \mathsf{Hom}_L(L \otimes_K A, L).$$ □

Proposition 2.2.4 *Let $K \subseteq L$ be a field extension and $p(X) \in K[X]$ a polynomial. The following isomorphism holds:*

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

where in the right hand side, $p(X)$ is viewed as a polynomial with coefficients in L.

Proof It is straightforward to observe that the maps

$$L \otimes_K \frac{K[X]}{\langle p(X) \rangle} \longrightarrow \frac{L[X]}{\langle p(X) \rangle}, \quad \sum_{i=1}^n l_i \otimes [q_i(X)] \mapsto \left[\sum_{i=1}^n l_i q_i(X)\right],$$
$$\frac{L[X]}{\langle p(X) \rangle} \longrightarrow L \otimes_K \frac{K[X]}{\langle p(X) \rangle}, \quad \left[\sum_{i=1}^n l_i X^i\right] \mapsto \sum_{i=1}^n l_i \otimes [X^i],$$

are correctly defined and describe the required isomorphism. □

Proposition 2.2.5 *Let $K \subseteq L$ be a field extension and $p(X) \in K[X]$ a polynomial. There exists a bijection between*

(i) *the roots of $p(X)$ in L,*
(ii) *the homomorphisms of K-algebras $\frac{K[X]}{\langle p(X) \rangle} \longrightarrow L$.*

Proof An element $l \in L$ such that $p(l) = 0$ yields a corresponding well-defined evaluation morphism of K-algebras

$$\mathsf{ev}_l : \frac{K[X]}{\langle p(X) \rangle} \longrightarrow L, \quad [q(X)] \mapsto q(l).$$

Conversely, given a morphism $f : \frac{K[X]}{\langle p(X) \rangle} \longrightarrow L$ of K-algebras, let us put $l = f([X])$, where $[X]$ denotes the equivalence class of the polynomial $X \in K[X]$. It follows at once that l is a root of $p(X)$ since

$$p(l) = p\Big(f([X])\Big) = f\Big(p([X])\Big) = f\Big([p(X)]\Big) = f(0) = 0$$

since f, as a homomorphism of K-algebras, fixes the elements of K, thus the coefficients of $p(X)$.

Starting with a root l of $p(X)$, it is immediate that $\mathsf{ev}_l([X]) = l$. Next, beginning with f as above, for every polynomial $q(X) \in K[X]$,

$$\mathsf{ev}_{f([X])}\Big([q(X)]\Big) = q\Big(f([X])\Big) = f\Big(q([X])\Big) = f\Big([q(X)]\Big),$$

again since f fixes K, thus the coefficients of $q(X)$. □

Theorem 2.2.6 *Let $K \subset L$ be a field extension and A a K-algebra. The homomorphisms of K-algebras $A \longrightarrow L$ are linearly independent over K, in the vector space of K-linear maps $A \longrightarrow L$.*

Proof By corollary 2.2.3,

$$\mathsf{Hom}_K(A, L) \cong \mathsf{Hom}_L(L \otimes_K A, L),$$

from which it suffices to prove that for every L-algebra B, the homomorphisms of L-algebras $B \longrightarrow L$ are linearly independent over L, from which, a fortiori, the linear independence over K follows.

Every homomorphism of L-algebras $f\colon B \longrightarrow L$ is surjective, because given $l \in L$, one has $l = l \cdot 1 = l \cdot f(1) = f(l \cdot 1)$. As a consequence, $L \cong B/\mathsf{Ker}\, f$ where, by corollary 2.1.2, $\mathsf{Ker}\, f$ is a maximal ideal of B. If $f, g\colon B \longrightarrow\!\!\!\!\rightarrow L$ are distinct homomorphisms of B-algebras, they are thus quotient maps and therefore their kernels must be distinct; by maximality of these kernels, $\mathsf{Ker}\, f + \mathsf{Ker}\, g = B$. Let us then consider a finite family $f_i\colon B_i \longrightarrow\!\!\!\!\rightarrow L$ of distinct homomorphisms of K-algebras, such that $\sum_{1\leq i\leq n} l_i f_i = 0$, for some $l_i \in L$. The Chinese lemma applies (see 2.1.12), thus the map

$$B \longrightarrow L^n, \quad b \mapsto \big(f_i(b_i)\big)_{1\leq i\leq n}$$

is surjective. If at least one l_i is non zero, the equation $\sum_{1\leq i\leq n} l_i X_i = 0$ is that of a proper linear subspace of L^n and, since $\sum_{1\leq i\leq n} l_i f_i = 0$, this proper subspace contains the image of the previous map, which contradicts its surjectivity. Therefore all l_i are zero. □

2.3 Split algebras

In the first chapter, we were interested in Galois extensions of fields, that is, algebraic field extensions $K \subseteq L$ such that the minimal polynomial $p(X) \in K[X]$ of each element $l \in L$ factors in $L[X]$ into factors of degree 1 with distinct roots. This recollection indicates at once the spirit of the next definition.

