On Twisted Cyclic Algebras and the Chain Equivalence of Kummer Elements

Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften (Dr. rer. nat.)
der Fakultät für Mathematik
der Universität Regensburg

vorgelegt von
Wieland Fischer
aus Amberg

Fakultät für Mathematik der Universität Regensburg
Regensburg im Juni 1999

Table of Contents

Introduction 3

Notations 7

Chapter I . Twisted Cyclic Extensions 8

§ 1. Twisted Cyclic Extensions 8

1. Preliminaries 8
2. Twisted Cyclic Structures 12
3. Uniqueness of Twisted Cyclic Structures 16

§ 2. C_0-Extensions 19

1. C_0-Extensions 19
2. Classification of C_0-Extensions 19
3. μ_n-Extensions and Kummer Extensions 25

Chapter II . Twisted Cyclic Algebras 30

§ 3. Twisted Cyclic Algebras 30

1. Twisted Cyclic Algebras 30
2. Pairs of Twisted Cyclic Extensions associated to Twisted Cyclic Algebras 32
3. Twisted Cyclic Algebras associated to Pairs of Twisted Cyclic Extensions 38
4. A Cohomological Classification of Twisted Cyclic Algebras 41

§ 4. Existence of Twisted Cyclic Decompositions of Central Simple Algebras . . 49

1. A Cohomological Lemma 49
2. Galois Actions on $\bar{A}_0$ 53
3. The Existence of a Twisted Cyclic Decomposition 57

§ 5. A Cohomological Description of Twisted Cyclic Algebras 59

1. The Theorem 59
2. Cocycles Associated to a Twisted Cyclic Algebra 60
3. The 1-Cocycles Associated to the Pairs (L, ρ_L) and (K, ρ_K) 62
4. Proof of the Theorem 65

Chapter III . The Notion of Chain Equivalence 67

§ 6. Kummer Elements and Kummer Relation 67

1. Kummer Elements 67
2. Description of Twisted Cyclic Algebras via Elements in Kummer Relation 70
3. Galois Action on Kummer Elements and Twisted Cyclic Decompositions 72
4. Description of Split Twisted Cyclic Algebras 73

§ 7. Chains of Twisted Cyclic Extensions 75

1. Definition of Chains 75
2. Chains with Fixed Starting and End Points 75

Table of Contents

§ 8. Chains of Kummer Elements 80
1. Definition of Chains of Kummer Elements 80
2. The Notion of Chain Equivalence of Kummer Elements 82
3. Connection between K-Chains and c-Chains 83

Chapter IV . Geometry of Kummer Elements and Chains 85

§ 9. The Variety of Kummer Elements 85
1. A as a k-Scheme 85
2. $\mathcal{W}(A)$ and $\mathrm{W}(A)$ as Varieties over an Algebraically Closed Field 88
3. $\mathcal{W}(A)$ and $\mathrm{W}(A)$ as k-Schemes 91

§ 10. The Variety of Chains 92
1. The "Vectorbundle of Kummer Pairs" 92
2. Construction of the Varieties of Chains 98
3. Chains with Starting Point 102

§ 11. The Topological Closure of $\mathrm{W}^1(A)$ 103
1. Some Linear Algebra 103
2. The Closure of $\mathrm{W}^1(A)$ 108

Chapter V . Chain Equivalence for Algebras of Degree 2 and 3 110

§ 12. The Case of Algebras of Degree 2 111
1. Chain Equivalence for $n = \ell = 2$ 111
2. The Geometric Point of View 113

§ 13. The Case of Algebras of Degree 3 and Length 3 117
1. Preliminaries and Conditions for Chains of Length 2 117
2. Existence of Connecting Chains of Length 3 120

§ 14. The Case of Algebras of Degree 3 and Length 4 124

Chapter VI . Relation to the Product Map of Tori 128

§ 15. A Covering of $\mathrm{W}(A)$ 128
1. The Variety $\mathrm{GL}_1(A)/D$ 128
2. The Covering 130

§ 16. A Covering of Chain Varieties 133
1. The Kummer Relation 133
2. The Covering 136

§ 17. Reformulation in the Product Map of Tori 140

References 143

Introduction

A well known theorem about quaternion algebras is the common slot lemma by A. Albert: For a, b, c, $d \in k^*$, non-zero elements in a field such that $(a,b) \cong (c,d)$ there exists an element $e \in k^*$ such that

$$(a,b) \;\cong\; (a,e) \;\cong\; (c,e)\ .$$

For non-zero elements a, b in a field k of characteristic not 2, the symbol (a,b) denotes the central simple k-algebra of degree 2 defined by the presentation

$$\langle X, Y : X^2 = a,\, Y^2 = b,\, XY = -YX\rangle\ .$$

There are several other theorems of this form. One example is the chain-p-equivalence of Pfister forms, cf. chapter 4, §1 in Scharlau [SchQF].
Another example is Witt's chain equivalence theorem of diagonal quadratic forms, cf. chapter 1, (5.2) in Lam [LaQF].

Concerning the first example, one may ask similar questions for central simple algebras of degree > 2. E.g., for some integer $n \geq 2$ let k be a field of characteristic prime to n, containing a primitive n-th root of unity ζ. Then for a, b, c, $d \in k^*$ such that $(a,b)_\zeta \cong (c,d)_\zeta$, does there exist elements $e_1, \ldots, e_{\ell-1} \in k^*$ such that there is a chain of isomorphisms of length ℓ of the form

$$(a,b)_\zeta \;\cong\; (e_1,b)_\zeta \;\cong\; (e_1,e_2)_\zeta \;\cong\; \cdots \;\cong\; (e_{\ell-2},e_{\ell-1})_\zeta \;\cong\; (c,e_{\ell-1})_\zeta$$

if ℓ is odd, or

$$(a,b)_\zeta \;\cong\; (a,e_1)_\zeta \;\cong\; (e_2,e_1)_\zeta \;\cong\; \cdots \;\cong\; (e_{\ell-2},e_{\ell-1})_\zeta \;\cong\; (c,e_{\ell-1})_\zeta$$

if ℓ is even?
Here $(a,b)_\zeta$ denotes the central simple k-algebra of degree n defined by the presentation

$$\langle X, Y : X^n = a,\, Y^n = b,\, XY = \zeta YX\rangle\ .$$

If this statement is true, i.e., answered with "yes", we call it a common slot lemma for central simple k-algebras of degree n and chains of length ℓ.

J.-P. Tignol answered the question for central simple algebras of degree $n = 3$ and chains of length $\ell = 2$, by giving a counter-example: There are fields k and elements a, b, c, $d \in k^*$ with $(a,b)_\zeta \cong (c,d)_\zeta$, such that for no $e \in k^*$ the following holds:

$$(a,b)_\zeta \;\cong\; (a,e)_\zeta \;\cong\; (c,e)_\zeta\ .$$

Cf. the appendix in [RoCL].

A common slot lemma for exceptional Jordan algebras over quadratically closed fields was proven by H. P. Petersson & M. L. Racine in [PeSR]. Their methods were used by M. Rost in [RoCL] in order to show a common slot lemma for central simple algebras of degree 3 and chains of length 4.
For completeness we reproduce his proof (with minor adaptations) in §14 of this paper.

M. Rost announced a chain lemma for Kummer elements, which we are going to state below.—A Kummer element in a central simple k-algebra A of degree n is an

invertible element X in A such that its reduced characteristic polynomial has the form $\mathrm{Prd}(X,t) = t^n - a$. Furthermore, a ζ-pair in A is a pair (X,Y) of Kummer elements in A such that $XY = \zeta YX$, where ζ denotes a primitive n-th root of unity.
We will see in §6 that a ζ-pair (X,Y) generates the algebra A; so with $a := X^n$ and $b := Y^n \in k^*$ we have $A \cong (a,b)_\zeta$.

Now ROST's chain lemma says: Let $n = p$ be a prime number and k a p'-closed field, i.e., k has no finite algebraic extension of degree prime to p. Let A be a division algebra over k of degree p and $\zeta \in k^*$ a primitive p-th root of unity. Then for any two Kummer elements Z_0 and Z_p in A, there exist Kummer elements $Z_1, \ldots, Z_{p-1}$ in A such that (Z_{i-1}, Z_i) are ζ-pairs for $i = 1, \ldots, p$.
For the last fact we are going to say that $Z_0, \ldots, Z_p$ is a (ζ-)chain of Kummer elements in A of length p.

As a corollary we easily get a common slot lemma for central simple k-algebras of degree p and chains of length p, with the field k from above: Let a, b, c, $d \in k^*$ with $A := (a,b)_\zeta \cong (c,d)_\zeta$, then there are Kummer elements Z_0 and Z_p in A with $Z_0^p = b$ if ($p \equiv 1 \bmod 4$) or $Z_0^p = b^{-1}$ if ($p \equiv 3 \bmod 4$) and $Z^p = c$. We assume that p is odd. Then there are (in the generic case) Kummer elements $Z_1, \ldots, Z_{p-1}$ such that Z_0, …, Z_p is a ζ-chain of Kummer elements in A, and we get

$$A = \langle Z_0, Z_1 \rangle \;=\; \langle Z_1, Z_2 \rangle \;=\; \cdots \;=\; \langle Z_{p-1}, Z_p \rangle \;.$$

In the language of symbols this is

$$(a,b)_\zeta \;\cong\; (e_1,b)_\zeta \;\cong\; (e_1,e_2)_\zeta \;\cong\; \cdots \;\cong\; (e_{p-2},e_{p-1})_\zeta \;\cong\; (c,e_{p-1})_\zeta$$

for suitable $e_i := Z_i^{\pm n} \in k^*$.

The following paper consists of two parts:
In the first part we set the notion of ζ-pairs in a more conceptual frame: If (X,Y) is a ζ-pair in a central simple k-algebra A of degree n, then we get other ζ-pairs by taking powers of the two elements X and Y with exponents prime to n, i.e., (X^ν, Y^μ) is a $\zeta^{\nu\mu}$-pair. The same we can do more generally for a whole chain of Kummer elements. But the pairs we got by this process do not give anything new. In particular the entries a and b in the associated symbol $(a,b)_\zeta$ just change to the ν-th and μ-th power. We also observe that X and Y generate maximal commutative subalgebras $L = k[X]$ and $K = k[Y]$ of A, cf. §6, and that these algebras remain unchanged, even if we first applied any operation of taking powers, mentioned above. We call the pairs (L,K) arising in this way a decomposition of A.
In chapter II we analyze these kinds of objects—the triples (A,L,K). We even consider objects, which are models (over a subfield of k) of this triple.

It is easy to see (cf. §3) that the powers of Y act on L and mutatis mutandis X on K by conjugation in A. This situation is the subject of chapter I.

In chapter III we give the connection between the decompositions of A and ζ-pairs in A: We specify several notions of chains and show how they are related. This chapter is the link to the second part of the paper.

Here we give a geometric view of the main objects—Kummer elements and chains of Kummer elements: We will find smooth irreducible k-schemes $\mathrm{W}^0(A)$ and $\mathrm{W}^\ell(A)$ which

classify by their points the Kummer elements and chains of Kummer elements of length ℓ, up to scaling of the Kummer elements (i.e., we work in projective spaces). By this interpretation, the problem of the chain lemma becomes a question in Algebraic Geometry, where we have much additional structure. For example we may stress dimension theory. The problem, if any two (generic) Kummer elements can be connected by a chain of Kummer elements of length ℓ now has the following form: Let

$$\pi\colon \mathrm{W}^{\ell}(A) \longrightarrow \mathrm{W}^{0}(A) \times_k \mathrm{W}^{0}(A)$$

be the morphism of schemes which on the points is just the projection $(Z_0, \ldots, Z_\ell) \mapsto (Z_0, Z_\ell)$ of a chain of Kummer elements of the length ℓ onto the first and last factor. Question: Is the morphism dominant, and—if $\dim \mathrm{W}^{\ell}(A) = \dim \mathrm{W}^{0}(A) \times_k \mathrm{W}^{0}(A)$—what is the degree of π?

We will find that $\dim \mathrm{W}^{\ell}(A) = (\ell+n)(n-1)$ and $\dim \mathrm{W}^{0}(A) = n(n-1)$. So one easily can see that for a chain lemma of a central simple algebra A of degree n we need at least $\ell \geq n$.
In the case from above, for central simple algebras of degree 3 we recognize that there is no chance connecting 2 arbitrary Kummer elements by a chain of length 2—for dimensional reasons! In his counter-example, Tignol even showed more: He proved that one can find two Kummer elements X and Y such that X can not be connected to any conjugate of Y, by a chain of length 2.
In the end of chapter IV, we show an interesting property about the topology of the scheme $\mathrm{W}^{1}(A)$ of ζ-pairs, i.e., we will describe the closure of the space.

In chapter V, we explicitly work out three cases:
The first case is concerned with the common slot lemma for central simple algebras of degree 2 and chains of length 2; the "classical" common slot lemma, given at the beginning.—But of course we do it in our terminology of Kummer elements. We will see the geometric structure of the chain lemma:
The morphism $\pi\colon \mathrm{W}^{2}(A) \longrightarrow \mathrm{W}^{0}(A) \times_k \mathrm{W}^{0}(A)$ will be revealed as part of the blowing-up morphism along the diagonal.
The second case is the chain lemma for central simple algebras of degree 3 and chains of length 3. We will see that for a quadratically closed field k, almost any two Kummer elements X and Y can be connected by exactly two chains of Kummer elements of length 2.
The third case is the case of central simple algebras of degree 3 and chains of length 4, already mentioned above.

