JOURNAL OF ALGEBRA 119, 1–22 (1988)

On Duality for Skew Field Extensions

JAN TREUR*

Potgieterweg 12, 1851 CH Heiloo, The Netherlands

Communicated by N. Jacobson

Received May 20, 1986

INTRODUCTION

In this paper a duality principle is formulated for statements about skew field extensions of finite (left or right) degree. A proof for this duality principle is given by constructing for every extension L/K of finite degree a dual extension L_1/K_1. These dual extensions are constructed by embedding a given L/K in an inner Galois extension N/K.

The Appendix shows that such an embedding can always be constructed, and introduces the notion of an inner closure N for L/K.

In Section 1 some properties of inner Galois (or bicentral) extensions are mentioned, leading to the notion of a dual extension and the duality theorem.

In Section 2 it is shown that the basic structures of L/K can be described by those of a dual extension L_1/K_1. A survey of this is the translation table at the end of Section 2. Based on these translations the general duality principle is formulated.

In Section 3 we establish dual connections between a number of notions known in the literature. For instance, it appears that cyclic Galois extensions and binomial extensions are duals of each other.

In Section 4 dual connections are used to prove in an easy way some results on cyclic Galois extensions, generalizing Amitsur's results [1].

Compared to [5], in this paper in Section 1 the proofs are much shorter and generalized to the new notion of a predual extension. In Sections 2 and 4 derivations are also handled. Section 3 follows some parts of Chapter 7 of [5]. In Section 4 most of the material is new, although some special cases already were handled in [5]. The construction in the Appendix is new.

We continue with some basic terminology. By a field we mean a skew field; we denote fields by K, L, N, D, E with or without subscripts. If $K \subset L$

* I am indebted to Professor P. M. Cohn for reading an earlier version of this paper and giving some useful advice.

0021-8693/88 $3.00

then by $Z_L(K)$ we denote the *centralizer* of K in L, and $Z(K)$ denotes the *center* of K. If $K \subset N$ and $Z_N Z_N(K) = K$ we call K *bicentral* in N (or N/K is inner Galois). The following rules are useful:

$$Z_L(K_2) \subset Z_L(K_1) \qquad \text{whenever} \quad K_1 \subset K_2$$

$$K \subset Z_L Z_L(K)$$

$$Z_L Z_L Z_L(K) = Z_L(K)$$

$$Z_L(K_1 \cdot K_2) = Z_L(K_1) \cap Z_L(K_2)$$

$$\omega Z_L(K) = Z_L(\omega K) \qquad \text{if} \quad \omega \in \mathrm{Aut}(L),$$

The structure of duality implies that one has to deal with a *left-right switch* while dualizing. This means that for every notion we use both the left-form and the right-form whenever one of them is defined. The same for notations: for instance, automorphisms are sometimes written on the left and sometimes on the right of the elements on which they act.

If $t \in N$, by l_t we denote the *left-multiplication* $x \to t \cdot x$, sometimes restricted to a subfield L of N.

An element θ of L^* is called a *left-normalizing* element of L/K if $\theta K \subset K\theta$. If L/K has a left basis consisting of left-normalizing elements we call L/K a *left-normalizing extension* and such a basis a *left-normalizing basis*; in that case the commutation rules for the elements of K with respect to this basis are in diagonal form. Therefore in [5] the word "diagonal" is used for "normalizing." If θ is both a left- and right-normalizing element of L/K, we speak of a *normalizing* element of L/K. The set of these is called the *normalizer* of K^* in L^* and is denoted by $N_{L^*}(K^*)$.

We call L/K a *left G-crossed product* if G is a group and there are given elements θ_i ($i \in G$) in L and $\mu_{i,j}$ ($i, j \in G$) in K such that θ_i, $i \in G$ is a left-normalizing basis of L/K and rules of multiplication $\theta_i \theta_j = \mu_{i,j} \theta_{ij}$ hold for all $i, j \in G$. In that case θ_i, $i \in G$ is called a *G-basis*. Notice that a binomial extension [3, p. 61] is a G-crossed product for a cyclic group G, and that a normalizing basis of the form $1, \theta, \theta^2, ..., \theta^{n-1}$ gives a pseudolinear extension with zero derivation.

1. Dual Extensions

We assume $K \subset L$ and $K \subset N$. By $\mathfrak{L}^l_K(L, N)$ we denote the set of left K-linear maps of L into N. We consider it as a right N-linear space. As in [4, p. 159] we have the following lemma; this lemma gives a relation between some left and right dimensions. Notice that we differentiate between infinite dimensions by considering them as (infinite) cardinalities.

LEMMA 1.1. *Let $K \subset N \subset N_1$ be given. Then the following hold*:

(a) $[L:K]_l \leqq \dim_N^r \mathfrak{L}_K^l(L, N)$.

(b) *Assume, moreover,* $[L:K]_l < \infty$. *Then*

$$[L:K]_l = \dim_N^r \mathfrak{L}_K^l(L, N)$$

$$\mathfrak{L}_K^l(L, N_1) = \mathfrak{L}_K^l(L, N) \cdot N_1.$$

If $\phi_1, ..., \phi_n$ are elements of $\mathfrak{L}_K^l(L, N)$ then these are right independent over N if and only if they are over N_1. They form a basis of $\mathfrak{L}_K^l(L, N)$ over N iff they form a basis of $\mathfrak{L}_K^l(L, N_1)$ over N_1.

Proof. Let e_i, $i \in I$, be a left basis of L/K. The dual elements $e_j^* \in \mathfrak{L}_K^l(L, N)$ defined by the relations $e_j^*(e_i) = 1$ if $i = j$ and zero else are right independent over N. This proves (a).

Now assume $[L:K]_l < \infty$. Then the e_j^*, $j \in I$, form a (dual) basis of $\mathfrak{L}_K^l(L, N)$ over N. Therefore the dimensions are equal; since the same holds for N_1 we have $\mathfrak{L}_K^l(L, N_1) = \mathfrak{L}_K^l(L, N) \cdot N_1$.

Finally, suppose $\phi_1, ..., \phi_n \in \mathfrak{L}_K^l(L, N)$ are right independent over N. Extend them to a basis of $\mathfrak{L}_K^l(L, N)$ over N. This basis spans $\mathfrak{L}_K^l(L, N_1)$ as a right N_1-space, hence must be independent over N_1 too. ▮

From now on we assume $K \subset L \subset N$ and $K_1 = Z_N(L)$, $L_1 = Z_N(K)$. Every element $t \in L_1$ induces the left K-linear mapping $l_t: x \to t \cdot x$ from L into N. These l_t for $t \in L_1$ span a right N-space $\mathfrak{A} \subset \mathfrak{L}_K^l(L, N)$. The following lemma gives a link between L_1 and $\mathfrak{L}_K^l(L, N)$ using these left multiplications.

LEMMA 1.2. $\dim_N^r \mathfrak{A} = [L_1 : K_1]_r$. *In particular, if $t_i \in L_1$ for $i \in I$, then the following are equivalent*:

(i) *t_i, $i \in I$, are right independent over K_1.*

(ii) *l_{t_i}, $i \in I$, are right independent over N.*

(iii) *the K-homomorphisms $\omega_i: L \to N$ given by $x \to t_i x t_i^{-1}$ are right independent over N.*

Furthermore, if $[L:K]_l < \infty$ then $[L_1 : K_1] \leqq [L:K]_l$.