Definition 2.3.1 Let $K \subseteq L$ be a field extension and A a K-algebra. The extension L splits the K-algebra A when

(i) the algebra A is algebraic over K,
(ii) the minimal polynomial $p(X) \in K[X]$ of every element of A factors in $L[X]$ into factors of degree 1 with distinct roots.

The K-algebra A is an étale K-algebra when it is split by the algebraic closure of K.

Proposition 2.3.2 *Let $K \subseteq L$ be a field extension. The following conditions are equivalent:*

(i) *$K \subseteq L$ is a Galois extension;*
(ii) *the extension L splits the K-algebra L.* □

Theorem 2.3.3 *Let $K \subseteq L$ be a field extension of finite dimension m and A a K-algebra of finite dimension n. The following conditions are equivalent:*

(i) *the extension L splits the K-algebra A;*
(ii) *the following map, called the "Gelfand transformation", is an isomorphism of L-algebras –*

$$\mathsf{Gel}\colon L \otimes_K A \longrightarrow L^{\mathsf{Hom}_L(L\otimes_K A, L)},$$
$$l \otimes a \mapsto \big(f(l\otimes a)\big)_{f\in \mathsf{Hom}_L(L\otimes_K A,L)};$$

(iii) *the following map is an isomorphism of L-algebras –*

$$L \otimes_K A \longrightarrow L^{\mathsf{Hom}_K(A,L)}, \quad l\otimes a \mapsto \big(lg(a)\big)_{g\in \mathsf{Hom}_K(A,L)};$$

(iv) $\#\mathsf{Hom}_L(L\otimes_K A, L) = n$;
(v) $\#\mathsf{Hom}_K(A, L) = n$;
(vi) *$L\otimes_K A$ is isomorphic to L^n as an L-algebra;*
(vii) $\forall x \in L\otimes_K A,\ x \neq 0,\ \exists f \in \mathsf{Hom}(L\otimes_K A, L)$ *such that* $f(x) \neq 0$;

where $\#$ is the cardinality symbol.

Proof The vector space of K-linear maps $L\otimes_K A \longrightarrow L$ has dimension $(mn)m$ over K, thus by 2.2.6 $\mathsf{Hom}_L(L\otimes_K L, L)$ is finite. By proposition 2.1.6, the algebra A is algebraic over K. Putting $B = L\otimes_K A$ in the proof of theorem 2.2.6 yields at once the surjectivity of the Gelfand transformation. For the sake of clarity, we split the proof into three lemmas.

Lemma 2.3.4 *Conditions* (ii) *to* (vii) *of theorem 2.3.3 are equivalent.*

Proof The equivalence of (ii), (iii) and the equivalence of (iv), (v) follow at once from corollary 2.2.3.

(ii) $\Rightarrow$ (iv) The K-vector space $L\otimes_K A$ has dimension mn and the K-vector space $L^{\mathsf{Hom}(L\otimes_K A, L)}$ has dimension $m\cdot\#\mathsf{Hom}(L\otimes_K A, L)$. If the Gelfand transformation is an isomorphism, the equality of these dimensions yields $n = \#\mathsf{Hom}(L\otimes_K A, L)$. This also proves (ii) $\Rightarrow$ (vi).

(iv) $\Rightarrow$ (ii) We know already that the Gelfand transformation is surjective; if its domain and codomain have the same finite dimension, it is an isomorphism.

(vi) $\Rightarrow$ (iv) We must prove that $\#\mathsf{Hom}_L(L^n, L) = n$. Observe that the projections $p_i\colon L^n \longrightarrow L$ constitute n distinct homomorphisms of L-algebras, linearly independent over L by theorem 2.2.6. Since the

space $\mathsf{Lin}_L(L^n, L)$ of all L-linear maps has dimension n, the p_i are all the morphisms of L-algebras, again by theorem 2.2.6.