The last chapter gives a new interpretation of the morphism π: We will construct a more explicit map ω between spaces which are coverings of degree n^ℓ and n of $\mathrm{W}^{\ell}(A)$ and $\mathrm{W}^{0}(A) \times_k \mathrm{W}^{0}(A)$ respectively, and via these coverings ω lies over π. So, one may ask the question of dominance and even (for $n = \ell$) of the degree anew for the map ω.
Finally we will see that our new map ω has a nice interpretation for $\ell = n$:
Let S and T be the maximal tori in $\mathrm{PGL}(A)$ given by the subalgebras generated by Kummer elements X and Y; where (X, Y) is a ζ-pair. Then for $\ell = n$ odd, the map ω can be interpreted as the multiplication map

$$S \times T \times S \times T \times \cdots \times S \times T = (S \times T)^{\frac{n+1}{2}} \longrightarrow \mathrm{PGL}(A)\ .$$

Acknowledgments: I deeply wish to express my thanks to PD Dr. M. Rost. He took care of me after the tragic death of my former teacher Jürgen Neukirch. I am greatly indebted to him for presenting to me this new interesting subject.

Notations

Throughout the paper k denotes a field and—unless specified in a different way—we denote by $\bar{k}$ a separable algebraic closure of k. Then $\Gamma = \mathrm{Gal}(\bar{k}|k)$ denotes the absolute Galois group of k.

Furthermore we use the following "standard" notations:

E_{ij}	quadratic matrix (of specified size) with entry 1 at the place (i,j) and 0 otherwise
$\mathrm{diag}(d_1,\ldots,d_n)$	diagonal $n \times n$-matrix with diagonal entries $d_1,\ldots, d_n$, in this order, i.e., $d_1E_{11} + \cdots + d_nE_{nn}$
$\mathrm{EigVal}(f)$	set of eigenvalues of some endomorphism f of a vector space
$\mathrm{EigVec}(f,\theta)$	set of (non-zero) eigenvectors of f to the eigenvalue θ
$\mathrm{EigVec}(f)$	$\coprod_{\theta\in\mathrm{EigVal}(f)} \mathrm{EigVec}(f,\theta)$
$\coprod$	sum in the category of sets, i.e., disjoint union
κ_x	conjugation with the element x in some domain, whenever this action is defined, i.e., $\kappa_x(y) = xyx^{-1}$
ev_x	evaluation in x, i.e., $\mathrm{ev}_x(f) = f(x)$, whenever f is a map which can be evaluated in x
$\mathrm{Prd}(X,t)$	reduced characteristic polynomial (in the variable t) of some element X in a central simple algebra
$\mathrm{Nrd}(X)$	reduced norm of some element X in a central simple algebra
$\mathrm{Trd}(X)$	reduced trace of some element X in a central simple algebra

If X is any scheme and $\mathscr{E}$ an $\mathcal{O}_X$-module on X, then we denote with $\mathscr{E}(x)$, for a point $x \in X$, the $\kappa(x)$-vector space $\mathscr{E}_x \otimes_{\mathcal{O}_{X,x}} \kappa(x)$, where in this context $\kappa(x)$ is the residue field $\mathcal{O}_{X,x}/\mathfrak{m}_x$ of x and $\mathscr{E}_x$ the stalk of $\mathscr{E}$ at x.

For such an $\mathscr{E}$ on a k-scheme X and a k-vector space E, we use the following notations:

$\mathbf{A}(E)$	$\mathrm{Spec}\big(S(\check{E})\big)$, the k-Scheme, which has E as its k-rational points
$\mathbf{P}(E)$	$\mathrm{Proj}\big(S(\check{E})\big)$, the k-Scheme, which has $E - \{0\}/k^*$ as its k-rational points
$\mathbb{V}(\mathscr{E})$	$\mathrm{Spec}\big(S(\mathscr{E})\big)$
$\mathbb{P}(\mathscr{E})$	$\mathrm{Proj}\big(S(\mathscr{E})\big)$

Here $\check{E}$ stands for the k-vector space dual $\mathrm{Hom}_{k\text{-lin}}(E,k)$ of E, and S is the (naturally graded) symmetric k-algebra on some k-vector space or sheaf of modules on some k-scheme X. In a similar way, one has to read the k-Schemes $\mathrm{GL}_1(A)$ and $\mathrm{PGL}_1(A)$ for k-algebras A.

Note that in this notation, if one interprets E as a sheaf of $\mathcal{O}_X$-modules, for $X = \mathrm{Spec}(k)$, this implies: $\mathbf{A}(\check{E}) = \mathbb{V}(E)$ and $\mathbf{P}(\check{E}) = \mathbb{P}(E)$.

In most cases we use the notation $[x]$ for some equivalence class of x, however, sometimes we write $\bar{a}$ for $(a \bmod n\mathbb{Z})$.

Chapter I

Twisted Cyclic Extensions

A cyclic Galois extension $L|k$ is known to be a Galois extension $L|k$ of finite degree n with a Galois group $\mathrm{Gal}(L|k) \cong \mathbb{Z}/n\mathbb{Z}$.
We can characterize a cyclic Galois extension in the following way: Let $L|k$ be a separable field extension of degree n and $\bar{k} = \bar{L}$ be a separable algebraic closure of L and k. Further we denote by $\tilde{L}$ the Galois closure of L in $\bar{k}$. If θ is a primitive element of L, i.e., $L = k(\theta)$, then θ has n conjugates $\theta_1, \ldots, \theta_n$ in $\bar{k}$ and hence $\tilde{L} = k(\theta_1, \ldots, \theta_n)$.
Now obviously we can say: $L|k$ is a cyclic Galois extension $\Leftrightarrow \mathrm{Gal}(\tilde{L}|k) \cong \mathbb{Z}/n\mathbb{Z}$.
From Galois theory one knows the morphism

$$\begin{aligned} \varphi\colon \mathrm{Gal}(\bar{k}|k) &\longrightarrow S(\{\theta_1, \ldots, \theta_n\}) \\ \gamma &\longmapsto \gamma|_{\{\theta_1,\ldots,\theta_n\}} \end{aligned}$$

from the absolute Galois group of k into the permutation group of the conjugates of θ. The kernel of this morphism in $\mathrm{Gal}(\bar{k}|\tilde{L})$ and therefore the image is isomorphic to $\mathrm{Gal}(\tilde{L}|k)$. So we can say: $L|k$ is a cyclic Galois extension $\Leftrightarrow \mathrm{im}(\varphi) \cong \mathbb{Z}/n\mathbb{Z}$.
In this case $\mathrm{im}(\varphi)$ is a group which acts free on the set $\{\theta_1, \ldots, \theta_n\}$. The group $\mathrm{Gal}(\bar{k}|k)$ acts on $S(\theta_1, \ldots, \theta_n)$ by conjugation via φ. However this action is trivial on $\mathrm{im}(\varphi)$.
In the following chapter we will treat objects which are slightly more general than the cyclic Galois extensions, namely pairs (L, C) where $C \subseteq S(\{\theta_1, \ldots, \theta_n\})$ is not any more the image of φ but some other cyclic subgroup of order n which is preserved by the action of the absolute Galois group of k.

§ 1. Twisted Cyclic Extensions

1. Preliminaries

Let M be a finite set of n elements, $S(M)$ denotes the symmetric group on M and let $C \subseteq S(M)$ be a *transitive* cyclic subgroup of order n, i.e., a cyclic subgroup of order n such that $M = \{\pi(m) : \pi \in C\}$ for any $m \in M$. About the normalizer subgroup $N_C := \{\pi \in S(M) : \pi C \pi^{-1} = C\}$ one knows:

(1.1) Claim. *There is a natural short exact sequence*

$$\begin{aligned} 1 \to C \overset{\text{incl}}{\hookrightarrow} N_C &\xrightarrow{\kappa} \mathrm{Aut}(C) \to 1 \\ \pi &\longmapsto \kappa_\pi \end{aligned}$$

where $\kappa_\pi(\varphi) = \pi\varphi\pi^{-1}$ is the inner automorphism on $S(M)$ restricted to C, given by conjugation with π.

Proof: We may assume $M = \{1, 2, \ldots, n\}$ and—since C is a transitive subgroup of order n—that C is generated by $\sigma := (1\ 2\ \ldots\ n)$, the permutation which maps i to $i+1$ modulo n.
Let $\pi \in \ker(\kappa)$ be an element of the kernel of κ. Then $\pi\varphi = \varphi\pi$ for all elements $\varphi \in C$. Let $i = \pi(n)$, then we have

$$\pi(j) \;=\; \sigma^j \pi \sigma^{-j}(j) \;=\; \sigma^j \pi(n) \;=\; \sigma^j(i) \;=\; \sigma^{i+j}(n) \;=\; \sigma^i(j)$$

for all j, hence $\pi = \sigma^i \in C$.
It remains to show the surjectivity of κ: An automorphism $f \in \mathrm{Aut}(C) = (\mathbb{Z}/n\mathbb{Z})^*$ is given by some $(m \bmod n\mathbb{Z}) \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $f\colon C \to C$, $\pi \mapsto \pi^m$. Define $\varphi \in S_n = S(\mathbb{Z}/n\mathbb{Z})$ to be $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$, $\ell \bmod n \mapsto m \cdot \ell \bmod n$, then considering

$$\sigma^m = (1m\ 2m\ \ldots\ nm) = \varphi\ (1\ 2\ \ldots\ n)\ \varphi^{-1} = \kappa_\varphi(\sigma)$$

one can see both—$\varphi \in N_C$ and $\kappa_\varphi = f$. □

The surjective homomorphism κ has sections. There is no canonical section, but we will see that there is indeed a class of sections which are given naturally.

(1.2) Lemma. *For each $m \in M$ the restriction of $\kappa\colon N_C \longrightarrow \mathrm{Aut}(C)$ to*

$$I_m := \{\pi \in N_C : \pi(m) \;=\; m\} \;\xrightarrow{\sim}\; \mathrm{Aut}(C)$$

is an isomorphism. It gives rise to a section $s_m\colon \mathrm{Aut}(C) \longrightarrow N_C$ of $\kappa\colon N_C \longrightarrow \mathrm{Aut}(C)$, namely its inverse. It can be described by

$$\begin{aligned} s_m(f)\colon M &\longrightarrow M \\ \pi(m) &\longmapsto ({}^f\pi)(m)\ , \end{aligned}$$

for all $f \in \mathrm{Aut}(C)$ and $\pi \in C$.

Proof: First of all, the restriction $\kappa\colon I_m \to \mathrm{Aut}(C)$ is injective: If $\pi, \pi' \in I_m$ are two elements such that $\kappa_\pi = \kappa_{\pi'}$, we can conclude $\pi'\pi^{-1} \in \ker(\kappa) = C$ and hence $\pi' = \pi$. In fact, since $\pi'\pi^{-1}(m) = m$ we know $\pi'\pi^{-1} = 1$.
Now, in order to show that the morphism is surjective, choose an $f \in \mathrm{Aut}(C)$. Then the permutation defined by $\tilde{s}\colon M \to M$, $\pi(m) \mapsto ({}^f\pi)(m)$ for $\pi \in C$, is a pre-image of f lying in I_m: We first claim for any $\pi \in C$:

$$\tilde{s}\ \pi\ \tilde{s}^{-1} \;=\; {}^f\pi\ .$$

Evaluation with $\psi(m) \in M$ for $\psi \in C$ gives

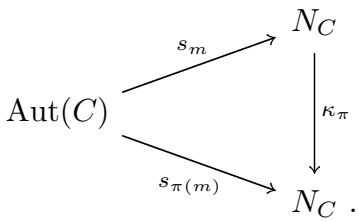
$$\begin{aligned} (\tilde{s}\ \pi\ \tilde{s}^{-1})\big(\psi(m)\big) \;&=\; (\tilde{s}\ \pi)({}^{f^{-1}}\psi)(m) \\ &=\; \tilde{s}(\pi\ {}^{f^{-1}}\psi)(m) \\ &=\; {}^f(\pi\ {}^{f^{-1}}\psi)(m) \\ &=\; ({}^f\pi\ \psi)(m) \\ &=\; ({}^f\pi)\big(\psi(m)\big)\ . \end{aligned}$$

This proves that $\tilde{s} \in N_C$—thus we get $\tilde{s} \in I_m$, since $\tilde{s}(m) = m$—and that $\kappa_{\tilde{s}} = f$. □

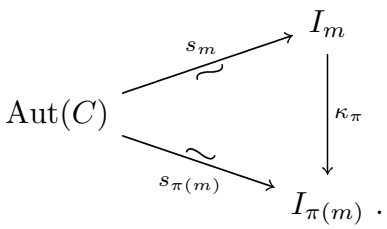
(1.3) Lemma. *For any $m \in M$ and $\pi \in C$ we have the formula $s_{\pi(m)}(f) = \pi s_m(f)\pi^{-1}$ for every $f \in \mathrm{Aut}(C)$, i.e.,*

$$s_{\pi(m)} \;=\; \kappa_\pi \circ s_m \;,$$

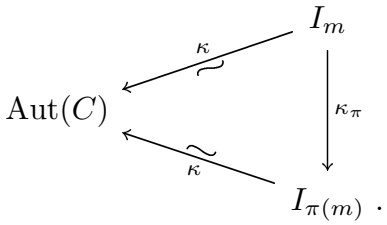
where κ_π is the conjugation $\kappa_\pi\colon N_C \longrightarrow N_C$, $\varphi \longmapsto \pi\varphi\pi^{-1}$. In other words, we have the commutative diagram