Proof. (i) $\Rightarrow$ (ii) Suppose l_{t_i}, $i \in I$, are dependent over N. Then we can find $\lambda_i \in N$, not all zero, such that $\sum l_{t_i} \cdot \lambda_i = 0$, $\lambda_{i_0} = 1$ for some i_0, and such that $\{i \in I \mid \lambda_i \neq 0\}$ is minimal. Let $x \in L$ be given; for any $y \in L$ we have

$$\sum t_i x \cdot y \lambda_i = \sum l_{t_i}(xy)\, \lambda_i = 0$$

$$\sum t_i x \cdot \lambda_i y = \sum l_{t_i}(x)\, \lambda_i \cdot y = 0.$$

From minimality it follows that for every $i \in I$ and $y \in L$, $y\lambda_i = \lambda_i y$. Therefore $\lambda_i \in K_1$. Now take $x = 1$.

(ii) $\Rightarrow$ (i) Suppose t_i, $i \in I$, are right dependent elements of L_1 over K_1, say $\sum t_i \lambda_i = 0$ for some $\lambda_i \in K_1$. Then for any $x \in L$ we have

$$\sum l_{t_i}(x)\, \lambda_i = \sum t_i x \lambda_i = \sum t_i \lambda_i x = 0.$$

Hence the l_{t_i}, $i \in I$, are dependent over N.

(ii) $\Rightarrow$ (iii) This is easy; the remainder follows from 1.1. ∎

Combining 1.1 and 1.2 we see that something special happens in case $[L:K]_l = [L_1:K_1]_r$. The following theorem shows that this is the case if K is bicentral in N. This generalizes Corollary 2 of p. 49 of [3].

THEOREM 1.3. *Let $K \subset L \subset N$ be a chain of fields with K bicentral in N. With $K_1 = Z_N(L)$ and $L_1 = Z_N(K)$ we have*:

(a) *The following are equivalent*:

(i) $[L:K]_l < \infty$,

(ii) $[L_1:K_1]_r < \infty$,

(iii) $\dim^r_N \mathfrak{A} < \infty$,

(iv) $\dim^r_N \mathfrak{L}^l_K(L, N) < \infty$.

(b) *If* (i)–(iv) *of* (a) *are satisfied, then*

$$[L:K]_l = [L_1:K_1]_r$$
$$\mathfrak{A} = \mathfrak{L}^l_K(L, N)$$

and L is bicentral in N.

Proof. (a) (i) $\Rightarrow$ (ii) $\Leftrightarrow$ (iii) follows from 1.2. (iv) $\Leftrightarrow$ (i) follows from 1.1.

We prove (ii) $\Rightarrow$ (i) and (b). Apply 1.2 to L_1/K_1 and L/K:

$$[Z_N(K_1) : Z_N(L_1)]_l \leqq [L_1 : K_1]_r \leqq [L:K]_l.$$

Since $Z_N(L_1) = K$ and $L \subset Z_N(K_1)$ we have

$$[L:K]_l \leqq [Z_N(K_1):K]_l = [Z_N(K_1) : Z_N(L_1)]_l.$$

We see (i) holds and (b). ∎

We come to the following notions:

DEFINITION. We call L/K and L_1/K_1 *dual* (*in* N) if

$$K_1 = Z_N(L), \qquad K = Z_N(L_1)$$
$$L_1 = Z_N(K), \qquad L = Z_N(K_1).$$

We call L_1/K_1 a *left predual* of L/K (in N) if $[L:K]_l = [L_1:K_1]_r < \infty$.

We also say "L_1/K_1 is a dual of L/K" or "L/K has a dual in N." In the following proposition it is established in (iii) that in case $[L:K]_l < \infty$ duality implies preduality.

PROPOSITION 1.4. *Assume $K \subset L \subset N$ and $K_1 = Z_N(L)$, $L_1 = Z_N(K)$.*

(a) *The following hold*:

$$Z(K) = K \cap L_1 \subset Z(L_1)$$
$$Z(L) = L \cap K_1 \subset Z(K_1)$$
$$Z_L(K) = L \cap L_1 \subset Z_{L_1}(K_1).$$

If L/K and L_1/K_1 are dual in N then the inclusions are equalities.

(b) *Assume $[L:K]_l < \infty$. Then*:

(i) *L_1/K_1 is a left predual of L/K if and only if $\mathfrak{A} = \mathfrak{L}^l_K(L, N)$.*

(ii) *L/K and L_1/K_1 are dual in N if and only if K is bicentral in N.*

(iii) *L/K and L_1/K_1 are dual in N if and only if*

$$L_1/K_1 \text{ is a left predual of } L/K$$

and

$$L/K \text{ is a right predual of } L_1/K_1.$$

Proof. (a) This is easy to verify.

(b) Part (i) follows from 1.1 and 1.2; (ii) and (iii) follow from 1.3. ∎

Notice that the notion of dual extension is right-left symmetric, so if both $[L:K]_l$ and $[L:K]_r$ are finite, and L_1/K_1 is a dual of L/K, then L_1/K_1 is a right and left predual of L/K.

The following proposition asserts that, if L/K has a left predual in N, then L/K also has a left predual in any extension of N; it follows from 1.1 and 1.2.

PROPOSITION 1.5. *Assume L/K has a left predual L_1/K_1 in N, $t_i \in L_1$ for $i \in I$ and $N_0 = L(t_i; i \in I)$. For $N_1 \supset N_0$ the following are equivalent*:

(i) *t_i, $i \in I$, are right independent elements of $Z_{N_1}(K)$ over $Z_{N_1}(L)$.*

(ii) *l_{t_i}, $i \in I$, are right independent elements of $\mathfrak{L}^l_K(L, N_1)$ over N_1.*

(iii) *t_i, $i \in I$, are right independent elements of L_1 over K_1.*

The same equivalence hold if "independent elements" is replaced by "basis." In particular L/K has a left predual in N_0 and in every extension of N. ∎

Theorem 1.3 is one of the two fundamental steps to construct dual extensions. The other step is the construction of inner closures (see Appendix). This enables us to formulate:

DUALITY THEOREM 1.6. (a) *Existence. Every L/K can be embedded in an N such that L/K has a dual in N.*

(b) *Dual correspondence. Suppose L/K has a left predual L_1/K_1 in N, and Φ and Φ_1 are the lattices of intermediate fields of L/K and L_1/K_1. Then*

$$\phi: D \to Z_N(D)$$

is an injective anti-homomorphism of Φ into Φ_1 and

$$[\phi(D) : \phi(E)]_r = [E : D]_l$$

for all $D, E \in \Phi$ with $D \subset E$; in this case $\phi(D)/\phi(E)$ is a left predual of E/D. If, moreover, L/K and L_1/K_1 are dual in N then ϕ is an anti-isomorphism between Φ and Φ_1 with inverse $D_1 \to Z_N(D_1)$ and for every $D, E \in \Phi$ with $D \subset E$, $\phi(D)/\phi(E)$ and E/D are dual in N.