(ii) $\Leftrightarrow$ (vii) Condition (vii) expresses precisely the injectivity of the Gelfand transformation, which is already known to be surjective. □

Lemma 2.3.5 *In the conditions of theorem 2.3.3, the class of those K-algebras satisfying the equivalent conditions* (ii) *to* (vii) *is stable under subobjects, quotients, finite products and tensor products. Moreover if a K-algebra A admits two subalgebras A_1, A_2 satisfying conditions* (ii) *to* (vii), *the same holds for the subalgebra of A generated by the elements of A_1 and A_2.*

Proof Condition (vii) is trivially stable under subobjects.

Consider now a quotient $A \twoheadrightarrow Q$ of a K-algebra A of dimension n, which satisfies conditions (ii) to (vii) of theorem 2.3.3. Since tensoring with L has a right adjoint by proposition 2.2.2, it preserves quotients, from which we obtain a quotient of L-algebras

$$L^n \cong L \otimes_K A \twoheadrightarrow L \otimes_K Q.$$

By proposition 2.1.13, the kernel of this second quotient is an ideal $J \subseteq L^n$ of the form

$$J = \{(l_i)_{1 \leq i \leq n} | \forall i \in X \; l_i = 0\}, \quad X \subseteq \{1, \ldots, n\}.$$

Putting $x = \#X$, we get $L \otimes_K Q \cong L^n/J \cong L^{n-x}$ and by condition (vi) of theorem 2.3.3, it remains to prove that Q has dimension $n-x$ over K. Since L has dimension m over K and L^n/J has dimension $n-x$ over L, it follows that L/J has dimension $m(n-x)$ over K. On the other hand $L \otimes_K Q$ has dimension $m \cdot \dim_K Q$ over K, from which $\dim_K Q = n - x$ since $L \otimes_K Q \cong L^n/J$.

To treat the case of finite products, observe first that tensoring with L is an additive, thus finite product preserving, functor

$$L \otimes_K - : \mathsf{Vect}_K \longrightarrow \mathsf{Vect}_L$$

between categories of vector spaces. Therefore if A, A' are K-algebras of respective dimensions n, n' and satisfying conditions (ii) to (vii) of theorem 2.3.3, then $A \times A'$ has dimension $n + n'$ and

$$L \otimes_K (A \times A') \cong (L \otimes_K A) \times (L \otimes_K A') \cong L^n \times L^{n'} \cong L^{n+n'}.$$

Thus condition (vi) is satisfied by $A \times A'$.

For the tensor product, with the same notation and applying once more the fact that tensoring with L commutes with finite products, $A \otimes_K A'$ has dimension nn' and

$$\begin{aligned} L \otimes_K (A \otimes_K A') &\cong (L \otimes_K A) \otimes_K A' \cong L^n \otimes_K A' \\ &\cong (L \otimes_K A')^n \cong \left(L^{n'}\right)^n \cong L^{nn'}. \end{aligned}$$

Again condition (vi) of theorem 2.3.3 is satisfied by $A \otimes_K A'$.

To prove the last assertion, observe that the subalgebra generated by A_1 and A_2 is precisely

$$A_1 \cdot A_2 = \left\{ \sum_{i=1}^{k} a_i^1 a_i^2 \middle| a_i^1 \in A_1, \quad a_i^2 \in A_2 \right\}.$$

This algebra can be presented as a quotient

$$A_1 \otimes_K A_2 \twoheadrightarrow A_1 \cdot A_2, \quad a_1 \otimes a_2 \mapsto a_1 a_2,$$

from which the result follows by the previous parts of the proof. □

Lemma 2.3.6 *In the conditions of theorem 2.3.3, L splits the K-algebra A if and only if its Gelfand transformation is an isomorphism. That is, conditions* (i) *and* (ii) *of theorem 2.3.3 are equivalent.*

Proof (i) ⇒ (ii) Let $a \in A$ have minimal polynomial $p(X) \in K[X]$ of degree n. In L, $p(X)$ admits n distinct roots, thus $\#\mathsf{Hom}_K\big(K(a), L\big) = n$. Applying propositions 2.1.10 and 2.2.5, we deduce that $K(a) \cong \frac{K[X]}{\langle p(X) \rangle}$ satisfies condition (v) of theorem 2.3.3, thus condition (ii) by lemma 2.3.4. Since A is finite dimensional over K, it is the K-algebra generated by finitely many such subalgebras $K(a_i)$, from which one deduces the conclusion by the last assertion in lemma 2.3.5, iterated finitely many times.