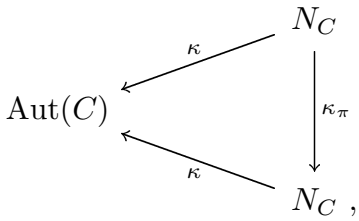
Proof: Since $\kappa_\pi(I_m) = I_{\pi(m)}$ we can change the two right hand side objects in the diagram to I_m and $I_{\pi(m)}$ such that we have to show the commutativity of



Now the two diagonal arrows are bijections, and in order to show the commutativity of the diagram it is equivalent to prove the commutativity of the diagram with the reversed arrows:



Thus we have to prove $\kappa \circ \kappa_\pi = \kappa$ on I_m. But this is clear. We even have the commutativity on N_C



since π is an element of the kernel of $\kappa\colon N_C \longrightarrow \mathrm{Aut}(C)$: For any $\tau \in N_C$

$$\begin{aligned} \kappa \circ \kappa_\pi(\tau) \;&=\; \kappa(\pi\tau\pi^{-1}) \\ &=\; \kappa(\pi)\kappa(\tau)\kappa(\pi^{-1}) \\ &=\; \kappa(\tau) \end{aligned}$$

and this completes the proof. □

(1.4) Claim. *For each $m \in M$ there is an isomorphism of groups*

$$\begin{aligned} \sigma_m\colon C \rtimes \mathrm{Aut}(C) &\xrightarrow{\sim} N_C \\ (\varphi, f) &\longmapsto \varphi\, s_m(f)\ . \end{aligned}$$

We have the commutative diagram for any $\pi \in C$

$$\begin{array}{ccc} C \rtimes \mathrm{Aut}(C) & \xrightarrow{\sigma_m} & N_C \\ {\scriptstyle \kappa_{(\pi,\mathrm{id}_C)}}\downarrow & \searrow^{\sigma_{\pi(m)}} & \downarrow{\scriptstyle \kappa_\pi} \\ C \rtimes \mathrm{Aut}(C) & \xrightarrow{\sigma_m} & N_C\ . \end{array}$$

Proof: With the last lemmas there is nothing to prove anymore. The commutativity of the right triangle follows from $\varphi\, s_{\pi(m)}(f) = \varphi\pi s_m(f)\pi^{-1} = \pi\varphi\, s_m(f)\pi^{-1}$ for $\varphi \in C$ and $f \in \mathrm{Aut}(C)$. To recall the multiplication in the semidirect product we show the homomorphism property:

$$\begin{aligned} \sigma_m\big((\varphi, f)(\varphi', f')\big)\big(\psi(m)\big) &= \sigma_m\big((\varphi\ {}^f\varphi', ff')\big)\big(\psi(m)\big) \\ &= \varphi \circ {}^f\varphi' \circ s_m(ff')\big(\psi(m)\big) \\ &= \varphi \circ {}^f\varphi' \circ ({}^{ff'}\psi)(m) \\ &= \varphi \circ s_m(f)\big((\varphi'\ {}^{f'}\psi)(m)\big) \\ &= \sigma_m(\varphi, f)\big(\sigma_m(\varphi', f')\big(\psi(m)\big)\big) \\ &= \sigma_m(\varphi, f) \circ \sigma(\varphi', f')\big(\psi(m)\big) \end{aligned}$$

for (φ, f), $(\varphi', f') \in C \rtimes \mathrm{Aut}(C)$ and $\psi \in C$. □

(1.5) Remark. Up to an inner automorphism with an element of C (which is a subgroup of either $C \rtimes \mathrm{Aut}(C)$ and N_C) there is a canonical isomorphism of the groups $C \rtimes \mathrm{Aut}(C) \cong N_C$.

(1.6) Lemma. *If n is of the form $n = 2^\delta n'$, where n' is an odd and squarefree number and $\delta = 0$, 1, 2, then in $(\mathbb{Z}/n\mathbb{Z}) \rtimes \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/n\mathbb{Z})^*$ one has*

$$\mathrm{ord}(\bar m, \bar a) = n \quad \Longrightarrow \quad \bar a = 1$$

for all $(\bar m, \bar a) \in (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/n\mathbb{Z})^*$.

Proof: Let $(\bar m, \bar a) \in (\mathbb{Z}/n\mathbb{Z}) \rtimes (\mathbb{Z}/n\mathbb{Z})^*$ and let $\bar m = (m \bmod n\mathbb{Z})$, $\bar a = (a \bmod n\mathbb{Z})$. Assume first that $n = p$ is a prime.
If $a \equiv 1 \pmod p$, then

$$(\bar m, \bar a)^p \ = \ (\bar m, 1)^p \ = \ (0, 1)\ .$$

If $a \not\equiv 1 \pmod p$, then

$$1 + a + a^2 + \cdots + a^{p-2} \ = \ \frac{a^{p-1} - 1}{a - 1} \ \equiv \ 0 \pmod p$$

and therefore

$$(\bar{m},\bar{a})^{p-1} \;=\; (m+am+\cdots+a^{p-2}m \bmod p\mathbb{Z}, a^{p-1} \bmod p\mathbb{Z}) \;=\; (0,1)\ .$$

Let first n be (not necessarily odd) squarefree and $n = p_1\cdots p_r$ be the prime factorization of n. We define for $i = 1,\ldots,r$

$$\mu_i \;:=\; \begin{cases} p_i, & \text{if } a \equiv 1 \pmod{p_i} \\ p_i - 1, & \text{if } a \not\equiv 1 \pmod{p_i} \end{cases}$$

and $\mu := \mu_1\cdots\mu_r$. Then

$$(\bar{m},\bar{a})^{\mu} \;=\; (0,1)$$

since

$$(\mathbb{Z}/n\mathbb{Z})\rtimes(\mathbb{Z}/n\mathbb{Z})^* \;= \prod_{i=1}^{r}(\mathbb{Z}/p_i\mathbb{Z})\rtimes(\mathbb{Z}/p_i\mathbb{Z})^*\ .$$

Now if $\bar{a} \neq 1$ we have an i such that $a \not\equiv 1 \pmod{p_i}$, hence $\mu_i = p_i - 1$ and therefore $\mu < n$. It follows that $\mathrm{ord}(\bar{m},\bar{a}) < n$.
In the case of $n = 4n' = p_1^2 p_2\cdots p_r$, where n' is odd squarefree and $p_1 = 2$ we modify

$$\mu_i \;:=\; \begin{cases} p_i, & \text{if } a \equiv 1 \pmod{p_i} \text{ and } 2 \le i \\ p_i - 1, & \text{if } a \not\equiv 1 \pmod{p_i} \text{ and } 2 \le i \\ 4, & \text{if } a \equiv 1 \pmod{p_i} \text{ and } 1 = i \\ 2, & \text{if } a \not\equiv 1 \pmod{p_i} \text{ and } 1 = i \end{cases}$$

with $\mu := \mu_1\cdots\mu_r$. Then one observes for $i = 1$ that in $(\mathbb{Z}/4\mathbb{Z})\rtimes(\mathbb{Z}/4\mathbb{Z})^*$

$$(\bar{m},\bar{a})^{\mu_1} = (0,1)$$

and therefore we have analogously in $(\mathbb{Z}/n\mathbb{Z})\rtimes(\mathbb{Z}/n\mathbb{Z})^*$

$$(\bar{m},\bar{a})^{\mu} = (0,1)$$

also with $\mu < n$ which implies $\mathrm{ord}(\bar{m},\bar{a}) < n$. □

(1.7) Corollary. *Let $\pi \in S(M)$ be an element of order n and C some transitive cyclic subgroup of $S(M)$. Assume $n = m$ or $n = 2m$ for some squarefree m. Then the condition $\pi C\pi^{-1} \subseteq C$ implies $\langle\pi\rangle = C$.*

Proof: The condition says that $\pi \in N_C \cong C\rtimes \mathrm{Aut}(C)$. It suffices to show the following statement: If $\pi \in \mathbb{Z}/n\mathbb{Z}\rtimes \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}\rtimes(\mathbb{Z}/n\mathbb{Z})^*$ is of order n, then $\pi \in \mathbb{Z}/n\mathbb{Z}$, i.e., $\pi = (m,1)$ for some $m \in \mathbb{Z}/n\mathbb{Z}$. But this is exactly (1.6). □

2. Twisted Cyclic Structures

We fix a separable algebraic closure $\bar{k}$ of a field k. Let $\Gamma := \mathrm{Gal}(\bar{k}|k)$ denote the absolute Galois group of k. In the following let L be a separable k-algebra of degree n, i.e., L is a commutative k-algebra with

$$\bar{L} \;:=\; L\otimes_k \bar{k} \;\cong\; \bar{k}^n$$

as $\bar{k}$-algebra (cf. (18.3) in [BI]). Γ acts (continuously) on $\bar{L}$ by semilinear automorphisms via $\Gamma\times\bar{L}\to\bar{L}$, $(\gamma,\ell\otimes x)\mapsto \ell\otimes\gamma(x)$. Obviously $\bar{L}^{\Gamma} = L$.

If M_L is the set of the n primitive idempotents of $\bar{L}$, then there is a canonical identification

$$\begin{aligned} \mathrm{Aut}_{\bar{k}}(\bar{L}) &= S(M_L) \\ f &\longmapsto f|_{M_L} \ , \end{aligned}$$

where $S(M_L)$ is the symmetric group on the set M_L.

(1.8) Remark. By this identification one can write the morphism considered in (1.4) as

$$\begin{aligned} \sigma_e\colon C \rtimes \mathrm{Aut}(C) &\longrightarrow \mathrm{Aut}_{\bar{k}}(\bar{L}) \\ (f,\varphi) &\longmapsto f \circ s_e(\varphi) \ , \end{aligned}$$

where $e \in M_L$ is a primitive idempotent of $\bar{L}$ and $C \subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})$ a transitive cyclic subgroup of order n, and $s_e(\varphi) \in \mathrm{Aut}_{\bar{k}}(\bar{L})$ is given by

$$\begin{aligned} s_e(\varphi)\colon \bar{L} &\longrightarrow \bar{L} \\ \sum_{c\in C} x_c \cdot c(e) &\longmapsto \sum_{c\in C} x_c \cdot ({}^{\varphi}c)(e) \ , \end{aligned}$$

where $x_c \in \bar{k}$. Recall that $\bar{L} = \bigoplus_{e\in M_L} \bar{k}\cdot e = \bigoplus_{c\in C} \bar{k}\cdot c(e)$.

There is a left action of Γ on the group $\mathrm{Aut}_{\bar{k}}(\bar{L})$ given by

$$\begin{aligned} \Gamma \times \mathrm{Aut}_{\bar{k}}(\bar{L}) &\longrightarrow \mathrm{Aut}_{\bar{k}}(\bar{L}) \\ (\gamma, f) &\longmapsto {}^{\gamma}f := (\mathrm{id}_L \otimes\gamma) \circ f \circ (\mathrm{id}_L \otimes\gamma^{-1}) \ . \end{aligned}$$

One checks that ${}^{\gamma}f$ again is $\bar{k}$-linear, even if the composition on the right hand side takes place in the larger group $\mathrm{Aut}_k(\bar{L})$.

(1.9) Remark. There is a canonical identification

$$\begin{aligned} \mathrm{Aut}_k(L) &\xrightarrow{\sim} \mathrm{Aut}_{\bar{k}}(\bar{L})^{\Gamma} \\ f &\longmapsto f \otimes \mathrm{id}_{\bar{k}} \\ g|_{L\otimes k} &\longmapsfrom g \ . \end{aligned}$$

Proof: All we have to show is $g(L\otimes k) \subseteq L \otimes k$, and this is clear since $\bar{L}^{\Gamma} = L$: Let $\gamma \in \Gamma$ and $\ell \in L$, then $g(\ell\otimes 1) = ({}^{\gamma}g)(\ell\otimes 1) = \gamma\big(g(\ell\otimes 1)\big)$. □

The action of Γ on $\mathrm{Aut}_{\bar{k}}(\bar{L})$ is already given by inner automorphisms. Define

$$\begin{aligned} \varphi_L\colon \Gamma &\longrightarrow \mathrm{Aut}_{\bar{k}}(\bar{L}) = S(M_L) \\ \gamma &\longmapsto \quad \varphi_L(\gamma) \quad = (\mathrm{id}_L \otimes\gamma)|_{M_L} \ , \end{aligned}$$

i.e., $\varphi_L(\gamma)$ has the same effect on M_L as $(\mathrm{id}_L \otimes\gamma)$ but is k-linear.