(c) *Uniqueness. Suppose L/K has a left predual in N. Then N can be extended to an N_1 such that L/K has a dual in N_1. Assume such an N_1 is given, and L_2/K_2 is the dual of L/K in N_1. If ϕ_i is the lattice of intermediate fields of L_i/K_i then $D_2 \to D_2 \cap N$ is an injective homomorphism of Φ_2 in Φ_1 which preserves right degrees, with one-sided inverse $D_1 \to K_2 \cdot D_1$. Any right basis of such D_1/K_1 is also a basis of $K_2 \cdot D_1/K_2$. Moreover, if L_1/K_1 is also a dual of L/K, then $D_2 \to D_2 \cap N$ is an isomorphism between Φ_2 and Φ_1 with inverse $D_1 \to K_2 \cdot D_1$.*

Proof. (a) *Existence.* This follows from the inner closure construction (see Appendix).

(b) *Dual correspondence.* The case that L/K and L_1/K_1 are dual in N follows from 1.3. General case: also from 1.3 it follows that any N_1 such that N/K has a dual in N_1 provides a dual extension of L/K, say L_2/K_2. If $D, E \in \Phi$ with $D \subset E$, then from a comparison according to 1.2,

$$[L : E]_l [E : D]_l [D : K]_l \geq [L_1 : \phi(D)]_r [\phi(D) : \phi(E)]_r [\phi(E) : K_1]_r,$$

it follows that these degrees must be equal, so $\phi(D)/\phi(E)$ is a left predual of

E/D. Therefore any right basis of $\phi(D)/\phi(L)$ is a right basis of $Z_{N_1}(D)/Z_{N_1}(L)$. From this it follows that ϕ is injective in the general case that L/K has a left predual in N.

(c) *Uniqueness.* In (b) we saw the first part of (c). Suppose L/K has a left predual in N and a dual L_2/K_2 in $N_1 \supset N$. If $D_2 \in \Phi_2$, then $D_2 = Z_{N_1}(D)$ for some $D = Z_{N_1}(D_2) \in \Phi$, and $D_2 \cap N = Z_N(D)$. Therefore $D_2 \to Z_{N_1}(D_2) \to Z_N Z_{N_1}(D_2) = D_2 \cap N$ is an injective homomorphism $\Phi_2 \to \Phi_1$ which preserves right degrees. From Proposition 1.5 it follows that any basis of $D_2 \cap N = Z_N(D)$ over K_1 is a basis of D_2 over K_2. Therefore $K_2 \cdot (D_2 \cap N) = D_2$. In case L_1/K_1 is a dual of L/K, it is clear we have an isomorphism. ∎

In Section 2 we will give a dual description of some more of the structure of L/K. This will give a more far-reaching uniqueness of the dual extension of L/K: all basic structures of one dual L_1/K_1 are in some sense isomorphic to those of another dual L_2/K_2.

2. Dualizing Basic Structures

The purpose of this section is to get a survey of how the basic structures of L/K can be translated (dualized) to basic structures of a dual L_1/K_1 of L/K. We already have the link between the centers and centralizer of L/K and those of L_1/K_1 given by Proposition 1.4(a). Further we have the general link between intermediate fields of L/K and those of L_1/K_1 given by the Duality Theorem 1.6. In this section we successively go into the following basic structures:

A. More specific intermediate fields of L/K in relation with specific intermediate fields of L_1/K_1.

B. K-homomorphisms, K-derivations, and other K-linear maps in relation with elements of L_1/K_1.

These structures are only well dualizable in dual extensions and in case of finite degree. In case of preduality, essential points miss.

As before we work with given $K \subset L \subset N$ and $K_1 = Z_N(L)$, $L_1 = Z_N(K)$.

A. *More Specific Intermediate Fields.*

In handling a general L/K, sometimes it is easier to split L/K into parts that are easier to handle. Many examples of this strategy can be found in the literature. A closer look at these examples shows us that two types of decomposing L/K are often used:

$K \subset K \cdot Z_L(K) \subset L$ (see, for instance, [3, p. 61, Theorem 3.4.2])

$K \subset Z_L Z_L(K) \subset L$ (see, for instance, [3, p. 52, Corollary]).

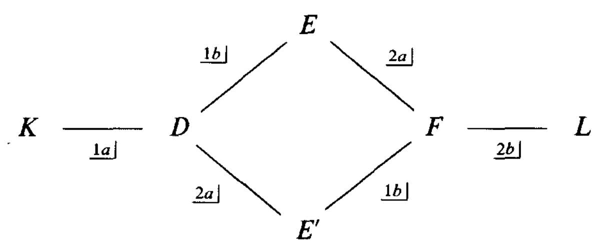
Notice that these specific intermediate fields are invariant, as a whole, under K-endomorphisms of L. We introduce:

DEFINITION. L/K is called

— *central* or of type $\underline{1}\rfloor$ if $K \cdot Z_L(K) = L$,
— *plain* or of type $\underline{2}\rfloor$ if $K = K \cdot Z_L(K)$,
— *outer* or of type $\underline{a}\rfloor$ if $Z_L Z_L(K) = L$,
— *inner* or of type $\underline{b}\rfloor$ if $K = Z_L Z_L(K)$.

In a similar way we can speak of L/K as an inner-central extension or of type $\underline{1b}\rfloor$, and so on. Notice that for the word "inner" sometimes "bicentral" is used, and that L/K is inner iff L/K has a dual inside L, namely $Z_L(K)/Z(L)$.

It can be verified that the first decomposition mentioned above splits L/K into a central extension followed by a plain extension, and that the second decomposition splits L/K into an outer extension followed by an inner extension. In [5, Chap. 6] some more is done on these decompositions. In fact almost half of the results there were found from the other half using the duality principle. At this point we only mention the fact that, in case $[L:K]_l < \infty$, repeated decomposing leads to a unique (standard) decomposition



with K-invariant intermediate fields D, E, E', F. What interests us here is how these structures can be dualized.

PROPOSITION 2.1. *For L/K and L_1/K_1 dual in N the following hold*:

(a) $Z_N(K \cdot Z_L(K)) = Z_{L_1} Z_{L_1}(K_1)$. *If, moreover,* $[L:K]_l < \infty$, *then also*

$$Z_N(Z_L Z_L(K)) = K_1 \cdot Z_{L_1}(K_1).$$

(b) *L/K is of type $\underline{2}\rfloor$ if and only if L_1/K_1 is of type $\underline{a}\rfloor$. If L/K is of type $\underline{1}\rfloor$ then L_1/K_1 is of type $\underline{b}\rfloor$; if moreover, $[L:K]_l < \infty$, then L/K is of type $\underline{1}\rfloor$ if and only if L_1/K_1 is of type $\underline{b}\rfloor$.*

(c) *The dual of the standard decomposition of L/K is the standard decomposition of L_1/K_1, assuming that $[L:K]_l < \infty$.*

Proof. (a) From Proposition 1.4(a) it follows that

$$\begin{aligned} Z_N(K \cdot Z_L(K)) &= Z_N(K) \cap Z_N Z_L(K) \\ &= L_1 \cap Z_N Z_{L_1}(K_1) \\ &= Z_{L_1} Z_{L_1}(K_1). \end{aligned}$$

Of couse, by symmetry we have $Z_N(K_1 \cdot Z_{L_1}(K_1)) = Z_L Z_L(K)$. In case $[L:K]_l < \infty$, by the duality theorem it follows that $Z_N(Z_L Z_L(K)) = K_1 \cdot Z_{L_1}(K_1)$.