(ii) ⇒ (i) Write $p(X) \in K[X]$ for the minimal polynomial, with degree n, of a given element $a \in A$. One has $\frac{K[X]}{\langle p(X) \rangle} \cong K(a)$ by proposition 2.1.10 and $K(a) \subseteq A$ satisfies condition (ii) of theorem 2.3.3 by assumption on A and lemma 2.3.5 (stability under subobjects). By lemma 2.3.4, it follows that $\#\mathsf{Hom}_K\left(\frac{K[X]}{\langle p(X) \rangle}, L\right) = n$ which implies, by proposition 2.2.5, that $p(X)$ has n distinct roots in L. □

2.4 The Galois equivalence

Let us recall that given a group G, whose composition law is written multiplicatively, a left G-set is a set X provided with a left action of G

$$G \times X \longrightarrow X, \quad (g, x) \mapsto gx$$

which satisfies the axioms $1x = x$ and $g(g'x) = (gg')x$, for all elements $x \in X$ and $g, g' \in G$. A morphism $f\colon X \longrightarrow Y$ of left G-sets is a map $f\colon X \longrightarrow Y$ which respects the action of G, that is, $f(gx) = gf(x)$ for all $x \in X$ and $g \in G$. Let us observe that G itself becomes a G-set with the multiplication of G as action. For a group G, we write G-Set for the category of left G-sets and their morphisms, and G-Set_f for the full subcategory of finite left G-sets. From now on, we shall refer to left G-sets just as G-sets.

Proposition 2.4.1 *Let G be a group. There exists a bijection between*

- *the subgroups of G,*
- *the quotients of the G-set G.*

This bijection puts a subgroup H in correspondence with the quotient G-set G/H.

Proof With every subgroup $H \subseteq G$ is associated the equivalence relation

$$x \equiv y \quad \text{iff} \quad x^{-1}y \in H;$$

the quotient set is written G/H. This quotient set can easily be provided with the structure of a G-set, by putting $g[x] = [gx]$, for all elements $g, x \in G$. This definition is easily seen to be independent of the choice of x in the equivalence class $[x]$: indeed, if $x \equiv y$, then

$$(gx)^{-1}(gy) = x^{-1}g^{-1}gy = x^{-1}y \in H$$

from which $[gx] = [gy]$. By construction, the projection $G \twoheadrightarrow G/H$ is a morphism of G-sets.

Observe that $1 \equiv x$ precisely when $x \in H$, that is, $H = [1]$.

Conversely, starting with a quotient $p\colon G \twoheadrightarrow Q$ of G-sets, let us consider the equivalence class $[1]$ of the unit of G. It follows at once that $[1]$ is a subgroup of G. Indeed if $x, y \in [1]$,

$$[x^{-1}] = [x^{-1}1] = x^{-1}[1] = x^{-1}[x] = [x^{-1}x] = [1],$$
$$[xy] = x[y] = x[1] = [x1] = [x] = [1].$$

Observe finally that the quotient Q of G is that induced by the subgroup $[1]$. Indeed, if $[x] = [y]$,

$$[x^{-1}y] = x^{-1}[y] = x^{-1}[x] = [x^{-1}x] = [1]$$

and on the other hand if $x^{-1}y \in [1]$,

$$[y] = [xx^{-1}y] = x[x^{-1}y] = x[1] = [x1] = [x]. \qquad \square$$

Proposition 2.4.2 *Let G be a group. Every G-set X is a sum of quotients of the G-set G. When X is finite, this sum is finite.*

Proof A sum of G-sets is their disjoint union, with the original action of G on each piece of the disjoint union. Given $x \in X$, it follows at once that

$$Gx = \{gx | g \in G\}$$

is a sub-G-set of X isomorphic to a quotient of the G-set G, that is,

$$G \longrightarrow\!\!\!\!\!\rightarrow Gx, \quad g \mapsto gx.$$

If $y \in X \setminus Gx$, observe that Gx and Gy are disjoint. Indeed, $gx = g'y$ would imply $y = (g')^{-1}gx \in Gx$. The result follows at once. $\square$

Theorem 2.4.3 (Galois theorem) *Let $K \subseteq L$ be a finite dimensional Galois extension of fields. Let us write $\mathsf{Gal}\,[L : K]$ for the group of K-automorphisms of L and $\mathsf{Gal}\,[L : K]\text{-}\mathsf{Set}_f$ for the category of finite $\mathsf{Gal}\,[L : K]$-sets. Let us also write $\mathsf{Split}_K(L)_f$ for the category of those finite dimensional K-algebras which are split by L. The functor on $\mathsf{Split}_K(L)_f$, represented by L, factors through the category $\mathsf{Gal}\,[L : K]\text{-}\mathsf{Set}_f$:*

$$\mathsf{Hom}_K(-, L) \colon \mathsf{Split}_K(L)_f \longrightarrow \mathsf{Gal}\,[L : K]\text{-}\mathsf{Set}_f, \quad A \mapsto \mathsf{Hom}_K(A, L)$$

with $\mathsf{Gal}\,[L : K]$ acting by composition on $\mathsf{Hom}_K(L)$. This factorization functor is a contravariant equivalence of categories.