(1.10) Claim. *The action of* Γ *on* $\mathrm{Aut}_{\bar{k}}(\bar{L})$ *is given by* $\kappa \circ \varphi_L$, *i.e.*,

$$\begin{aligned} \Gamma \times \mathrm{Aut}_{\bar{k}}(\bar{L}) &\longrightarrow \mathrm{Aut}_{\bar{k}}(\bar{L}) \\ (\gamma, f) &\longmapsto \kappa_{\varphi_L(\gamma)}(f) = \varphi_L(\gamma) \circ f \circ \varphi_L(\gamma)^{-1} \ . \end{aligned}$$

Proof:

$$\begin{aligned} \big(\varphi_L(\gamma) \circ f \circ \varphi_L(\gamma)^{-1}\big)|_{M_L} &= \varphi_L(\gamma)|_{M_L} \circ f|_{M_L} \circ \varphi_L(\gamma)^{-1}|_{M_L} \\ &= (\mathrm{id}_L \otimes \gamma)|_{M_L} \circ f|_{M_L} \circ (\mathrm{id}_L \otimes \gamma^{-1})|_{M_L} \\ &= {}^{\gamma}f|_{M_L} \ . \end{aligned}$$

□

(1.11) Remark. Let $L = k(\theta)|k$ be a separable field extension of degree n. We assume $L \subseteq \bar{k}$, so $\theta \in \bar{k}$. Let $\{\theta_1, \ldots, \theta_n\}$ be the set of the n distinct conjugates of θ in $\bar{k}$. Then we have the canonical identifications

$$\begin{aligned} M_L &= \mathrm{Hom}_k(L, \bar{k}) \\ e &\longmapsto e^* \ , \end{aligned}$$

where $e^*\colon L \to \bar{k}$, $\ell \mapsto \mathrm{tr}_{\bar{L}|\bar{k}}(e\ell)$ and

$$\begin{aligned} \mathrm{Hom}_k(L, \bar{k}) &= \{\theta_1, \ldots, \theta_n\} \\ f &\longmapsto f(\theta) \ . \end{aligned}$$

With this identification of M_L with $\{\theta_1, \ldots \theta_n\}$, we can give the following interpretation of φ_L: For $\gamma \in \Gamma$ the permutation $\varphi_L(\gamma) \in S(M_L)$ is given by

$$\begin{aligned} \varphi_L(\gamma)\colon \{\theta_1, \ldots, \theta_n\} &\xrightarrow{\sim} \{\theta_1, \ldots, \theta_n\} \\ \theta_i &\longmapsto \gamma\theta_i \ . \end{aligned}$$

So the map $\varphi_L\colon \Gamma \longrightarrow S(\{\theta_1, \ldots, \theta_n\})$ is just the morphism one knows from Galois theory.

(1.12) Definition. *We call the image* $\mathrm{im}(\varphi_L)\big(\subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})\big)$ *the* **Galois group** *of the* k*-algebra* L *and the fixed field* $\bar{k}^{\ker(\varphi_L)}$ *the* **splitting field** *of* L.

(1.13) Example. If $L|k$ is a separable field extension, then the splitting field of L is the Galois closure $\widetilde{L}$ of any embedding of L in $\bar{k}$, and φ_L induces the isomorphism $\mathrm{Gal}(\widetilde{L}|k) \xrightarrow{\sim} \mathrm{im}(\varphi_L)$.

(1.14) Definition. *A* **twisted cyclic structure** *on the separable* k*-algebra* L *is a* Γ*-invariant subgroup of* $\mathrm{Aut}_{\bar{k}}(\bar{L})$ *which is a transitive cyclic subgroup of order* n.
A **twisted cyclic extension** *of* k *of degree* n *is a pair* (L, C) *of a separable* k*-algebra* L *of degree* n *and a twisted cyclic structure* C *on* L.

(1.15) Remark. A transitive cyclic subgroup $C \subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})$ of order n is a twisted cyclic structure on L if and only if $\mathrm{im}(\varphi_L) \subseteq N_C$, i.e., if $\varphi_L\colon \Gamma \to \mathrm{Aut}_{\bar{k}}(\bar{L})$ factorizes in

the form $\Gamma \xrightarrow{\tau_e} C \rtimes \mathrm{Aut}(C) \xhookrightarrow{\sigma_e} \mathrm{Aut}_{\bar{k}}(\bar{L})$ (for any $e \in M_L$). Here τ_e is uniquely defined by the choice of e; and $\tau_e = \kappa_{(f,\mathrm{id})} \circ \tau_{f(e)}$ for any $f \in C$, as one can see regarding (1.4).

(1.16) Remark. Let $\tilde{k}$ be some other separable algebraic closure of k and $\alpha\colon \bar{k} \xrightarrow{\sim} \tilde{k}$ a k-isomorphism, then we have the induced isomorphism

$$\begin{aligned} \alpha_*\colon \mathrm{Aut}_{\bar{k}}(L \otimes_k \bar{k}) &\longrightarrow \mathrm{Aut}_{\tilde{k}}(L \otimes_k \tilde{k}) \\ f &\longmapsto \alpha_*(f) = (\mathrm{id}_L \otimes \alpha) \circ f \circ (\mathrm{id}_L \otimes \alpha)^{-1} \ . \end{aligned}$$

which gives a twisted cyclic structure $\alpha_*(C)$ on L if and only if C is one. In this case, i.e., if C is a twisted cyclic structure, the subgroup $\alpha_*(C)$ is independent of the choice of the k-isomorphism α: Let $\beta = \alpha \circ \gamma$, $(\gamma \in \Gamma)$ be a second k-isomorphism. Then $\beta_*(C) = (\mathrm{id}_L \otimes \alpha)(\mathrm{id}_L \otimes \gamma) C (\mathrm{id}_L \otimes \gamma)^{-1}(\mathrm{id}_L \otimes \alpha)^{-1} = (\mathrm{id}_L \otimes \alpha)\,{}^{\gamma}C\,(\mathrm{id}_L \otimes \alpha)^{-1} = \alpha_*(C)$, since ${}^{\gamma}C = C$.

(1.17) Example. If $n = 2, 3$ there is a unique twisted cyclic structure on L because S_2 and S_3 have exactly one cyclic subgroup of order n, and this one is a normal subgroup.

(1.18) Remark. In general there is not only *one* twisted cyclic structure on the algebra L. For example if $\bar{k} = k$, then the absolute Galois group $\Gamma = 1$ is trivial, so is $\mathrm{im}(\varphi_L)$ and every transitive cyclic subgroup of $S(M_L) \cong S_n$ of order n is a twisted cyclic structure, and there are exactly $(n-1)!/\varphi(n)$ transitive cyclic subgroups of order n. (φ is the Euler phi function.)

(1.19) Definition. *A twisted cyclic structure C on L is called a* **cyclic structure** *on L, if Γ acts trivially on C. Then the pair (L, C) is called a* **cyclic extension** *of k of degree n.*

(1.20) Remark. A transitive cyclic subgroup $C \subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})$ of order n is a cyclic structure on L, if and only if $\mathrm{im}(\varphi_L) \subseteq C$, because the only elements of $\mathrm{Aut}_{\bar{k}}(\bar{L}) \cong S_n$ commuting with the elements of C are the elements of C. In other words: C is a cyclic structure, if and only if one gets the (unique) factorization of φ_L in the form

$$\begin{array}{ccc} \Gamma & \xrightarrow{\varphi_L} & \mathrm{Aut}_{\bar{k}}(\bar{L}) \\ \big\downarrow{\scriptstyle \tau_e} & & \big\uparrow{\scriptstyle \sigma_e} \\ C = C \rtimes \{1\} & \hookrightarrow & C \rtimes \mathrm{Aut}(C) \ , \end{array}$$

where again $e \in M_L$ is any primitive idempotent of $\bar{L}$.

(1.21) Remark. If C is a cyclic structure on L, then one has

$$C = C^{\Gamma} \subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})^{\Gamma} = \mathrm{Aut}_k(L) \ .$$

Therefore, if L is a field, then from $\#\,\mathrm{Aut}_k(L) \leq n$ follows $C = \mathrm{Aut}_k(L)$. Hence $L|k$ is a cyclic Galois extension with Galois group C.

(1.22) Example. If $L|k$ is a cyclic Galois extension of degree n, then $\mathrm{im}(\varphi_L) = \mathrm{Gal}(L|k)$ is a cyclic structure. It is the only *cyclic* structure on L, as we have seen

in (1.21). In the following we will see that it is in fact the only *twisted cyclic* structure on L.

(1.23) Definition. *A twisted cyclic structure C on L is called a* **dihedral structure** *on L, if Γ acts on C only as identity and taking the inverse, i.e., if one has the following factorization:*

$$\begin{array}{ccccc} \Gamma & \xrightarrow{\varphi_L} & N_C & \xrightarrow{\kappa} & \mathrm{Aut}(C) \\ & \searrow & & \nearrow & \\ & & \mathbb{Z}/2\mathbb{Z} & & \end{array}$$

where the lower right hand arrow takes $(0 \bmod 2\mathbb{Z})$ *to* id_C *and* $(1 \bmod 2\mathbb{Z})$ *to* $f \mapsto f^{-1}$.

(1.24) Remark. A transitive cyclic subgroup $C \subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})$ of order n is a dihedral structure on L, if and only if $\varphi_L\colon \Gamma \to \mathrm{Aut}_{\bar{k}}(\bar{L})$ factorizes in the form

$$\begin{array}{ccc} \Gamma & \xrightarrow{\varphi_L} & \mathrm{Aut}_{\bar{k}}(\bar{L}) \\ \downarrow & \overset{\tau_e}{\searrow} & \uparrow{\scriptstyle \sigma_e} \\ C \rtimes \{\pm 1\} & \hookrightarrow & C \rtimes \mathrm{Aut}(C)\ , \end{array}$$

where $\{\pm 1\} \subseteq (\mathbb{Z}/n\mathbb{Z})^* = \mathrm{Aut}(C)$ and $e \in M_L$.

(1.25) Example. For $n = 3, 4, 6$ every twisted cyclic structure on L is dihedral. In fact in this case is $\mathrm{Aut}(C) = (\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}$.

(1.26) Example. Let $L|k$ be a separable field extension of degree $n = 4$ of the form $L = k(\sqrt{a}, \sqrt{b})$. Then $L|k$ is Galois and $\mathrm{Gal}(L|k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. There are three twisted cyclic structures on L (which are already dihedral by (1.25))—the $3 = (n-1)!/\varphi(n)$ (transitive) cyclic subgroups of order 4. The action of Γ on M_L can be identified with the action of Γ on $M := \{\pm\sqrt{a} \pm \sqrt{b}\}$. One observes that $\mathrm{im}(\varphi_L) \subseteq S(M)$ is the Klein Four Group

$$\begin{aligned} U \ &:= \ \{\sigma \in S(M) : \sigma^2 = 1,\ \mathrm{sgn}\,\sigma = 1\} \\ &= \ \{(rs)(tu) : \{r, s, t, u\} = M\}\ . \end{aligned}$$

The claim follows since the Klein Four Group U operates on the three cyclic subgroups by conjugation: One checks this for $M = \{1, 2, 3, 4\}$, e.g., consider first

$$\big((rs)(tu)\big)(1\ 2\ 3\ 4)\big((rs)(tu)\big)^{-1} \ = \ \begin{cases} (1\ 2\ 3\ 4) \\ (4\ 3\ 2\ 1)\ , \end{cases}$$

with $\{r, s, t, u\} = \{1, 2, 3, 4\}$.
The permutation $(1\ 2\ 3\ 4)$ is a generator of one of the three transitive cyclic subgroups and conjugating it with an element of the group U yields the element itself or its inverse, i.e., U acts by conjugation on the group generated by $(1\ 2\ 3\ 4)$. We get all the other generators of the transitive cyclic subgroups by conjugating $(1\ 2\ 3\ 4)$ by any element of $S(M) = S_4$, and so the conjugation of these generators by an elements of U again yields the element itself or its inverse. Note that the Klein Four Group is a normal subgroup.

3. Uniqueness of Twisted Cyclic Structures

Let's start with a "counter-example" for $n = 6$.

(1.27) Example. Let $n = 6$. In S_6 we have the elements $\sigma_1 := (1\ 2\ 3\ 4\ 5\ 6)$, $\sigma_2 := (1\ 4\ 3\ 6\ 5\ 2)$ and $\sigma_3 = (1\ 6\ 3\ 2\ 5\ 4)$ of order 6, furthermore $\varphi := (1\ 6)(2\ 5)(3\ 4)$ of order 2 and finally $\psi := (1\ 3\ 5)(2\ 4\ 6)$ of order 3. Also we know for $i = 1, 2, 3$

$$\begin{aligned} \psi &= \sigma_i^2 \ , \\ \varphi\sigma_i\varphi^{-1} &= \sigma_i^{-1} \ , \\ \varphi\psi\varphi^{-1} &= \psi^2 \ . \end{aligned}$$

Obviously, the subgroup $U := \langle\varphi, \psi\rangle$ (of order 6) generated by φ and ψ acts on $C_i := \langle\sigma_i\rangle$ by conjugation, i. e., $U \subseteq N_{C_i}$. Notice that the three groups C_1, C_2 and C_3 are different! They are the only cyclic subgroups of order 6 with this last property:
Let $\tilde{C} = \langle\tilde{\sigma}\rangle \subseteq S_6$ be a transitive cyclic subgroup of order 6 with $U \subseteq N_{\tilde{C}} \cong \tilde{C} \rtimes \mathrm{Aut}(\tilde{C})$. After some identification $N_{\tilde{C}} = \tilde{C} \rtimes \mathrm{Aut}(\tilde{C})$ we can write $\psi = (c, f) \in \tilde{C} \rtimes \mathrm{Aut}(\tilde{C})$. Since $\psi = \psi^4$ and $\mathrm{Aut}(\tilde{C}) \cong \mathbb{Z}/2\mathbb{Z}$ we have $f = 1$, i. e., $\psi = c \in \tilde{C}$. Hence by $\mathrm{ord}(\psi) = 3$ we have $\psi = \tilde{\sigma}^2$ or $\psi = \tilde{\sigma}^{-2}$. Since $\tilde{\sigma}$ and $\tilde{\sigma}^{-1}$ are the only two generators of $\tilde{C}$, we may assume $(1\ 3\ 5)(2\ 4\ 6) = \psi = \tilde{\sigma}^2$. Therefore $\tilde{\sigma}$ has the form $\tilde{\sigma} = (1\ a\ 3\ b\ 5\ c)$ with $(a\ b\ c) = (2\ 4\ 6)$. There are three possibilities for substituting the variables a, b and c by the numbers 2, 4 and 6 (in the right order!), and they yield the elements σ_1, σ_2 and σ_3.
Now, set $k = \mathbb{Q}$ and $L := \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ where ζ_3 is a primitive third root of unity. Then $L|k$ is Galois of degree 6 and the Galois group $\mathrm{Gal}(L|k) = \mathrm{im}(\varphi_L)$ can easily be identified with U. So L has exactly three twisted cyclic structures.
Note that $L|k$ is a non-abelian Galois extension. This is interesting, since for cyclic Galois extensions of fields we have the following:

(1.28) Proposition. *A cyclic Galois extension $L|k$ of fields of degree n has a unique twisted cyclic structure—namely the cyclic structure mentioned in (1.22).*

Proof: Let $C := \mathrm{im}(\varphi_L)$ be our cyclic (hence twisted cyclic) structure from (1.22), and we assume that C' is another twisted cyclic structure on L. We choose generators: $\langle\sigma\rangle = C$ and $\langle\tau\rangle = C'$.
Then by definition, $\mathrm{im}(\varphi_L) = C \subseteq N_{C'}$, i. e., $\tau\sigma\tau^{-1} \in C$. So there is an integer i with $\tau\sigma\tau^{-1} = \sigma^i$. But $\sigma^i = \tau\sigma\tau^{-1}$ is also a generator of C, hence $(i \bmod n\mathbb{Z}) \in (\mathbb{Z}/n\mathbb{Z})^*$. Chose an integer j such that $ij \equiv 1 \pmod n$. Then $\tau^j\sigma\tau^{-j} = \sigma^{ij} = \sigma$. Since C is a transitive subgroup of $S(M_L)$ we know by (1.1) that $\tau^j \in C$, hence $\tau = \tau^{ij} \in C$. Therefore $C = C'$. □

(1.29) Proposition. *Assume $n = m$ or $n = 2m$ for some squarefree m. Let C be a twisted cyclic structure on a separable k-algebra L of degree n, and suppose that there exists an element $\pi \in \mathrm{im}(\varphi_L)$ of order n, then $C = \langle\pi\rangle$, and C is the only twisted cyclic structure on L.*

Proof: After the identification $\mathrm{Aut}_{\bar{k}}(\bar{L}) = S(M_L)$ one can use (1.7), which says that $\pi C\pi^{-1} \subseteq C$ implies $\langle\pi\rangle = C$. □

(1.30) Proposition. *Let $L|k$ be a separable field extension of degree n. If the condition $\big(n, \varphi(n)\big) = 1$ holds—in this case n is squarefree—then there exists at most one twisted cyclic structure on L. (φ denotes the Euler phi function!)*

Proof: Assume C is a twisted cyclic structure on L, by (1.29) it is enough to find an element $\pi \in \operatorname{im}(\varphi_L)$ of order n. Certainly there are elements $\pi_i \in \operatorname{im}(\varphi_L)$, $i = 1, \ldots, m$ of order p_i, where $n = p_1 \cdots p_m$. This follows from the fact that $n | \# \operatorname{im}(\varphi_L)$.
Identifying somehow $N_C = C \rtimes \operatorname{Aut}(C)$ we can write $\pi_i = (c_i, \varphi_i)$ for $c_i \in C$ and $\varphi_i \in \operatorname{Aut}(C)$. We claim $\varphi_i = \mathrm{id}_C$ for all i. Otherwise we have $1 \neq \operatorname{ord}(\varphi_i) \mid \operatorname{ord}(c_1, \varphi_i) = p_i$, i. e., $\operatorname{ord}(\varphi_i) = p_i$. But $\operatorname{ord}(\varphi_i) \mid \varphi(n)$, which is prime to n. Therefore $\pi := \pi_1 \cdots \pi_m = (c_1 \cdots c_m, \mathrm{id}_C)$ has order $p_1 \cdots p_m = n$. □

(1.31) Remark. Example (1.27) shows that (1.30) doesn't hold without the condition $\big(n, \varphi(n)\big) = 1$.

§ 2. C_0-Extensions

1. C_0-Extensions

Again, let k be a field and $\Gamma = \mathrm{Gal}(\bar{k}|k)$ the absolute Galois group of k (for some separable algebraic closure $\bar{k}$ of k).
Now fix a natural number n and a continuous discrete Γ-module C_0 which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ as a group. Let $\alpha\colon \Gamma \to \mathrm{Aut}(C_0)$ denote the morphism given by the action of Γ on C_0, i.e., $\alpha(\gamma)(c) = {}^{\gamma}c$ for $\gamma \in \Gamma, c \in C_0$.

(2.1) Definition. *Let L be a separable k-algebra of degree n. A* **C_0-structure** *on L is an injective Γ-equivariant morphism $\rho\colon C_0 \hookrightarrow \mathrm{Aut}_{\bar{k}}(\bar{L}) = S(M_L)$ of groups such that $\mathrm{im}(\rho)$ is a transitive cyclic subgroup of order n.*
A **C_0-extension** *is a pair (L, ρ) of a separable k-algebra L of degree n and a C_0-structure ρ on L.*

(2.2) Remark. If (L, ρ) is a C_0-extension, then $\mathrm{im}(\rho) \subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})$ is a twisted cyclic structure on L and $\big(L, \mathrm{im}(\rho)\big)$ is a twisted cyclic extension of k of degree n. On the other hand: If (L, C) is a twisted cyclic extension, it gives rise to the C-extension $\big(L, \rho\colon C \overset{\mathrm{incl}}{\hookrightarrow} \mathrm{Aut}_{\bar{k}}(\bar{L})\big)$.

(2.3) Example. Let us take a look at the case of a trivial Γ-module:
If C_0 is a trivial Γ-module, then $\mathrm{im}(\rho)$ is a *cyclic* structure on L for any C_0-extension (L, ρ). From (1.21) already follows $\mathrm{im}(\rho) \subseteq \mathrm{Aut}_k(L) \subseteq \mathrm{Aut}_{\bar{k}}(\bar{L})$. So the C_0-structures on L are already the injective morphisms $C_0 \hookrightarrow \mathrm{Aut}_k(L)$ of groups. Therefore after fixing some generator c_0 of C_0, there is a bijection

$$\begin{aligned} \{C_0\text{-structures on } L\} &\xrightarrow{\sim} \{c \in \mathrm{Aut}_k(L) : \mathrm{ord}(c) = n\} \\ \rho &\longmapsto \rho(c_0)\ . \end{aligned}$$

Since a cyclic group of order n has exactly $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$ generators (i.e., elements of order n), there is a $\varphi(n)$ to 1 correspondence between C_0-structures and cyclic structures on L. In the case $C_0 = \mathbb{Z}/n\mathbb{Z}$ we have the canonical generator $(1 \bmod n\mathbb{Z})$ and instead of writing (L, ρ) we may write $\big(L, \rho(1 \bmod n\mathbb{Z})\big)$.

2. Classification of C_0-Extensions

There is a classification of the C_0-extensions of k by the Galois cohomology group $H^1(k, C_0) = H^1(\Gamma, C_0)$.

(2.4) Definition. *A morphism $f\colon (L, \rho) \longrightarrow (L', \rho')$ of C_0-extensions of k is a morphism $f\colon L \to L'$ of k-algebras such that for every $c \in C_0$, the diagram*

$$\begin{array}{ccc} \bar{L} & \xrightarrow{\bar{f}} & \bar{L}' \\ {\scriptstyle \rho(c)}\downarrow & & \downarrow{\scriptstyle \rho'(c)} \\ \bar{L} & \xrightarrow{\bar{f}} & \bar{L}' \end{array}$$

is commutative. Here $\bar{f}$ is the morphism

$$f \otimes \mathrm{id}_{\bar{k}} \colon \bar{L} \;=\; L \otimes_k \bar{k} \;\longrightarrow\; L' \otimes_k \bar{k} \;=\; \bar{L}' \;.$$

(2.5) Remark. In other words: $\bar{L}$ and $\bar{L}'$ become C_0-modules via $\rho\colon C_0 \to \mathrm{Aut}_{\bar{k}}(\bar{L})$ and $\rho'\colon C_0 \to \mathrm{Aut}_{\bar{k}}(\bar{L}')$ and $\bar{f}$ is a morphism of C_0-modules.

(2.6) Remark. The morphisms f and $\bar{f}$ are then already isomorphisms. In fact $\bar{f}$ is bijective, since $\bar{f}|_{M_L}\colon M_L \to M_{L'}$ is bijective: C_0 acts free on the sets of primitive idempotents M_L and $M_{L'}$.

(2.7) Remark. Recall some well known facts about Galois cohomology; one has the following groups: Let

$$\mathscr{Z}^1(\Gamma, C_0) \;=\; \{\text{continuous crossed homomorphisms } \Gamma \to C_0\}$$

denote the group of the 1-cocycles of Γ with values in C_0. On this group we have (an equivalence relation given by) the normal subgroup

$$\mathscr{B}^1(\Gamma, C_0) \;=\; \{f\colon \Gamma \to C_0 : \text{there exists a } c \in C_0 \text{ such that } f(\gamma) = \gamma c - c \text{ for all } \gamma \in \Gamma\}$$

of the 1-coboundaries.
Then we have the cohomology group $H^1(\Gamma, C_0) = \mathscr{Z}^1(\Gamma, C_0)/\mathscr{B}^1(\Gamma, C_0)$. Let

$$\mathrm{Hom}_{\mathrm{cont},\Gamma}(\Gamma, C_0 \rtimes \Gamma) \;:=\; \{f \in \mathrm{Hom}_{\mathrm{cont}}(\Gamma, C_0 \rtimes \Gamma) : \mathrm{pr}_2 \circ f = \mathrm{id}_\Gamma\} \;,$$

where $\mathrm{pr}_2\colon C_0 \rtimes \Gamma \to \Gamma$ is the projection on the second factor. On this group we have the equivalence relation given by:

$$f \sim g \quad :\Longleftrightarrow \quad f = \kappa_{(c,1_\Gamma)} \circ g \text{ for some } c \in C_0 \;.$$

Here $\kappa_{(c,1_\Gamma)}$ is the conjugation in $C_0 \rtimes \Gamma$ with the element $(c, 1_\Gamma)$. Let

$$\mathrm{Hom}_{\mathrm{cont},\alpha}\big(\Gamma, C_0 \rtimes \mathrm{Aut}(C_0)\big) \;:=\; \big\{f \in \mathrm{Hom}_{\mathrm{cont}}\big(\Gamma, C_0 \rtimes \mathrm{Aut}(C_0)\big) : \mathrm{pr}_2 \circ f = \alpha\big\} \;,$$

where $\mathrm{pr}_2\colon C_0 \rtimes \mathrm{Aut}(C_0) \to \mathrm{Aut}(C_0)$ is the projection on the second factor. On this group we have the equivalence relation given by:

$$f \sim g \quad :\Longleftrightarrow \quad f = \kappa_{(c,\mathrm{id}_{C_0})} \circ g \text{ for some } c \in C_0 \;.$$

Here $\kappa_{(c,\mathrm{id}_{C_0})}$ is the conjugation in $C_0 \rtimes \mathrm{Aut}(C_0)$ with the element (c, id_{C_0}). Also, there are the identifications of these groups

$$\begin{aligned} \mathscr{Z}^1(\Gamma, C_0) \;&\xrightarrow{\sim}\; \mathrm{Hom}_{\mathrm{cont},\Gamma}(\Gamma, C_0 \rtimes \Gamma) \\ h \;&\longmapsto\; \widetilde{h} \;, \end{aligned}$$

where $\widetilde{h}(\gamma) = \big(h(\gamma), \gamma\big)$ and

$$\begin{aligned} \mathscr{Z}^1(\Gamma, C_0) \;&\xrightarrow{\sim}\; \mathrm{Hom}_{\mathrm{cont},\alpha}\big(\Gamma, C_0 \rtimes \mathrm{Aut}(C_0)\big) \\ h \;&\longmapsto\; \widetilde{h} \;, \end{aligned}$$

where $\widetilde{h}(\gamma) = \big(h(\gamma), \alpha(\gamma)\big)$. They respect the equivalence relations, such that canonically

$$\begin{aligned} H^1(\Gamma, C_0) \;&\cong\; \mathrm{Hom}_{\mathrm{cont},\Gamma}\big(\Gamma, C_0 \rtimes \Gamma\big)/\sim \\ &\cong\; \mathrm{Hom}_{\mathrm{cont},\alpha}\big(\Gamma, C_0 \rtimes \mathrm{Aut}(C_0)\big)/\sim \;. \end{aligned}$$

The theorem (2.10) states that there is an identification of isomorphism classes of C_0-extensions and the elements of $H^1(\Gamma, C_0)$.