(b) Note that L/K is of type $\underline{2}\rfloor$ if and only if $Z_L(K) = Z(K)$ and that L_1/K_1 is of type $\underline{a}\rfloor$ if and only if $Z_{L_1}(K_1) = Z(L_1)$. Hence the first part of (b) follows from Proposition 1.4(a). The remainder of (b) follows from (a).

(c) Follows from (b). See Fig. 1. ▮

B. *K-Homomorphisms and K-Derivations*

From Proposition 1.5 we see that every left K-linear map $L \to N$ can be described by a linear combination of left multiplications by elements of L_1. In case of more specific kinds of K-linear maps some more can be said. We treat K-homomorphisms and K-derivations in the following generalized form of the Skolem–Noether theorem.

THEOREM 2.2 (Skolem–Noether). *Let L_1/K_1 be a right predual of L/K in N, and E an intermediate field of L/K. Then the following hold:*

(a) *If $\phi: E \to N$ is a K-homomorphism, then there exists an element $\theta \in L_1^*$ such that $x\phi = \theta^{-1} x \theta$ for all $x \in E$.*

(b) *If $D: E \to N$ is a K-derivation, then there exists an element $\theta \in L_1$ such that $xD = x\theta - \theta x$ for all $x \in E$.*

Proof. Notice that E/K also has a right predual in N, hence $\mathfrak{L}^l_K(E, N)$ is spanned over N by the l_t, $t \in L_1$.

(a) Write ϕ as a linear combination of independent l_{t_i} with $t_i \in L_1^*$; given $y \in L$, for any $x \in L$ compare $(xy)\phi$ with $x\phi \cdot y\phi$, as follows:

$$(xy)\phi = \sum l_{e_i}(x) \cdot y\lambda_i$$

$$x\phi \cdot y\phi = \sum l_{e_i}(x)\, \lambda_i \cdot y\phi.$$

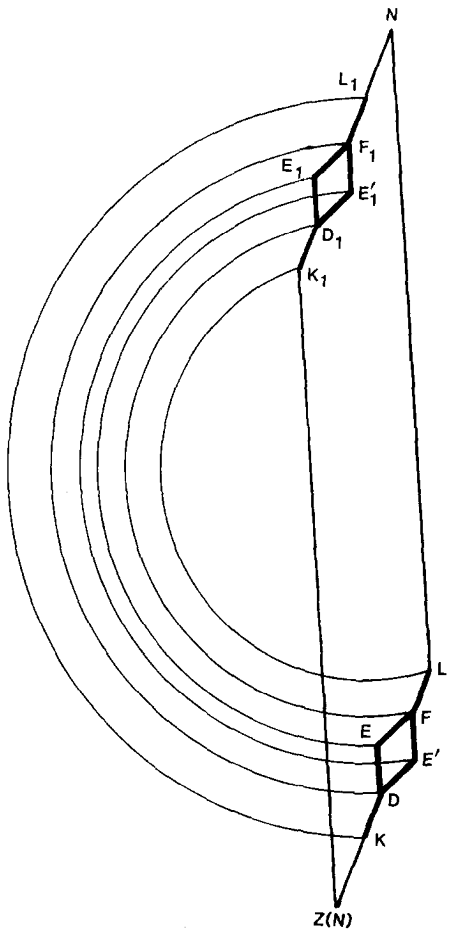


FIGURE 1

It follows that

$$\lambda_i \cdot y\phi = y\lambda_i.$$

By taking $\theta = \lambda_i$ we finish the proof.

(b) As in (a), but this time take $t_i = 1$ for some i and compare $(xy)D$ with $xD \cdot y + x \cdot yD$, as follows:

$$(xy)D = \sum l_{e_i}(x) \cdot y\lambda_i$$

$$xD \cdot y + x \cdot yD = \sum l_{e_i}(x) \cdot \lambda_i y + l_1(x) \cdot yD.$$

By independency of the l_{e_i}, $i \in I$, it follows that

$$l_1 \cdot (y\lambda_{i_0} - \lambda_{i_0} y) = l_i \cdot yD,$$

where i_0 is chosen such that $e_{i_0} = 1$. Taking $\theta = \lambda_{i_0}$ finishes the proof. ∎

See also [4, pp. 162, 174]. This theorem tells us that K-homomorphisms and K-derivations can be dualized to elements of L_1. In what follows we take a closer look to find what can be said of these elements under more specific conditions, such as $\phi: L \to L$, $D: L \to L$, or $\phi \in G_{L/K}$, the group of K-automorphisms of L.

LEMMA 2.3. *Let L_1/K_1 and L/K be dual in N and $\theta \in N^*$. If $\omega: L \to N$ is given by $x \to \theta^{-1}x\theta$ then the following hold:*

(a) *θ is a left-normalizing element of L_1/K_1 if and only if $\omega: L \to L$ is a K-homomorphism of L into L.*

(b) *If $[L:K]_r < \infty$ or $[L:K]_l < \infty$, then every left-normalizing element of L_1/K_1 is also a right-normalizing element.*

Proof. (a) From $\theta Z_N(L)\theta^{-1} = Z_N(\theta L\theta^{-1})$ it follows that $\theta Z_N(L)\theta^{-1} \subset Z_N(L)$ if and only if $\theta L\theta^{-1} \supset L$ if and only if $L \supset L\omega$.

(b) In this case ω is an injective K-linear map of a finite-dimensional K-space L. Hence ω is surjective, which means $\theta^{-1}L\theta = L$. From (a) it follows that θ is also a right-normalizing element. ∎

Notice that every L_1/K_1 can occur as some $Z_N(K)/Z_N(L)$. From Lemma 2.3(b) it follows that in general in the finite-dimensional case we can omit the prefix "left." In that case $\theta \in N_{L_1^*}(K_1^*)$. Next we give the dual characterization of the group $G_{L/K}$ of K-automorphisms of L.

PROPOSITION 2.4. *Let L_1/K_1 and L/K be dual in N with $[L:K]_r < \infty$. For any $\theta \in L_1^*$ define the K-homomorphism $\pi(\theta): L \to N$ by $x\pi(\theta) = \theta^{-1}x\theta$. Then:*

(a) *$\pi(\theta_1) = \pi(\theta_2)$ if and only if $K_1^*\theta_1 = K_1^*\theta_2$.*

(b) *Every K-homomorphism $L \to N$ occurs as a π-image and π induces an isomorphism*

$$N_{L_1^*}(K_1^*)/K_1^* \cong G_{L/K}.$$

Proof. (a) This follows from

$$\pi(\theta_1) = \pi(\theta_2) \quad \begin{array}{ll} \text{iff} \ \ \theta_1^{-1}x\theta_1 = \theta_2^{-1}x\theta_2 & \text{for all} \ \ x \in L \\ \text{iff} \ \ \theta_1\theta_2^{-1} \in K_1. & \end{array}$$

(b) In this case from Theorem 2.2 it follows that π is surjective. ∎

Lemma 2.3 and Proposition 2.4 open the possibility to interpret Galois extensions as duals of normalizing extensions. This will be worked out in Section 3.