Proof The action of $\mathsf{Gal}\,[L : K]$ is thus given by

$$\mathsf{Gal}\,[L : K] \times \mathsf{Hom}_K(A, L) \longrightarrow \mathsf{Hom}_K(A, L), \quad (g, f) \mapsto g \circ f.$$

For the sake of clarity, we split the proof into five lemmas. Lemmas 2.4.6, 2.4.7 and 2.4.8 imply the result at once. $\square$

Lemma 2.4.4 *In the conditions of theorem 2.4.3, for every algebra* $A \in \mathsf{Split}_K(L)_f$, *we get the structure of a* $\mathsf{Gal}\,[L:K]$*-set on* $L \otimes_K A$ *by putting*

$$\mathsf{Gal}\,[L:K] \times (L \otimes_K A) \longrightarrow L \otimes_K A, \quad (g, l \otimes a) \mapsto g(l) \otimes a.$$

Via the Gelfand isomorphism of theorem 2.3.3, this action becomes

$$\mathsf{Gal}\,[L:K] \times L^{\mathsf{Hom}_K(A,L)} \longrightarrow L^{\mathsf{Hom}_K(A,L)},$$
$$(g, \varphi) \mapsto \Big[f \mapsto g\big(\varphi(g^{-1} \circ f)\big)\Big]$$

where $\varphi\colon \mathsf{Hom}_K(A,L) \longrightarrow L$ *and* $f \in \mathsf{Hom}_K(A,L)$.

Proof Let us fix an element $g \in \mathsf{Gal}\,[L:K]$ and consider the morphism

$$\gamma\colon L^{\mathsf{Hom}_K(A,L)} \longrightarrow L^{\mathsf{Hom}_K(A,L)}, \quad \big(\gamma(\varphi)\big)(f) = g\big(\varphi(g^{-1} \circ f)\big).$$

One computes at once that

$$\begin{aligned}
\Big((\gamma \circ \mathsf{Gel})(l \otimes a)\Big)(f) &= \Big(\gamma\big(\mathsf{Gel}(l \otimes a)\big)\Big)(f) \\
&= g\Big(\mathsf{Gel}(l \otimes a)(g^{-1} \circ f)\Big) \\
&= g\Big(l\big((g^{-1} \circ f)(a)\big)\Big) \\
&= g\Big(lg^{-1}\big(f(a)\big)\Big) \\
&= g(l)gg^{-1}\big(f(a)\big) \\
&= g(l)f(a) \\
&= \mathsf{Gel}\Big((g \otimes \mathsf{id})(l \otimes a)\Big)(f) \\
&= \Big(\big(\mathsf{Gel} \circ (g \otimes \mathsf{id})\big)(l \otimes a)\Big)(f).
\end{aligned}$$

This proves the commutativity of the diagram

$$\begin{array}{ccc}
L \otimes_K A & \xrightarrow[\cong]{\mathsf{Gel}} & L^{\mathsf{Hom}_K(A,L)} \\
{\scriptstyle g \otimes \mathsf{id}}\downarrow & & \downarrow{\scriptstyle \gamma} \\
L \otimes_K A & \xrightarrow[\mathsf{Gel}]{\cong} & L^{\mathsf{Hom}_K(A,L)}
\end{array}$$

and this expresses precisely the equivalence between the two formulations of the statement.

The fact of having the structure of a $\mathsf{Gal}\,[L:K]$-set is obvious. □

Lemma 2.4.5 *In the conditions of theorem 2.4.3, for every algebra* $A \in \mathsf{Split}_K(L)_f$*, one has*

$$\begin{aligned} A &\cong \mathsf{Fix}_{\mathsf{Gal}[L:K]}(L \otimes_K A) \\ &= \left\{ x \in L \otimes_K A \middle| \forall g \in \mathsf{Gal}[L:K]\ (g \otimes \mathsf{id})(x) = x \right\}. \end{aligned}$$

Proof First of all let us identify A with a subset of $L \otimes_K A$ via the inclusion

$$A \cong K \otimes_K A \rightarrowtail L \otimes_K A, \quad a \mapsto 1 \otimes a.$$

(Every vector space is flat: tensoring with a vector space preserves monomorphisms.) For every $g \in \mathsf{Gal}[L:K]$, one obviously gets $(g \otimes \mathsf{id})(1 \otimes a) = 1 \otimes a$, which proves already that $A \subseteq \mathsf{Fix}_{\mathsf{Gal}[L:K]}(L \otimes_K A)$.