First, we want to assign a cohomology class $[h_{(L,\rho)}] \in H^1(\Gamma, C_0)$ to a C_0-extension (L, ρ): Let $C := \mathrm{im}(\rho)$ be the twisted cyclic structure associated to ρ. Choose a primitive idempotent $e \in M_L$ of $\bar{L}$. Now ρ induces the isomorphism

$$\rho_*\colon C_0 \rtimes \mathrm{Aut}(C_0) \xrightarrow{\sim} C \rtimes \mathrm{Aut}(C) \ ,$$

and there is the commutative diagram

$$\begin{array}{ccccc} \Gamma & \xrightarrow{\tau_e} & C \rtimes \mathrm{Aut}(C) & \xhookrightarrow{\sigma_e} & \mathrm{Aut}_{\bar{k}}(\bar{L}) \ = \ S(M_L) \\ & \searrow^{\rho_*^{-1}\circ\tau_e} & \uparrow{\scriptstyle \rho_*} & & \\ & & C_0 \rtimes \mathrm{Aut}(C_0) & & \end{array}$$

of the factorization of φ_L.
Now define the crossed homomorphism $h_{(L,\rho)}\colon \Gamma \to C_0$ by the equation $\widetilde{h_{(L,\rho)}} = \rho_*^{-1} \circ \tau_e$, so

$$\varphi_L \ = \ \sigma_e \circ \rho_* \circ \widetilde{h_{(L,\rho)}} \ . \tag{1}$$

The cohomology class $[h_{(L,\rho)}] \in H^1(\Gamma, C_0)$ is independent of the choice of the primitive idempotent e: Let $c_0 \in C_0$, $c := \rho(c_0) \in C$, then by (1.15) $\tau_e = \kappa_{(c,\mathrm{id})} \circ \tau_{c(e)}$, therefore

$$(\rho_*^{-1} \circ \tau_e) \ = \ \rho_*^{-1} \circ \kappa_{(c_0,\mathrm{id})} \circ \tau_{c(e)} \ = \ \kappa_{(c_0,\mathrm{id})} \circ (\rho_*^{-1} \circ \tau_{c(e)}) \ .$$

Furthermore it is obvious that $[h_{(L,\rho)}] = [h_{(L',\rho')}]$, if $(L, \rho) \cong (L', \rho')$.

(2.8) Lemma. *For the 1-cocycle $h_{(L,\rho)}$ which is given by $\widetilde{h_{(L,\rho)}} := \rho_*^{-1} \circ \tau_e$ we have the explicit description: The diagram*

$$\begin{array}{ccc} \Gamma & \xrightarrow{h_{(L,\rho)}} & C_0 \\ & \searrow^{\varphi_L(-)(e)} & \wr\downarrow{\scriptstyle \rho(-)(e)} \\ & & M_L \end{array}$$

is commutative, i.e., for any $\gamma \in \Gamma$,

$$\rho\big(h_{(L,\rho)}(\gamma)\big)(e) \ = \ \varphi_L(\gamma)(e) \ = \ (\mathrm{id}_L \otimes \gamma)(e) \ .$$

Proof: By definition

$$(\rho_*^{-1} \circ \tau_e)(\gamma) \ = \ \widetilde{h_{(L,\rho)}}(\gamma) \ = \ \big(h_{(L,\rho)}(\gamma), \alpha(\gamma)\big)$$

for any $\gamma \in \Gamma$. Therefore

$$\tau_e(\gamma) \ = \ \big(\rho\big(h_{(L,\rho)}(\gamma)\big), \rho_*\alpha(\gamma)\big) \ ,$$

where $\rho_*\alpha(\gamma) = \rho \circ \alpha(\gamma) \circ \rho^{-1}$. Hence

$$\begin{aligned} \varphi_L(\gamma) \ &= \ (\sigma_e \circ \tau_e)(\gamma) \\ &= \ \sigma_e\big(\rho\big(h_{(L,\rho)}(\gamma)\big), \rho_*\alpha(\gamma)\big) \\ &= \ \rho\big(h_{(L,\rho)}(\gamma)\big) \circ s_e\big(\rho_*\alpha(\gamma)\big) \ ; \end{aligned}$$

for s_e cf. (1.8). Evaluation in $e \in M_L$ yields

$$\begin{aligned}\varphi_L(\gamma)(e) &= \rho\big(h_{(L,\rho)}(\gamma)\big) \circ s_e\big(\rho_*\alpha(\gamma)\big)\big(1_C(e)\big) \\ &= \rho\big(h_{(L,\rho)}(\gamma)\big)\big({}^{\rho_*\alpha(\gamma)}1_C(e)\big) \\ &= \rho\big(h_{(L,\rho)}(\gamma)\big)(e) \ .\end{aligned}$$

and we are done. □

For the other direction we want to assign a C_0-extension (L_h, ρ_h) to a 1-cocycle h:
Let $h \in \mathscr{Z}^1(\Gamma, C_0)$, and set $M := C_0$.
Then C_0 is canonically embedded in the symmetric group $S(M)$ viz

$$\begin{aligned} l\colon C_0 &\longrightarrow S(M) \\ c &\longmapsto l_c \ ,\end{aligned}$$

where $l_c : M \to M$ is the left multiplication with c. Denote $C := \mathrm{im}(l)$. Now let Γ act on M in the following way: The cocycle h gives a homomorphism

$$\widetilde{h}\colon \Gamma \longrightarrow C_0 \rtimes \mathrm{Aut}(C_0) \ ,$$

as described above. The embedding l yields the embedding (which maps isomorphically to the normalizer N_C—cf. (1.4))

$$\begin{aligned}\sigma_1 \circ l_*\colon C_0 \rtimes \mathrm{Aut}(C_0) &\longrightarrow S(M) \\ (c, \varphi) &\longmapsto l_c \circ \varphi \ ,\end{aligned}$$

where $l_c \circ \varphi\colon M \to M$, $m \mapsto c \cdot \varphi(m)$ and $1 = 1_{C_0} \in M$.
Composing these two maps one gets the (continuous) morphism

$$\begin{aligned}\phi_h\colon \Gamma &\longrightarrow S(M) \\ \gamma &\longmapsto l_{h(\gamma)} \circ \alpha(\gamma) \ ,\end{aligned} \tag{2}$$

which gives an action of Γ on M. Now let Γ act semilinear on $\overline{L_h} := \bigoplus_{m\in M} \bar{k} \cdot m$ by

$$\begin{aligned}\Gamma \times \bigoplus_{m\in M} \bar{k} \cdot m &\longrightarrow \bigoplus_{m\in M} \bar{k} \cdot m \\ \big(\gamma, (x_m \cdot m)\big) &\longmapsto \big(\gamma(x_m) \cdot \phi_h(\gamma)(m)\big)\end{aligned}$$

for $x_m \in \bar{k}$. Then $L_h := \overline{L_h}^{\Gamma}$ is a separable k-algebra of degree n. (cf. (18.1) in [BI])

(2.9) Remark. Because of $L_h \otimes_k \bar{k} = \overline{L_h}$, we can identify M with M_{L_h}, and then one has the equality

$$\varphi_{L_h} = \phi_h\colon \Gamma \longrightarrow S(M_{L_h}) = S(M) \ , \tag{3}$$

since both morphisms describe the Galois action of Γ on the set of the primitive idempotents $M = M_{L_h}$.

Finally we define the C_0-structure ρ_h as the injection l from above:

$$\begin{aligned}\rho_h\colon C_0 &\longrightarrow S(M_{L_h}) = S(M) \\ c &\longmapsto l_c \ .\end{aligned} \tag{4}$$

We have to prove that ρ_h is Γ-equivariant, i.e., for every $\gamma \in \Gamma$, the diagram

$$\begin{array}{ccc} C_0 & \xrightarrow{\rho_h} & S(M) \\ {\scriptstyle \alpha(\gamma)}\downarrow & & \downarrow{\scriptstyle \kappa\circ\varphi_{L_h}(\gamma)=\kappa_{\phi_h(\gamma)}} \\ C_0 & \xrightarrow{\rho_h} & S(M) \end{array}$$

is commutative. For every $c \in C_0$ we have to verify

$$\kappa_{\phi_h(\gamma)}\big(\rho_h(c)\big) \;=\; \rho_h\big(\alpha(\gamma)(c)\big)\;,$$

i.e., $\phi_h(\gamma) \circ \rho_h(c) = \rho_h({}^{\gamma}c) \circ \phi_h(\gamma)$ in $S(M)$. Indeed, evaluation in $m \in M$ gives

$$\begin{aligned} \phi_h(\gamma) \circ \rho_h(c)(m) &\overset{(2),(4)}{=} l_{h(\gamma)} \circ \alpha(\gamma) \circ l_c(m) \\ &= h(\gamma) \cdot {}^{\gamma}(c \cdot m) \\ &= {}^{\gamma}c \cdot h(\gamma) \cdot {}^{\gamma}m \\ &= l_{({}^{\gamma}c)} \cdot \big(h(\gamma) \cdot {}^{\gamma}m\big) \\ &\overset{(2),(4)}{=} \rho_h({}^{\gamma}c) \circ \phi_h(\gamma)(m)\;. \end{aligned}$$

If $[h] = [h']$, then $(L_h, \rho_h) \cong (L_{h'}, \rho_{h'})$. One can check this directly as in the previous case or it follows with the proof of (2.10).

Now we can state and prove the Theorem.

(2.10) Theorem. *There is a canonical bijection*

$$\begin{aligned} \{C_0\text{-extensions of k}\}/\!\cong \;&\xrightarrow{\sim}\; H^1(\Gamma, C_0) \\ [(L, \rho)] \;&\longmapsto\; [h_{(L,\rho)}] \\ [(L_h, \rho_h)] \;&\longmapsfrom\; [h] \end{aligned}$$

between the set of isomorphism classes of C_0-extensions and the first Galois cohomology group.

Proof: We have to prove that the two maps are inverse to each other.
Let $h \in \mathscr{Z}^1(\Gamma, C_0)$ be a 1-cocycle and write $\mathscr{L}_h$ for (L_h, ρ_h) We will show: $h = h_{\mathscr{L}_h}$. But it is enough to show $\widetilde{h} = \widetilde{h_{\mathscr{L}_h}}\colon \Gamma \longrightarrow C_0 \rtimes \mathrm{Aut}(C_0)$. It is even enough to show

$$\sigma_1 \circ l_* \circ \widetilde{h} \;=\; \sigma_1 \circ l_* \circ \widetilde{h_{\mathscr{L}_h}}\colon \Gamma \;\longrightarrow\; S(M) = S(M_{L_h})\;,$$

where $1 = 1_{C_0} \in M$. But that follows from

$$\begin{aligned} \sigma_1 \circ l_* \circ \widetilde{h_{\mathscr{L}_h}} \;&=\; \sigma_1 \circ (\rho_h)_* \circ \widetilde{h_{\mathscr{L}_h}} \\ &\overset{(1)}{=} \varphi_{L_h} \\ &\overset{(3)}{=} \phi_h \\ &\overset{(2)}{=} \sigma_1 \circ l_* \circ \widetilde{h}\;. \end{aligned}$$

§ 2. C_0-extensions

Now let $\mathscr{L} = (L, \rho)$ be a C_0-extension. $h_{\mathscr{L}}$ is defined by the equation

$$\varphi_L = \sigma_e \circ \rho_* \circ \widetilde{h_{\mathscr{L}}}$$

for some primitive idempotent $e \in M_L$. We have to show

$$(L, \rho) \;\cong\; (L_{h_{\mathscr{L}}}, \rho_{h_{\mathscr{L}}}) \;,$$

but that means just

$$\bar{L} \;\cong\; \overline{L_{h_{\mathscr{L}}}}$$

as $\bar{k}$-algebra, Γ-module and C_0-module (as described in (2.5)).
The bijective map

$$\begin{aligned} r\colon M &\longrightarrow M_L \\ c &\longmapsto \rho(c)(e) \end{aligned}$$

(remember $M = C_0$!) gives an isomorphism

$$\begin{aligned} r\colon \overline{L_{h_{\mathscr{L}}}} \;=\; \bigoplus_{c \in M} \bar{k} \cdot c \;&\xrightarrow{\sim}\; \bigoplus_{m \in M_L} \bar{k} \cdot m \;=\; \bar{L} \\ (x_c \cdot c) \;&\longmapsto\; (x_c \cdot r(c)) \end{aligned}$$

of $\bar{k}$-algebras. But r is also Γ- and C_0-equivariant: First we claim that the diagram

$$\begin{array}{ccc} C_0 \rtimes \operatorname{Aut}(C_0) & \xhookrightarrow{\sigma_1} & S(M) = S(M_{L_{h_{\mathscr{L}}}}) \\ {\scriptstyle \rho_*}\big\downarrow\wr & & {\scriptstyle r_*}\big\downarrow\wr \\ C \rtimes \operatorname{Aut}(C) & \xhookrightarrow{\sigma_e} & S(M_L) \end{array}$$

with $C := \operatorname{im}(\rho)$ and $1 = 1_{C_0} \in M$, is commutative, i.e., for $(c, \varphi) \in C_0 \rtimes \operatorname{Aut}(C_0)$, we have the identity

$$\sigma_e\big(\rho(c), \rho_*(\varphi)\big) \;=\; r_*\big(\sigma_1(c, \varphi)\big) \;.$$