We give the results as in 2.3 and 2.4 for derivations. We call $\theta \in L$ a *Δ-normalizing element* of L/K if there exists a $D: K \to K$ such that

$$\theta a = a\theta + Da$$

for all $a \in K$. It is well known that such a D is a derivation of K. If L/K has a left basis consisting of products of Δ-normalizing elements then the matrices induced by right multiplications r_a, $a \in K$, are triangular with ones on the diagonal. If K^- and L^- are the Lie-algebras induced by K and L, then the set of Δ-normalizing elements of L/K forms a Lie-subalgebra of L^- normalizing K^-. We denote it by $N_{L^-}(K^-)$. Now we have the following analogue of 2.3 and 2.4:

PROPOSITION 2.5. *Let L_1/K_1 and L/K be dual in N with $[L:K]_r < \infty$. For any $\theta \in L$ we define the K-derivation $\tau(\theta): L \to N$ by $x\tau(\theta) = x\theta - \theta x$. Then the following hold*:

(a) *θ is a Δ-normalizing element of L_1/K_1 if and only if $\tau(\theta)$ is a K-derivation of L into L.*

(b) *$\tau(\theta_1) = \tau(\theta_2)$ if and only if $\theta_1 + K_1 = \theta_2 + K_1$.*

(c) *Every K-derivation $L \to N$ occurs as a τ-image and τ induces an isomorphism of Lie-algebras*

$$N_{L_1^-}(K_1^-)/K_1^- \cong \mathrm{Der}(L/K).$$

Proof. (a) Suppose $a \in K_1$. Then for any $x \in L$

$$\begin{aligned} x \cdot (\theta a - a\theta) &= x\theta a - ax\theta \\ &= (\theta x + x\tau(\theta)) \cdot a - a \cdot (\theta x + x\tau(\theta)) \\ &= (\theta a - a\theta) \cdot x + x\tau(\theta) \cdot a - a \cdot x\tau(\theta). \end{aligned}$$

Hence x commutes with $\theta a - a\theta$ if and only if $x\tau(\theta)$ commutes with a. This proves (a).

(b) Suppose $\tau(\theta_1) = \tau(\theta_2)$. Then for all $x \in L$

$$x\theta_1 - \theta_1 x = x\theta_2 - \theta_2 x.$$

This can be rewritten to

$$x(\theta_1 - \theta_2) = (\theta_1 - \theta_2)x.$$

Hence $\theta_1 - \theta_2 \in Z_N(L) = K_1$. The converse is clear.

(c) From Theorem 2.2(b) it follows that every K-derivation $D: L \to N$ occurs as a τ-image. Especially this holds for the K-derivations $L \to L$. Now the isomorphism follows from (b). ∎

With this result we finish the section on K-homomorphisms and K-derivations. Now we have dualized a number of basic structures (see Table 2.6). This list can be extended to more specific structures, such as

TABLE 2.6

List of Dual Structures

	L/K	L_1/K_1	
Centers and centralizer	$Z(K)$ $Z(L)$ $Z_L(K)$	$Z(L_1)$ $Z(K_1)$ $Z_{L_1}(K_1)$	Centers and centralizer
Intermediate fields	$K \subset D \subset L$ $K \cdot Z_L(K)$ $Z_L Z_L(K)$	$K_1 \subset D_1 \subset L_1$ $Z_{L_1} Z_{L_1}(K_1)$ $K_1 \cdot Z_{L_1}(K_1)$	Intermediate fields
	Standard decomposition	Standard decomposition	
	$\begin{array}{ccc} & E & \\ \rotatebox{45}{$\subset$} & & \rotatebox{135}{$\subset$} \\ K \subset D & & F \subset L \\ \rotatebox{135}{$\subset$} & & \rotatebox{45}{$\subset$} \\ & E' & \end{array}$	$\begin{array}{ccc} & E_1 & \\ \rotatebox{45}{$\subset$} & & \rotatebox{135}{$\subset$} \\ K_1 \subset D_1 & & F_1 \subset L_1 \\ \rotatebox{135}{$\subset$} & & \rotatebox{45}{$\subset$} \\ & E'_1 & \end{array}$	
	type $\underline{1}\rfloor$ type $\underline{2}\rfloor$ type $\underline{a}\rfloor$ type $\underline{b}\rfloor$	type $\underline{b}\rfloor$ type $\underline{a}\rfloor$ type $\underline{2}\rfloor$ type $\underline{1}\rfloor$	
K-Mappings	Homomorphisms $\phi: L \to N$ $\phi: L \to L$ $G_{L/K}$ Derivations $D: L \to N$ $D: L \to L$ $\mathrm{Der}(L/K)$	 $\theta \in L_1^*$ θ normalizing element of L_1/K_1 $N_{L_1^*}(K_1^*)/K_1^*$ $\theta \in L_1$ θ Δ-normalizing element of L_1/K_1 $N_{L_1^-}(K_1^-)/K_1^-$	Elements
Elements	(the converse of the above)		K_1-Mappings

binomial extensions which appear as duals of cyclic Galois extensions (see Section 3). Also the dual relations from this list can be used to find dual statements of known statements. This provides a (meta-mathematical) *duality principle*:

> Every statement formulated in terms of basic structures considered here can be dualized to a dual statement, which is true if and only if the original statement is true. Sometimes also proofs can be dualized and can provide new proofs.

3. Galois Extensions and Normalizing Extensions

In this section we study Galois extensions and normalizing extensions, which appear to be duals of each other. First a lemma on normalizing extensions.

LEMMA 3.1. *Assume $[L:K]_l < \infty$. If L is generated over K (as a field) by the normalizing elements θ_i, $i \in I$, then L/K is a normalizing extension, with a normalizing basis consisting of products of the θ_i.*

Proof. One can easily verify that the left K-linear space R spanned by all products of the θ_i is a subring of L. Since $[L:K]_l < \infty$ this subring must be a field; therefore $R = L$. ∎

The next theorem makes use of π as defined in 2.4. Remember that in case of preduality π was surjective, so given ω we can always find a θ_ω with $\pi(\theta_\omega) = \omega$.

THEOREM 3.2. *Let L_1/K_1 and L/K be dual in N with $[L:K]_r < \infty$. The following are equivalent:*

(i) *L/K is a Galois extension,*

(ii) *L_1/K_1 is a normalizing extension.*

Further, assume that (i) *and* (ii) *are satisfied.*

(a) *If $G \subset G_{L/K}$ is a submonoid with $K = \operatorname{Inv} G$ and θ_ω, $\omega \in G$, are elements of L_1^* such that $\pi\theta_\omega = \omega$, then θ_i, $i \in I$, is a normalizing basis for L_1/K_1 for some subset $I \subset G$.*

(b) *If θ_i, $i \in I$, is a normalizing basis for L_1/K_1, and $G = \{\pi(\theta_i) \mid i \in I\}$, then* $\operatorname{Inv} G = K$.