To prove the equality, let us recall that the K-algebra A is finite dimensional over K, thus, as a K-vector space, is isomorphic to K^n for some $n \in \mathbb{N}$. Let us consider the commutative diagram

$$\begin{array}{ccc} L \otimes_K K^n & \xrightarrow{g \otimes \mathsf{id}} & L \otimes_K K^n \\ \cong \downarrow & & \downarrow \cong \\ L^n & \xrightarrow[g^n]{} & L^n \end{array}$$

for every $g \in \mathsf{Gal}[L:K]$. It reduces the problem to considering those points of L^n which are fixed by all g^n. With the notation of section 1.4 and by the classical Galois theorem (see 1.4.5),

$$\mathsf{Fix}_{\mathsf{Gal}[L:K]}(L \otimes KK^n) \cong \left(\mathsf{Fix}\left(\mathsf{Gal}[L:K]\right)\right)^n \cong K^n.$$

Remembering the form of the isomorphism

$$L^n \xrightarrow{\cong} L \otimes_K K^n, \quad (l_i)_{1 \le i \le n} \mapsto \sum_{i=1}^{n} l_i \otimes e_i,$$

where e_i is the ith vector of the canonical basis of K^n, we obtain

$$\begin{aligned} \mathsf{Fix}_{\mathsf{Gal}[L:K]}(L \otimes_K K^n) &\cong \left\{ \sum_{i=1}^{n} k_i \otimes e_i \middle| k_i \in K \right\} \\ &\cong \left\{ 1 \otimes \left(\sum_{i=1}^{n} k_i e_i \right) \middle| k_i \in K \right\} \\ &\cong A \end{aligned}$$

which concludes the proof.

Lemma 2.4.6 *The functor described in theorem 2.4.3 is full.*

Proof Let us fix two K-algebras A and B in $\mathsf{Split}_K(L)$, and a morphism of $\mathsf{Gal}\,[L:K]$-sets

$$\varphi\colon \mathsf{Hom}_K(B,L) \longrightarrow \mathsf{Hom}_K(A,L).$$

This yields at once a map

$$\begin{aligned} L^{\varphi}\colon L^{\mathsf{Hom}_K(A,L)} &\longrightarrow L^{\mathsf{Hom}_K(B,L)},\\ (l_f)_{f\in\mathsf{Hom}_K(A,L)} &\mapsto (l_{\varphi(h)})_{h\in\mathsf{Hom}_K(B,L)}. \end{aligned}$$

In lemma 2.4.4, we described the structures of $\mathsf{Gal}\,[L:K]$-sets on these powers of L; let us observe that L^{φ} is a morphism of $\mathsf{Gal}\,[L:K]$-sets for these structures. Indeed, let $g \in \mathsf{Gal}\,[L:K]$; to avoid ambiguity with taking the image under the map g, let us write $*$ for the action of g on the $\mathsf{Gal}\,[L:K]$-sets. One has

$$\begin{aligned} L^{\varphi}\left(g * (l_f)_{f\in\mathsf{Hom}_K(A,L)}\right) &= L^{\varphi}\left(g(l_{g^{-1}\circ f})\right)_{f\in\mathsf{Hom}_K(A,L)}\\ &= \left(g(l_{g^{-1}\circ\varphi(h)})\right)_{h\in\mathsf{Hom}_K(B,L)}\\ &= g * \left(l_{\varphi(h)}\right)_{h\in\mathsf{Hom}_K(B,L)}\\ &= g * L^{\varphi}\left((l_f)_{f\in\mathsf{Hom}_K(A,L)}\right). \end{aligned}$$

Since L^{φ} is a morphism of $\mathsf{Gal}\,[L:K]$-sets, it factors through the corresponding $\mathsf{Gal}\,[L:K]$-subset of those points which are fixed by the action of every element g. By lemma 2.4.5 and using the Gelfand isomorphism of theorem 2.3.3, this yields the following situation:

$$\begin{array}{ccccc} A & \xrightarrow{\cong} & \mathsf{Fix}_{\mathsf{Gal}\,[L:K]}(L\otimes_K A) & \xrightarrow{\cong} & \mathsf{Fix}_{\mathsf{Gal}\,[L:K]}\left(L^{\mathsf{Hom}_K(A,L)}\right)\\ & & & & \Big\downarrow{\scriptstyle L^{\varphi}}\\ B & \xleftarrow{\cong} & \mathsf{Fix}_{\mathsf{Gal}\,[L:K]}(L\otimes_K B) & \xleftarrow{\cong} & \mathsf{Fix}_{\mathsf{Gal}\,[L:K]}\left(L^{\mathsf{Hom}_K(B,L)}\right) \end{array}$$

Let us write $\psi\colon A \longrightarrow B$ for this composite; we shall prove that $\varphi = \mathsf{Hom}_K(\psi, L)$.