To show this, evaluate the equation in an element $m = r(d) \in M_L$, $d \in M = C_0$, and the claim follows from

$$\begin{aligned} \sigma_e\big(\rho(c), \rho_*(\varphi)\big)(m) \;&=\; \sigma_e\big(\rho(c), \rho_*(\varphi)\big)\big(\rho(d)(e)\big) \\ &=\; \rho(c) \cdot {}^{\varphi}\big(\rho(d)\big)(e) \\ &=\; \rho(c \cdot {}^{\varphi}d)(e) \\ &=\; r(c \cdot {}^{\varphi}d) \\ &=\; r\big(c \cdot {}^{\varphi}(r^{-1}(m))\big) \\ &=\; r\big(\sigma_1(c, \varphi)(r^{-1}(m))\big) \\ &=\; r_*\big(\sigma_1(c, \varphi)\big)(m) \;. \end{aligned}$$

Composing this diagram in the upper left corner with either $C_0 \hookrightarrow C_0 \rtimes \operatorname{Aut}(C_0)$ and $\widetilde{h_{\mathscr{L}}}\colon \Gamma \to C_0 \rtimes \operatorname{Aut}(C_0)$ one gets the commutative diagrams

$$\begin{array}{ccc} & {\scriptstyle \rho_{h_{\mathscr{L}}}} \nearrow & S(M) \\ C_0 & & \big\downarrow {\scriptstyle r_*} \\ & {\scriptstyle \rho} \searrow & S(M_L) \end{array}$$

and

$$\begin{array}{ccc} & \overset{\phi_{h_{\mathscr{L}}}}{\nearrow} & S(M) \\ \Gamma & & \big\downarrow r_* \\ & \underset{\varphi_L}{\searrow} & S(M_L)\ . \end{array}$$

But this is just the C_0- and Γ-equivariance of r, and we are done. □

(2.11) Notation. *If (L, C) is a twisted cyclic extension of k, then—by virtue of (2.10)—the C-extension $(L, \rho\colon C \overset{\text{incl}}{\hookrightarrow} \mathrm{Aut}_{\bar{k}}(\bar{L}))$ maps to $[h_{(L,\rho)}] \in H^1(\Gamma, C)$. We will denote this cohomology class by $[L, C] \in H^1(\Gamma, C)$.*

(2.12) Remark. If (L, ρ) is a C_0-extension and $C := \mathrm{im}(\rho)$, then ρ induces an isomorphism

$$\rho_*\colon H^1(\Gamma, C_0) \xrightarrow{\sim} H^1(\Gamma, C)\ ,$$

which maps $[h_{(L,\rho)}]$ to $[L, C]$.

3. μ_n-Extensions and Kummer Extensions

Now we take a look at the case where C_0 is $\mu_n := \mu_n(\bar{k})$, the Γ-module of the n-th roots of unity. We assume that the characteristic of k does not divide n, so that μ_n is a cyclic group of order n.
Let (L, ρ) be a μ_n-extension of k, i.e., $\rho\colon \mu_n \to \mathrm{Aut}_{\bar{k}}(\bar{L})$ is Γ-equivariant. That means

$$\begin{aligned} \rho({}^{\gamma}\zeta) &= \kappa_{\varphi_L(\gamma)}\big(\rho(\zeta)\big) \\ &= \varphi_L(\gamma) \circ \rho(\zeta) \circ \varphi_L(\gamma)^{-1} \\ &= (\mathrm{id}_L \otimes\gamma) \circ \rho(\zeta) \circ (\mathrm{id}_L \otimes\gamma)^{-1} \end{aligned}$$

for $\zeta \in \mu_n$ and $\gamma \in \Gamma$ (cf. (1.10)), therefore

$$\rho({}^{\gamma}\zeta) \circ (\mathrm{id}_L \otimes\gamma) = (\mathrm{id}_L \otimes\gamma) \circ \rho(\zeta)\ , \tag{5}$$

which takes place in $\mathrm{Aut}_k(\bar{L}) = \mathrm{Aut}_k(L \otimes_k \bar{k})$.
Define

$$\overline{\mathcal{K}}_\rho := \{x \in \bar{L} : \rho(\zeta)(x) = \zeta \cdot x, \text{ for all } \zeta \in \mu_n\}\ .$$

Of course, if one chooses a primitive n-th root of unity $\xi \in \mu_n$, one has

$$\overline{\mathcal{K}}_\rho = \{x \in \bar{L} : \rho(\xi)(x) = \xi \cdot x, \}\ .$$

(2.13) Claim. *The subset $\overline{\mathcal{K}}_\rho (\subseteq \bar{L})$ is Γ-invariant with respect to the semilinear action of Γ on $\bar{L}$ (cf. the beginning of §1, 2.)*

Proof: Let $x \in \overline{\mathcal{K}}_\rho$ and $\gamma \in \Gamma$. Then for any $\zeta \in \mu_n$,

$$\begin{aligned} \rho(\zeta)\big((\mathrm{id}_L \otimes\gamma)(x)\big) &= \big(\rho(\zeta) \circ (\mathrm{id}_L \otimes\gamma)\big)(x) \\ &\overset{(5)}{=} \big((\mathrm{id}_L \otimes\gamma) \circ \rho({}^{\gamma^{-1}}\zeta)\big)(x) \\ &= (\mathrm{id}_L \otimes\gamma)\big({}^{\gamma^{-1}}\zeta \cdot x\big) \\ &= \zeta \cdot (\mathrm{id}_L \otimes\gamma)(x)\ . \end{aligned}$$

and that means $(\mathrm{id}_L \otimes\gamma)(x) \in \overline{\mathcal{K}}_\rho$. □

(2.14) Claim. *$\overline{\mathcal{K}}_\rho$ is a one dimensional $\bar{k}$-vector space. The Γ-semilinear action on $\overline{\mathcal{K}}_\rho$ gives a k-vector space $\mathcal{K}_\rho := \overline{\mathcal{K}}_\rho^\Gamma \subseteq \bar{L}^\Gamma = L$ of k-dimension one.*

Proof: $\overline{\mathcal{K}}_\rho$ is obviously a vector space, so all we have to prove is $\dim_{\bar{k}} \overline{\mathcal{K}}_\rho = 1$. But that is clear, regarding the following explicit description: Since

$$\bar{L} \;=\; \bigoplus_{\nu=0}^{n-1} \bar{k} \cdot \pi^\nu(e) \;,$$

where $e \in M_L$ is any primitive idempotent and $\pi := \rho(\xi) \in S(M_L) = \mathrm{Aut}_{\bar{k}}(\bar{L})$ for some fixed primitive n-th root of unity $\xi \in \mu_n$, it is obvious that

$$\overline{\mathcal{K}}_\rho \;=\; \left\{ \sum_{\nu=0}^{n-1} \alpha \xi^{-\nu} \cdot \pi^\nu(e) : \alpha \in \bar{k} \right\} \;,$$

because for any $y := \sum_{\nu=0}^{n-1} \alpha_\nu \xi^{-\nu} \cdot \pi^\nu(e) \in \bar{L}$, one has $\rho(\xi)(y) = \xi \cdot \sum_{\nu=0}^{n-1} \alpha_{\nu-1} \xi^{-\nu} \cdot \pi^\nu(e)$, where one has to read the index ν modulo n.
For the last claim cf. again (18.1) in [BI]. □

(2.15) Claim. *If $x \in \mathcal{K}_\rho$ is non-zero, i.e., $\mathcal{K}_\rho = k \cdot x$, then one has $x^n \in k^* = k - \{0\}$ and $L = k(x)$.*

Proof: Let $\alpha \in \bar{k}$ such that $x = \sum_{\nu=0}^{n-1} \alpha \xi^{-\nu} \cdot \pi^\nu(e) \in \mathcal{K}_\rho - \{0\}$. Then

$$x^n \;=\; \sum_{\nu=0}^{n-1} \alpha^n \cdot \pi^\nu(e) \;=\; \alpha^n \cdot \sum_{\nu=0}^{n-1} \pi^\nu(e) \;=\; \alpha^n \cdot 1 \;.$$

But of course $x^n = \alpha^n$ is Γ-invariant, i.e., $\alpha^n = x^n \in \bar{k}^\Gamma = k$.
Because the Vandermonde determinant

$$\det(\xi^{\nu\omega})_{\nu,\omega=0,\ldots,n-1} \;=\; \pm \prod_{0 \le \nu < \omega \le n} (\xi^\nu - \xi^\omega) \;\neq\; 0$$

is non-zero, the set $\{1, x, x^2, \ldots, x^{n-1}\}$ is $\bar{k}$-linearly independent and therefore a basis of $\bar{L}|\bar{k}$ and (since $x \in L$) of $L|k$. □

This claim gives rise to the following

(2.16) Definition. *A* **Kummer structure** *on a separable k-algebra L of degree n is a one dimensional k-vector subspace $\mathcal{K} \subseteq L$ such that for some non-zero element x of $\mathcal{K}$, one has the following properties*

(i) $x^n \in k^*$,

(ii) *the morphism of k-algebras $k[t]/(t^n - x^n) \to L\,,\ t \mapsto x$ is an isomorphism.*

(In this case these properties hold for any non-zero element x of $\mathcal{K}$.)
A **Kummer extension** *is a pair $(L, \mathcal{K})$ of a separable k-algebra L of degree n and a Kummer structure $\mathcal{K}$ on L.*

(2.17) Proposition. *For a separable k-algebra L of degree n there is a bijection between the set of μ_n-structures on L and the set of Kummer structures on L, given by*

$$\begin{aligned} \{\text{Kummer structures on } L\} &\xrightarrow{\sim} \{\mu_n\text{-structures on } L\} \\ \mathcal{K} &\longmapsto \rho_{\mathcal{K}} \\ \mathcal{K}_\rho &\longmapsfrom \rho \ , \end{aligned}$$

where $\rho_{\mathcal{K}}\colon \mu_n \to \mathrm{Aut}_{\bar{k}}(\bar{L})$ is given by $\rho_{\mathcal{K}}(\zeta)(x) = \zeta \cdot x$ for some non-zero element x of $\mathcal{K}$.

Proof: Note that the definition of $\rho_{\mathcal{K}}$ is independent of the choice of x and since $\bar{L} = \bar{k}(x)$, the morphism $\rho_{\mathcal{K}}$ is well defined.—The two maps are inverse to each other: First we prove $\mathcal{K} = \mathcal{K}_{\rho_{\mathcal{K}}}$: Let $x \in \mathcal{K}$ be non-zero, then

$$\mathcal{K}_{\rho_{\mathcal{K}}} \ = \ \{y \in L : \rho_{\mathcal{K}}(\zeta)(y) = \zeta \cdot y\} \ \supseteq \ k \cdot x \ = \ \mathcal{K} \ ,$$

and both are one dimensional vector spaces.
Now for $\rho = \rho_{\mathcal{K}_\rho}$: $\rho(\zeta)(x) = \zeta \cdot x = \rho_{\mathcal{K}_\rho}(\zeta)(x)$ for some $x \in \mathcal{K}_\rho$. □

(2.18) Definition. *Two Kummer extension $(L, \mathcal{K})$ and $(L', \mathcal{K}')$ of k are said to be isomorphic, if there exists an isomorphism $f\colon L \xrightarrow{\sim} L'$ of k-algebras such that $f(\mathcal{K}) = \mathcal{K}'$.*

(2.19) Remark. Of course the bijection of (2.17) respects this notion of being isomorphic, i.e.,

$$(L, \mathcal{K}) \cong (L', \mathcal{K}') \quad \Longleftrightarrow \quad (L, \rho_{\mathcal{K}}) \cong (L', \rho_{\mathcal{K}'})$$

Therefore (2.17) gives us a bijection

$$\begin{aligned} \{\text{Kummer extensions of degree } n\}/\cong \ &\longrightarrow \ \{\mu_n\text{-extensions of } k\}/\cong \\ [(L, \mathcal{K})] \ &\longmapsto \ [(L, \rho_{\mathcal{K}})] \\ [(L, \mathcal{K}_\rho)] \ &\longmapsfrom \ [(L, \rho)] \ , \end{aligned}$$

between the isomorphism classes of Kummer extensions and the isomorphism classes of μ_n-extensions.

Taking the long exact cohomology sequence to the short exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \bar{k}^* \xrightarrow{n} \bar{k}^* \longrightarrow 1$$

of Γ-modules and using Hilbert's Theorem 90 we get the well known isomorphism

$$\begin{aligned} \partial\colon k^*/k^{*n} &\xrightarrow{\sim} H^1(\Gamma, \mu_n) \\ a \cdot k^{*n} &\longmapsto [h_\alpha] \ , \end{aligned}$$

where $h_\alpha\colon \Gamma \to \mu_n$ is given by $h_\alpha(\gamma) = \frac{\alpha}{\gamma\alpha}$ for some root $\alpha \in \bar{k}^*$ of the polynomial $t^n - a$. With this interpretation of the cohomology group we can describe the composition of the maps mentioned in (2.19) and (2.10):

(2.20) Proposition. *The composition of the two maps of (2.19) and (2.10)*

$$\begin{aligned}\{\text{Kummer extensions of degree } n\}/\cong \;&\longrightarrow\; \{\mu_n\text{-extensions}\}/\cong\\ &\longrightarrow\; H^1(\Gamma,\mu_n)\\ &\xrightarrow{\partial^{-1}}\; k^*/k^{*n}\end{aligned}$$

is given by the application

$$[(L,\mathcal{K})] \;\longmapsto\; \mathcal{K}^{*n}\ ,$$

where $\mathcal{K}^{*n} = x^n \cdot k^{*n}$, *if* $\mathcal{K} = k \cdot x$.