Proof. We start with the following observation: if θ_i, $i \in I$, are normalizing elements of L_1/K_1 and $G = \{\pi(\theta_i) \mid i \in I\}$, then

$$\begin{aligned}\operatorname{Inv} G &= L \cap Z_N(\{\theta_i \mid i \in I\}) \\ &= Z_N(K_1) \cap Z_N(\{\theta_i \mid i \in I\}) \\ &= Z_N(K_1(\theta_i; i \in I)).\end{aligned}$$

(a) and (i) $\Rightarrow$ (ii) By 2.3 the θ_ω, $\omega \in G$, are normalizing elements of L_1/K_1. From the observation, by duality it follows that L_1 is generated over K_1 by θ_ω, $\omega \in G$. By Lemma 3.1 we see that L_1/K_1 has a normalizing basis consisting of products of the θ_ω, $\omega \in G$. We are done if we prove that for any $\omega_1, \omega_2 \in G$ there exists a $\lambda \in K_1$ with

$$\theta_{\omega_1} \cdot \theta_{\omega_2} = \lambda \theta_{\omega_1 \omega_2}.$$

In fact this follows from 2.4(a) and

$$\begin{aligned}\pi(\theta_{\omega_1} \cdot \theta_{\omega_2}) &= \pi(\theta_{\omega_1}) \cdot \pi(\theta_{\omega_2}) \\ &= \omega_1 \cdot \omega_2 \\ &= \pi(\theta_{\omega_1 \omega_2}).\end{aligned}$$

(b) and (ii) $\Rightarrow$ (i) Follows from the observation. ∎

One can use this dual relation between Galois extensions and normalizing extensions to derive the main theorems of finite Galois theory from duality. There is an analogue of Dedekind's lemma for the dependence of normalizing elements. This line is worked out in [5, Chap. 7]. At this point we continue asserting dual relations between different notions. The first specific Galois extension we consider is the *G-regular* Galois extension, that is, a Galois extension L/K such that $\operatorname{Inv} G = K$ and $\operatorname{card}(G) = [L : K]$ (both finite).

THEOREM 3.3. *Let L_1/K_1 and L/K be dual in N with $[L : K]_r < \infty$. The following are equivalent*:

(i) *L/K is a regular Galois extension.*

(ii) *L_1/K_1 is a crossed product.*

Further, assume that (i) *and* (ii) *are satisfied.*

(a) *Suppose G is a subgroup of $G_{L/K}$ such that L/K is G-regular. If elements θ_ω, $\omega \in G$, of L_1^* are given such that $x\omega = \theta_\omega^{-1} x \theta_\omega$ for $x \in L$, and $\theta_{id} = 1$, then θ_ω, $\omega \in G$ is a G-basis of L_1/K_1.*

(b) *Suppose θ_i, $i \in G$, is a G-basis of L_1/K_1 for some group G. If for*

$i \in G$ we define $\omega_i \in G_{L/K}$ by $x\omega_i = \theta_i^{-1} x \theta_i$ then $i \to \omega_i$ is an embedding of G into $G_{L/K}$; identification of G with its image in $G_{L/K}$ makes L/K a G-regular extension.

Proof. (a) and (i) $\Rightarrow$ (ii) Suppose L/K is G-regular. From Theorem 3.2 it follows that θ_ω, $\omega \in G$, is a normalizing basis of L_1/K_1. Since $\pi(\theta_i\theta_j) = \pi(\theta_{ij})$, L_1/K_1 is a G-crossed product with G-basis θ_i, $i \in G$.

(b) and (ii) $\Rightarrow$ (i) Suppose L_1/K_1 is a G-crossed product with G-basis θ_i, $i \in G$. It is clear that $i \to \omega_i$ is a homomorphism. If $\omega_i = id$, then $\theta_i \in Z_N(L) = K_1$, so $i = e$, the unit element of G. We see that $i \to \omega_i$ is an embedding. Theorem 3.2 implies that $\operatorname{Inv} G = K$. Furthermore, by the duality theorem $\operatorname{card}(G) = [L_1 : K_1] = [L : K]$. ∎

Theorem 3.3 generalizes Theorem 3.3.8 on page 55 of [3]. The following corollary establishes that binomial extensions and cyclic Galois extensions are duals of each other.

COROLLARY 3.4. *Let L_1/K_1 and L/K be dual in N with $[L : K]_r < \infty$. The following are equivalent:*

(i) *L/K is a cyclic Galois extension.*

(ii) *L_1/K_1 is a binomial extension.*

Further, assume that (i) *and* (ii) *are satisfied.*

(a) *Suppose $\omega \in G_{L/K}$ of order n is given such that* $\operatorname{Inv} \omega = K$. *If $\theta \in N^*$ is such that $x\omega = \theta^{-1} x \theta$ for all $x \in L$, then θ is a generator of the binomial extension L_1/K_1.*

(b) *Suppose θ is a generator of the binomial extension L_1/K_1, and $\omega \in G_{L/K}$ is given by $x\omega = \theta^{-1} x \theta$ for $x \in L$. Then ω has order n and* $\operatorname{Inv} \omega = K$.

PROPOSITION 3.5. *Let L_1/K_1 and L/K be dual in N with $[L : K]_r < \infty$.*

(a) *Assume L_1/K_1 is a pseudolinear extension with generator θ and zero derivation. Define $\omega \in G_{L/K}$ by $x\omega = \theta^{-1} x \theta$ and take $G = \{\omega^i \mid i \in \mathbb{Z}\}$, the cyclic group generated by ω. Then* $\operatorname{Inv} G = K$.

(b) *Assume G is a cyclic subgroup of $G_{L/K}$, say generated by ω, and assume* $\operatorname{Inv} G = K$. *Let an element θ of L_1^* be given such that $x\omega = \theta^{-1} x \theta$ for all $x \in L$, then L_1/K_1 is a pseudolinear extension with generator θ and zero derivation.*

(c) *In particular* (a) *and* (b) *imply that the following are equivalent:*

(i) *L_1/K_1 is a pseudolinear extension with zero derivation.*

(ii) *There exists a cyclic subgroup G (possibly infinite) of $G_{L/K}$ with* $\operatorname{Inv} G = K$, *Proof.* (a) Apply Theorem 3.2(b) with $\theta_{\omega^i} = \theta^i$ for $i = 0, ..., n-1$.

(b) From 3.2(a) it follows that $1, \theta, \theta^2, ...$ span L_1 over K_1. Let $m \geqq 0$ be maximal such that $1, \theta, ..., \theta^{m-1}$ are left independent over K_1. Then all higher powers of θ are linear combinations of these $1, \theta, ..., \theta^{m-1}$. Therefore $m = n$. ▌

This proposition again gives a link between two notions known in the literature, namely, pseudolinear extensions and invariant fields of one automorphism or of a cyclic group of automorphisms, which are dealt with in Bortfeld [2].

Many of the results of this section have counterparts for the case of derivations instead of automorphisms. One can define notions of Δ-normalizing extension and Δ-Galois extension such that these are duals of each other. We will not go into the details of this at this point, although in Section 4 some special cases are treated in relation with binomial extensions.

4. Applications of Duality

We continue with binomial extensions and cyclic Galois extensions. If θ is a binomial generator of L/K of degree n then we have the *norm*

$$RN_k(\lambda; S) = \lambda \cdot S(\lambda) \cdot \cdots \cdot S^{k-1}(\lambda)$$

for $\lambda \in N \supset L$; here S is given by $S(x) = \theta x \theta^{-1}$. Further take $\mu = \theta^n$.