Given $h \in \mathsf{Hom}_K(B,L)$, consider the following diagram:

$$\begin{array}{ccc} L \otimes_K B & \xrightarrow[\cong]{\mathsf{Gel}_B} & L^{\mathsf{Hom}_K(B,L)} \\ \uparrow{\scriptstyle i_B} & & \downarrow{\scriptstyle p_h} \\ B & \xrightarrow[h]{} & L \end{array}$$

where $i_B(b) = 1 \otimes b$ and p_h is the projection of index h. This diagram is commutative since

$$(p_h \circ \mathsf{Gel}_B \circ i_B)(b) = (p_h \circ \mathsf{Gel}_B)(1 \otimes b) = p_h\left(h'(b)_{h' \in \mathsf{Hom}_K(B,L)}\right) = h(b).$$

Let us also write $\overline{\varphi}\colon L \otimes_K B \longrightarrow L \otimes_K B$ for the morphism corresponding to L^{φ} by the Gelfand isomorphism of theorem 2.3.3. The following diagram is commutative by definition of ψ and $\overline{\psi}$:

$$\begin{array}{ccccc} A & \xrightarrow{i_A} & L \otimes_K A & \xrightarrow[\cong]{\mathsf{Gel}_A} & L^{\mathsf{Hom}_K(A,L)} \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \overline{\varphi}} & & \downarrow{\scriptstyle L^{\varphi}} \\ B & \xrightarrow[i_B]{} & L \otimes_K B & \xrightarrow[\mathsf{Gel}_B]{\cong} & L^{\mathsf{Hom}_K(B,L)} \end{array}$$

It yields

$$\begin{aligned} \mathsf{Hom}_K(\psi, L)(h) &= h \circ \psi \\ &= p_h \circ \mathsf{Gel}_B \circ i_B \circ \psi \\ &= p_h \circ \mathsf{Gel}_B \circ \overline{\varphi} \circ i_A \\ &= p_h \circ L^{\varphi} \circ \mathsf{Gel}_A \circ i_A \\ &= p_{\varphi(h)} \circ \mathsf{Gel}_A \circ i_A \\ &= \varphi(h), \end{aligned}$$

which concludes the proof. □

Lemma 2.4.7 *The functor described in theorem 2.4.3 is faithful.*

Proof With the notation of lemma 2.4.6, consider a second morphism $\psi'\colon A \longrightarrow B$ such that $\mathsf{Hom}_K(\psi', L) = \varphi$. For every $h \in \mathsf{Hom}_K(B, L)$,

we get

$$\begin{aligned} p_h \circ \mathsf{Gel}_B \circ i_B \circ \psi' &= h \circ \psi' \\ &= \varphi(h) \\ &= p_{\varphi(h)} \circ \mathsf{Gel}_A \circ i_A \\ &= p_h \circ L^{\varphi} \circ \mathsf{Gel}_A \circ i_A \\ &= p_h \circ \mathsf{Gel}_B \circ i_B \circ \psi. \end{aligned}$$

Since this relation holds for every projection p_h, it follows that

$$\mathsf{Gel}_B \circ i_B \circ \psi' = \mathsf{Gel}_B \circ i_B \circ \psi$$

and since both Gel_B and i_B are injective, $\psi' = \psi$. □

Lemma 2.4.8 *The functor described in theorem 2.4.3 is essentially surjective on the objects.*

Proof Consider first a subgroup $H \subseteq \mathsf{Gal}\,[L : K]$ and the corresponding $\mathsf{Gal}\,[L : K]$-quotient-set $\mathsf{Gal}\,[L : K]/H$ as in proposition 2.4.1. We shall prove that

$$\frac{\mathsf{Gal}\,[L : K]}{H} \cong \mathsf{Hom}_K\big(\mathsf{Fix}\,(H), L\big).$$