Lemma 4.1. *Let L/K be binomial with generator θ of degree n, and $K \subset L \subset N$. If $\lambda \in N^*$ and $\theta_1 = \lambda\theta$, then the following hold:*

(a) $\theta_1^n = \mu_1$ *with* $\mu_1 = RN_n(\lambda; \mathrm{S})\mu$, *and,* $\theta_1 a = S_1(a)\theta_1$ *with* $S_1(a) = \lambda S(a)\lambda^{-1}$ *for* $a \in K$.

(b) *The following are equivalent:*

(i) $\theta \to \theta_1$ *induces a K-isomorphism between L and* $K(\theta_1)$.

(ii) $RN_n(\lambda; S) = 1$ *and* $\lambda \in Z_N(K)$.

Proof. (a) This is easy to verify.

(b) (i) ⇒ (ii) If (i) holds, then $\mu_1 = \mu$ and $S_1 = S$, hence (ii) follows from (a).

(ii) ⇒ (i) We must prove that $X^n - \mu$ is the minimal polynomial of θ_1. The K-homomorphisms

$$\pi_0, \pi\colon K[X; S] \to N$$

with $\pi_0(X) = \theta$ and $\pi(X) = \theta_1$ satisfy

$$K[X; S](X^n - \mu) = \ker \pi_0 \subset \ker \pi.$$

Since $L \cong_K K[X; S]/\ker \pi_0$ is a field, $\ker \pi_0$ is a two-sided ideal, maximal as a left ideal. Therefore $\ker \pi_0 = \ker \pi$. This gives the K-isomorphism between L and $K(\theta_1)$. ∎

Using duality it is very easy to give the following characterization of cyclic Galois extensions:

THEOREM 4.2. *Assume $Z(K) \cap Z(L)$ contains a primitive* nth *root of unity, where $[L:K]_l = n$. Then the following are equivalent:*

(i) *L/K is a binomial extension.*

(ii) *L/K is a cyclic Galois extension.*

Proof. (i) ⇒ (ii) If ζ is a primitive root of unity in $Z(K) \cap Z(L)$, then $S(\zeta) = \zeta$ and $RN_n(\zeta; S) = \zeta^n = 1$. Lemma 4.1(b) gives that $\theta \to \zeta\theta$ induces a K-automorphism ω of L, which is of order n. It is easily verified that for $x = \sum_{i=0}^{n-1} a_i \theta^i \in L$ one has $\omega(x) = x$ if and only if $x \in K$. Hence $\mathrm{Inv}\, \omega = K$.

(ii) ⇒ (i) Follows from (i) ⇒ (ii) in a dual L_1/K_1 of L/K, using 3.4. ∎

This theorem generalizes the results of Amitsur [1] (see also [3, p. 67]) by dropping the condition "outer" and simplifies the proof a lot.

The following result is a generalization of the corollary on p. 68 of [3].

THEOREM 4.3 (Hilbert 90). *Let L/K be a cyclic Galois extension and let $\alpha \in L$ satisfy $RN_n(\alpha; \omega) = 1$, where ω is a K-automorphism of order n with $K = \mathrm{Inv}\, \omega$. Then there is a $\beta \in L^*$ with $\alpha = \beta^{-1} \cdot \omega(\beta)$.*

Proof. Take a dual L_1/K_1 of L/K in some N. By 3.4 we have a binomial generator of L_1/K_1 such that $\omega(x) = \theta x \theta^{-1}$ for all $x \in L$. Now apply Lemma 4.1(b) on α and L_1/K_1. From Proposition 2.4 it follows that the K_1-homomorphism $\phi: L_1 \to N$ given by $\theta \to \alpha\theta$ can be described by a $\beta \in L^*$: $\phi(x) = \beta^{-1} x \beta$ for all $x \in L_1$. Taking $x = \theta$ finishes the proof. ∎

The above results and their proofs illustrate how duality can be used to find new results and to prove them in a completely different way, compared with the usual proofs. In a similar way one can find new proofs for the classical results of Wedderburn on finite skew fields and of Frobenius on finite-dimensional extensions of the real numbers.

Most of the results of this section have counterparts for the case of derivations instead of automorphisms. We sketch some of these:

PROPOSITION 4.4. *Assume* char$(K)=p$. *Let* L_1/K_1 *be a dual of* L/K. *The following are equivalent*:

(i) *There exists a* K*-derivation* $D_0\colon L\to L$ *with* $D_0^p=D_0$ *and* $D_0x=0$ *if and only if* $x\in K$.

(ii) L_1/K_1 *has a left basis* $1, \theta, ..., \theta^{p-1}$ *with* $\theta^p-\theta=\mu\in K_1$, *where* θ *is a* Δ*-normalizing element of* L_1/K_1.

If (i) *and* (ii) *are satisfied then one can relate* D_0 *and* θ *by*

$$D_0x=\theta x-x\theta \qquad \textit{for} \quad x\in L.$$

Proof. (i)$\Rightarrow$(ii) By 2.5 we can find a θ inducing D_0 as an inner derivation.

From (i) it follows that $K=Z_N(K_1(\theta))$. By the duality theorem we have $K_1(\theta)=L_1$. Since θ is a Δ-normalizing element of L_1/K_1 this implies $1, \theta, ..., \theta^{p-1}$ is a left basis of L_1/K_1.

From $D_0^p=D_0$ it follows that $\theta^p-\theta=\mu\in K_1$ for some μ.

(ii)$\Rightarrow$(i) Take for D_0 the inner derivation induced by θ; then (i) easily follows. ▮

This proposition again gives a link between two known types of extensions. We use it to generalize another result of Amitsur [1] (see also Proposition 3.5.8 on page 72 of [3]).

PROPOSITION 4.5. *Assume* $[L:K]_l=$ char$(K)=p$.

(a) *The following are equivalent*:

(i) L/K *is a cyclic Galois extension.*

(ii) L/K *has a left basis* $1, \theta, ..., \theta^{p-1}$ *with* Δ*-normalizing element* θ *of* L/K *and* $\theta^p-\theta=\mu\in K$.

If (i) *and* (ii) *are satisfied then one can relate them by* $\omega(\theta)=\theta+1$, *where* ω *is a generator for the cyclic Galois group.*

(b) *The following are equivalent*:

(i) L/K *is a binomial extension.*

(ii) *There exists a* K*-derivation* $D_0\colon L\to L$ *with* $D_0^p=D_0$ *and* $D_0x=0$ *if and only if* $x\in K$.

If (i) *and* (ii) *are satisfied then one can relate them by* $D_0\eta=\eta$, *where* η *is a binomial generator for* L/K.