Considering the inclusion $\mathsf{Fix}\,(H) \subseteq L$, we get by functoriality a morphism of finite $\mathsf{Gal}\,[L : K]$-sets

$$\rho\colon \mathsf{Gal}\,[L : K] \cong \mathsf{Hom}_K(L, L) \longrightarrow \mathsf{Hom}_K\big(\mathsf{Fix}\,(H), L\big)$$

sending $f\colon L \longrightarrow L$ onto its restriction $f\colon \mathsf{Fix}\,(H) \longrightarrow L$; let us prove that this defines a quotient map. Considering the diagram

$$\begin{array}{ccccc} K & \rightarrowtail & \mathsf{Fix}\,(H) & \rightarrowtail & L \\ \| & & \downarrow & & \vdots \\ K & \rightarrowtail & L & = & L \end{array}$$

and proposition 1.3.3, we conclude already that every morphism of K-algebras $\mathsf{Fix}\,(H) \longrightarrow L$ is indeed the restriction of a morphism $L \longrightarrow L$; thus the map ρ is a quotient map.

To prove that $\mathsf{Hom}_K\big(\mathsf{Fix}\,(H), L\big)$ is precisely the expected quotient $\mathsf{Gal}\,[L : K]/H$, it remains to prove that two morphisms of K-algebras

$f, g\colon L \rightrightarrows L$ have the same restriction to $\mathsf{Fix}(H)$ if and only if $f^{-1} \circ g \in H$. Indeed, f and g have the same restriction to $\mathsf{Fix}(H)$ precisely when $f^{-1} \circ g$ fixes the points of $\mathsf{Fix}(H)$, that is

$$f^{-1} \circ g \in \mathsf{Gal}\big[L : \mathsf{Fix}(H)\big] = H$$

by the classical Galois theorem (see 1.4.5) and using its notation.

Every quotient of the $\mathsf{Gal}[L : K]$-set $\mathsf{Gal}[L : K]$ is thus isomorphic to an object of the form $\mathsf{Hom}_K(A, L)$ for some $A \in \mathsf{Split}_K(L)_f$. On the other hand every finite $\mathsf{Gal}[L : K]$-set is, by proposition 2.4.2, a finite disjoint union of quotients of $\mathsf{Gal}[L : K]$. Since the category $\mathsf{Split}_K(L)_f$ has finite products by lemma 2.3.5, it suffices, for concluding the proof, to prove that the contravariant functor $\mathsf{Hom}_K(-, L)$ of theorem 2.4.3 transforms finite products into finite sums.

Consider for this two algebras $A, B \in \mathsf{Split}_K(L)_f$, of respective dimensions n and m. Composing with the projections

$$A \twoheadleftarrow A \times B \twoheadrightarrow B$$

yields maps

$$\mathsf{Hom}_K(A, L) \rightarrowtail \mathsf{Hom}_K(A \times B, L) \leftarrowtail \mathsf{Hom}_K(B, L)$$

which are injective since the projections are surjective. The corresponding subsets are disjoint, as observed by checking the actions on the elements $(1, 0)$ and $(0, 1)$ of $A \times B$. Theorem 2.3.3 and various previous arguments show that

$$\begin{aligned}
\#\mathsf{Hom}_K(A \times B, L) &= \#\mathsf{Hom}_L\big(L \otimes_K (A \times B), L\big) \\
&= \#\mathsf{Hom}_K\big((L \otimes_K A) \times (L \otimes_K B), L\big) \\
&= \#\mathsf{Hom}_L(L^n \times L^m, L) \\
&= \#\mathsf{Hom}_L(L^{n+m}, L) \\
&= n + m \\
&= \#\mathsf{Hom}_K(A, L) + \#\mathsf{Hom}_K(B, L).
\end{aligned}$$

This concludes the proof of this lemma, thus also the proof of theorem 2.4.3. □

To conclude this chapter, it remains to observe that the Galois theorem we have just proved (theorem 2.4.3) contains the classical Galois theorem (theorem 1.4.5). Indeed, the contravariant equivalence of theorem 2.4.3 implies in particular the existence of an isomorphism between

the lattice of subobjects M

$$K \rightarrowtail M \rightarrowtail L$$

in $\mathsf{Split}_K(L)_f$ and the lattice of quotients $\mathsf{Hom}_K(M, L)$,

$$\mathsf{Gal}\,[L : K] \cong \mathsf{Hom}_K(L, L) \twoheadrightarrow \mathsf{Hom}_K(M, L) \twoheadrightarrow \mathsf{Hom}_K(K, L) \cong \{*\},$$

in $\mathsf{Gal}\,[L : K]$-Set_f. By propositions 2.2.1 and 2.4.1, this is precisely the classical Galois isomorphism.