The statements in (a) *and* (b) *are duals of each other.*

Proof. Notice that by 3.4 and 4.4 the statements in (a) and (b) are dual. Let L_1/K_1 be a dual of L/K. We will make the cycle

$$\begin{array}{cccccc} L_1/K_1 & (a)(i) & \Rightarrow & (b)(i) & L/K \\ & \Uparrow & & \Downarrow & \\ L_1/K_1 & (a)(ii) & \Leftarrow & (b)(ii) & L/K. \end{array}$$

Suppose L_1/K_1 is cyclic Galois. Then L/K is binomial, say with generator η. One easily verifies that $D_0\eta = \eta$ defines a $D_0: L \to L$ satisfying (b)(ii). By 4.4 we find a $\theta \in L_1$ satisfying (a)(ii) for L_1/K_1. Again one easily verifies that $\theta \to \theta + 1$ induces a K-automorphism ω of L_1/K_1 with $\omega^p = id$ and $\text{Inv}\,\omega = K_1$. This closes the cycle and proves 4.5. ▮

APPENDIX: Inner Closures

A useful tool is the following notion of inner closure; it is similar to the notion of a normal closure for an extension of commutative fields. Notice that we call $\theta, \theta' \in N$ of the same *K-type* if $K \subset N$ and $\theta \to \theta'$ gives a K-isomorphism $K(\theta) \cong_K K(\theta')$; we call L' a *K-copy* of L if $L \cong_K L'$.

Definition. An extension N of K is called an *inner* (*normal*) *closure* of L/K if $K \subset L \subset N$ and

(i) For every $\theta \in N \backslash K$ there exists a $\theta' \in N$ of the same K-type such that $\theta' \neq \theta$ and the K-isomorphism $\theta \to \theta'$ is induced by an inner K-automorphism of N.

(ii) N is generated by K-copies of L of the form $t^{-1}Lt$ for $t \in Z_N(K)^*$.

In this appendix we prove that every L/K can be embedded in an inner closure. Notice that (i) holds if and only if N/K is an inner Galois extension if and only if N/K is bicentral.

Proposition A.1. *Assume $K \subsetneq L \subset N$.*

(a) *If K is bicentral in N then the subfield $L \cdot Z_N(K)$ of N is an inner closure for L/K.*

(b) *If N is an inner closure for L/K, then K is bicentral in N and $N = L \cdot Z_N(K)$ and $Z(N) = Z(K) \cap Z(L)$.*

Proof. (a) Take $N_0 = L \cdot Z_N(K)$, then $Z_{N_0}(K) = Z_N(K)$. Therefore N_0/K is bicentral:

$$Z_{N_0}Z_{N_0}(K) = N_0 \cap Z_N Z_{N_0}(K) = N_0 \cap Z_N Z_N(K) = K.$$

Take N_1 the subfield of N_0 generated by all $t^{-1}Lt$ for $t \in Z_{N_0}(K)^*$. Then $t^{-1}N_1 t \subset N_1$ for all $t \in Z_{N_0}(K)^*$. From the Cartan–Brauer–Hua theorem it follows that $Z_{N_0}(K) \subset N_1$ or $Z_{N_0}(K) \subset Z_{N_0}(N_1)$ (see [4, p. 186]). In the first case we have $N_0 = N_1$ and we are done. In the second case

$$Z_{N_0}(K) \supset Z_{N_0}(L) \supset Z_{N_0}(N_1) \supset Z_{N_0}(K).$$

Then we have the contradiction

$$L \subset Z_{N_0} Z_{N_0}(L) = Z_{N_0} Z_{N_0}(K) = K.$$

(b) In case N itself is an inner closure for L/K, both N and $L \cdot Z_N(K)$ are generated by the fields $t^{-1}Lt$ for $t \in Z_N(K)^*$. So $N = L \cdot Z_N(K)$. Finally,

$$\begin{aligned} Z(N) = Z_N(N) &= Z_N(L \cdot Z_N(K)) \\ &= Z_N(L) \cap Z_N Z_N(K) \\ &= Z_N(L) \cap K \\ &= Z(K) \cap Z(L). \quad \blacksquare \end{aligned}$$

Next we make constructions for inner closures. The following key-lemma is helpful for that (see Cohn [3, p. 120]). It provides in an extension (infinitely) many K-copies of elements of L which are tied by inner K-automorphisms.

KEY-LEMMA A.2. (a) *Given L/K there exists an extension E of L and an element $t \in Z_E(K)^*$ such that $t^{-1}xt \neq x$ for every $x \in L \backslash K$.*

(b) *One can take the E of* (a) *of the form $E = L \circ_K K(t)$; this field contains as a subfield the field coproduct of countably many K-copies of L in the form of ${}_{i \in Z} \circ_K t^{-i} L t^i$.*

This lemma introduces new elements for which again K-copies should be constructed, of course by the same construction. So applying repeatedly this lemma gives us an inner closure:

PROPOSITION A.3. *For every L/K there exists an inner closure N.*

(a) *One can choose N as*

$$N = L \circ_K D \qquad \textit{with} \quad D = {}_{i=1}^{\infty} \circ_K K(t_i)$$

and t_i, $i \geqq 1$, are commuting with the elements of K.

(b) *It is also possible to choose N as the field*

$$N = L(t_1, t_2, \ldots)$$

generated by L and t_i, $i \geqq 1$, *satisfying*

$$\begin{aligned} &t_1 \in Z_N(K) & & \\ &t_i \in Z_N(L) & &\text{for} \quad i \geqq 2 \\ &t_i t_j = t_j t_i & &\text{for} \quad j \geqq i+2. \end{aligned}$$

In that case also L is bicentral in N.

Proof. We may assume $K \subsetneqq L$.

(a) We construct a chain

$$E_0 = K \subset L = E_1 \subset E_2 \subset E_3 \subset \cdots \bigcup_{i=1}^{\infty} E_i = N,$$

where for $i \geqq 1$

$$E_{i+1} = E_i \circ_K K(t_i).$$

Then we have (by the key-lemma)

$$t_i \in Z_N(K), \qquad t_i^{-1} x t_i \neq x \qquad \text{for all} \quad x \in E_i \backslash K.$$

Therefore K is bicentral in N. Furthermore $N = L(t_1, t_2, ...) = L \cdot Z_N(K)$. From Proposition A.1 it follows that N is an inner closure of L/K.

(b) We modify the construction of (a) by taking

$$E_{i+1} = E_i \circ_{E_{i-1}} E_{i-1}(t_i).$$

Then $t_i \in Z_N(E_{i-1})$, $t_i^{-1} x t_i \neq x$ for all $x \in E_i \backslash E_{i-1}$. In particular $t_i \in Z_N(K)$, and for $i \geqq 2$, $t_i \in Z_N(L)$. Therefore both K and L are bicentral in N. As in (a), N is an inner closure of L/K. ▌

In [5, Chapters 2 and 3], different constructions are made using model theoretic concepts like λ-closed fields and generic fields. These notions are similar to the notion of algebraic closure for the case of commutative fields.

References

1. S. A. Amitsur, Non commutative cyclic fields, *Duke Math. J.* **21** (1954), 87–105.
2. R. Bortfeld, Ein Satz zur Galoistheorie in Schiefkörpern, *J. Reine Angew. Math.* **201** (1959), 196–206.
3. P. M. Cohn, "Skewfield Constructions," Cambridge Univ. Press, London/New York, 1977.
4. N. Jacobson, "Structure of Rings," rev. ed., Amer. Math. Soc., Providence, RI, 1968.
5. J. Treur, "A Duality for Skew Field extensions," Thesis, Utrecht, 1976.