Proof: We prove this by going a "step back" via ∂, i.e., we show $[h_{(L,\rho_\mathcal{K})}] = [h_\alpha]$, where α is a solution of $t^n - x^n = 0$ in $\bar{k}^*$. (Note first that $x^n \in k^*$ and second that $\alpha = 1 \otimes \alpha \in \bar{k} = k \otimes_k \bar{k}$ but $x = x \otimes 1 \in L = L \otimes_k k$.)
Going a second step back, we are actually proving the equality

$$(*) \qquad \varphi_L \;=\; \sigma_e \circ \rho_{\mathcal{K}*} \circ \widetilde{h_\alpha}\colon \Gamma \;\longrightarrow\; S(M_L) = \mathrm{Aut}_{\bar{k}}(\bar{L})\ ,$$

for a suitable $e \in M_L$—cf. formula (1). First observe that

$$e \;=\; \frac{1}{n}\sum_{\nu=0}^{n-1}\left(\frac{x}{\alpha}\right)^\nu$$

is an idempotent, since

$$e^2 \;=\; \frac{1}{n^2}\sum_{\nu,\omega=0}^{n-1}\left(\frac{x}{\alpha}\right)^{\nu+\omega} \;=\; e\ .$$

It is even a primitive idempotent because

$$\begin{aligned}\sum_{\zeta\in\mu_n}\rho_{\mathcal{K}*}(\zeta)(e) \;&=\; \frac{1}{n}\sum_{\zeta\in\mu_n}\sum_{\nu=0}^{n-1}\left(\frac{\zeta\cdot x}{\alpha}\right)^\nu\\ &=\; \frac{1}{n}\sum_{\nu=0}^{n-1}\sum_{\zeta\in\mu_n}\zeta^\nu\cdot\left(\frac{x}{\alpha}\right)^\nu\\ &=\; \frac{1}{n}\sum_{\zeta\in\mu_n}\zeta^0\cdot\left(\frac{x}{\alpha}\right)^0\\ &=\; 1\ .\end{aligned}$$

—Note that $\rho_\mathcal{K}(\zeta)(e) = \frac{1}{n}\sum_{\nu=0}^{n-1}\left(\frac{\zeta\cdot x}{\alpha}\right)^\nu$. Furthermore

$$\bar{L} \;=\; \bigoplus_{\nu=0}^{n-1}\bar{k}\cdot x^\nu \;\left(= \bigoplus_{\nu=0}^{n-1} x^\nu(k\otimes_k\bar{k})\right)\ .$$

Now evaluation of (*) in $\gamma \in \Gamma$ and then in the element (for an arbitrary $\zeta \in \mu_n$)

$$e' \;:=\; \rho_\mathcal{K}(\zeta)(e) \;=\; \frac{1}{n}\sum_{\nu=0}^{n-1}\left(\frac{\zeta\cdot x}{\alpha}\right)^\nu \;\in\; M_L$$

of the primitive idempotents, gives on the left side

$$\begin{aligned}\varphi_L(\gamma)(e') &= (\mathrm{id}_L \otimes\gamma)(e') \\ &= (\mathrm{id}_L \otimes\gamma)\left(\frac{1}{n}\sum_{\nu=0}^{n-1}\left(\frac{\zeta\cdot x}{\alpha}\right)^\nu\right) \\ &= \frac{1}{n}\sum_{\nu=0}^{n-1}\left(\frac{{}^\gamma\zeta\cdot x}{{}_\gamma\alpha}\right)^\nu\end{aligned}$$

On the other side of (*) we get

$$\begin{aligned}\big((\sigma_e\circ\rho_{\mathcal{K}*}\circ\widetilde{h_\alpha})(\gamma)\big)(e') &= \sigma_e\left(\rho_{\mathcal{K}}\left(\frac{\alpha}{{}_\gamma\alpha}\right),\rho_{\mathcal{K}*}(\gamma)\right)\big(\rho_{\mathcal{K}}(\zeta)(e)\big) \\ &= \rho_{\mathcal{K}}\left(\frac{\alpha}{{}_\gamma\alpha}\right)\big(\rho_{\mathcal{K}}({}^\gamma\zeta)(e)\big) \\ &= \rho_{\mathcal{K}}\left(\frac{\alpha}{{}_\gamma\alpha}{}^\gamma\zeta\right)\frac{1}{n}\sum_{\nu=0}^{n-1}\left(\frac{x}{\alpha}\right)^\nu \\ &= \frac{1}{n}\sum_{\nu=0}^{n-1}\left({}^\gamma\zeta\frac{\alpha}{{}_\gamma\alpha}\frac{x}{\alpha}\right)^\nu \\ &= \frac{1}{n}\sum_{\nu=0}^{n-1}\left(\frac{{}^\gamma\zeta\cdot x}{{}_\gamma\alpha}\right)^\nu\end{aligned}$$

This proves the claim. □

Chapter II

Twisted Cyclic Algebras

If we assume that the ground field k, of characteristic prime to n, contains the n-th roots of unity, then a cyclic algebra A of degree n is a k-algebra of the form

$$(a,b)_\zeta \;:=\; \langle X, Y : X^n = a,\, X^n = b,\, XY = \zeta YX\rangle$$

—the k-algebra generated by the two variables X and Y with the three relations $X^n - a$, $Y^n - b$ and $XY - \zeta YX$. Here, a, $b \in k^*$, and ζ is a primitive n-th root of unity.
After the base extension $\bar{k}|k$ we may assume $a = b = 1$ and we can identify $(a,b)_\zeta$ with $\mathrm{M}_n(\bar{k})$ in a way that $X = \mathrm{diag}(\zeta, \zeta^2, \ldots, \zeta^n)$ and Y is the invertible matrix which maps the canonical basis vector e_i of $\bar{k}^n$ to e_{i+1}.
In this chapter, we consider the twisted forms of this kind of algebras, i.e., algebras, which become, after base extension, isomorphic to a cyclic algebra, together with two generators fulfilling the three relations from above.

§ 3. Twisted Cyclic Algebras

In this section again fix a field k and some separable algebraic closure $\bar{k}$, and let be $\Gamma = \mathrm{Gal}(\bar{k}|k)$. Choose a positive integer $n \geq 2$ relatively prime to the characteristic of k. We abbreviate $\mu_n = \mu_n(\bar{k})$.

1. Twisted Cyclic Algebras

A twisted cyclic algebra is a twisted version of the *standard* triple (A_0, L_0, K_0), which is defined as follows: $A_0 := \mathrm{M}_n(k)$ is the k-algebra of the $n \times n$ matrices, L_0 and K_0 are two commutative subalgebras: L_0 is the subalgebra of the diagonal matrices and K_0 is the k-algebra generated by the matrix Y_0:

$$K_0 \;=\; k[Y_0] \;=\; \bigoplus_{\nu=0}^{n-1} k \cdot Y_0^\nu \;,\; \text{where } Y_0 := \begin{pmatrix} 0 & & & & & 0 & 1 \\ 1 & 0 & & & & & 0 \\ 0 & 1 & 0 & & & & \\ & \ddots & \ddots & \ddots & & & \\ & & \ddots & \ddots & 0 & & \\ & & & \ddots & 1 & 0 & \\ & & & & 0 & 1 & 0 \end{pmatrix}$$

is the matrix which maps e_i to e_{i+1}. L_0 and K_0 are maximal commutative k-subalgebras of A_0 (of degree n).

§ 3. Twisted cyclic algebras

If $\mu_n \subseteq k$ then in $\mathrm{M}_n(\bar{k})$ define for any $\zeta \in \mu_n$,

$$X_0(\zeta) := \begin{pmatrix} \zeta^1 & & & \\ & \zeta^2 & & \\ & & \ddots & \\ & & & \zeta^n \end{pmatrix}.$$

(3.1) Remark. If $\mu_n \subseteq k$, then $L_0 = k[X_0]$, where $X_0 := X_0(\zeta)$ for any primitive n-th root of unity $\zeta \in \mu_n$.

(3.2) Notation. *For k-algebras $A, L, K, A_0, L_0, K_0, \ldots$ we denote with $\bar{A}, \bar{L}, \ldots$ the $\bar{k}$-algebras $A \otimes_k \bar{k}, L \otimes_k \bar{k}, \ldots$*

(3.3) Definition. *A* **twisted cyclic k-algebra** *(of degree n) is a triple (A, L, K), where A is a central simple k-algebra of degree n, L and K are commutative k-subalgebras such that $(\bar{A}, \bar{L}, \bar{K}) \cong (\bar{A}_0, \bar{L}_0, \bar{K}_0)$ over $\bar{k}$, i.e., there exists an isomorphism*

$$\alpha\colon \bar{A} \longrightarrow \bar{A}_0 = \mathrm{M}_n(\bar{k})$$

of $\bar{k}$-algebras such that $\alpha(\bar{L}) = \bar{L}_0$ and $\alpha(\bar{K}) = \bar{K}_0$.
The pair (L, K) is called a **(twisted cyclic) decomposition** *of A.*

(3.4) Remark. If (A, L, K) is a twisted cyclic k-algebra and k' is any separable algebraic field extension of k, then $(A, L, K)_{k'} := (A \otimes_k k', L \otimes_k k', K \otimes_k k')$ is a twisted cyclic k'-algebra and vice versa. In §6 we will see that the fact holds even for algebraic field extensions which are not necessarily separable.

(3.5) Lemma. *If (A, K, L) is a twisted cyclic k-algebra, then the multiplication map $L \otimes_k K \to A$, $x \otimes y \mapsto xy$ is an isomorphism of k-modules.*

Proof: Of course it is enough to prove this after base change with $\bar{k}|k$. Because of the commutative diagram

$$\begin{array}{ccc} \bar{L} \otimes_{\bar{k}} \bar{K} & \longrightarrow & \bar{A} \\ \wr\downarrow\alpha & & \wr\downarrow\alpha \\ \bar{L}_0 \otimes_{\bar{k}} \bar{K}_0 & \longrightarrow & \bar{A}_0 \end{array}$$

of $\bar{k}$-modules, where α is defined as in (3.3) and the horizontal arrows are the multiplication maps, all we have to consider is the case $(\bar{A}_0, \bar{L}_0, \bar{K}_0)$. But it is easy to see that

$$\bar{A}_0 = \bigoplus_{\nu=0}^{n-1} \bar{L}_0 \cdot Y_0^{\nu}$$

and so the surjectivity of the map is clear, hence also the injectivity for dimension reasons. □

(3.6) Remark. Since $\bar{L} \cong \bar{L}_0 \cong \bar{k}^n$ and $\bar{K} \cong \bar{K}_0 \cong \bar{k}^n$ as $\bar{k}$-algebras, L and K are separable k-algebras of degree n for any twisted cyclic k-algebra (A, L, K) of degree n.

(3.7) Lemma. *If (A, L, K) is a twisted cyclic k-algebra, then (A, K, L) is also one.*

Proof: We only have to show it for the case (A_0, L_0, K_0), since then

$$(\bar{A}, \bar{K}, \bar{L}) \;\cong\; (\bar{A}_0, \bar{K}_0, \bar{L}_0) \;\cong\; (\bar{A}_0, \bar{L}_0, \bar{K}_0) \;.$$

So let $\zeta \in \mu_n$ be a primitive n-th root of unity, $\bar{L}_0 = \bar{k}[X_0]$, $\bar{K}_0 = \bar{k}[Y_0]$, where $X_0 := X_0(\zeta)$. For the inner automorphism

$$\kappa_{Z_0}\colon\; \bar{A}_0 = \mathrm{M}_n(\bar{k}) \;\xrightarrow{\sim}\; \bar{A}_0 = \mathrm{M}_n(\bar{k})$$

given by the conjugation with the matrix $Z_0 := Z_0(\zeta) := (\zeta^{-ij})_{i,j=1,\ldots,n} \in \mathrm{M}_n(\bar{k})$ we have $\kappa_{Z_0}(\bar{L}_0) = \bar{K}_0$ and $\kappa_{Z_0}(\bar{K}_0) = \bar{L}_0$; more precisely: One checks that $Z_0 X_0 Z_0^{-1} = Y_0$ and $Z_0 Y_0 Z_0^{-1} = X_0^{-1}$. (The second one follows from the first by taking transposes.) □

2. Pairs of Twisted Cyclic Extensions associated to Twisted Cyclic Algebras

Define for any twisted cyclic k-algebra (A, L, K) of degree n,

$$\mathcal{K}_{(L,K)} := \{X \in \bar{L} : X^n = 1,\, \kappa_X(\bar{K}) = \bar{K}\} \;,$$

—the elements of $\bar{L}^*$ of order dividing n which act on $\bar{K}$ by conjugation. Also

$$\mathcal{K}_{(K,L)} := \{Y \in \bar{K} : Y^n = 1,\, \kappa_Y(\bar{L}) = \bar{L}\} \;.$$

For these sets, we have the following obvious properties:

(3.8) Proposition. *Let (A, L, K) be a twisted cyclic k-algebra of degree n. Then*

(i) *$\mathcal{K}_{(L,K)}$ is a subgroup of $\bar{L}^*$.*

(ii) *$\mathcal{K}_{(L,K)}$ is Γ-invariant.*

(iii) *$\mu_n \subseteq \mathcal{K}_{(L,K)}$, where we view $(\mu_n \subseteq)\bar{k} \subseteq \bar{L}$ via $\bar{k} \hookrightarrow \bar{L}$, $x \mapsto 1 \otimes x$.*

(iv) *The isomorphism $\alpha\colon \bar{A} \xrightarrow{\sim} \bar{A}_0$ of $\bar{k}$-algebras of (3.3) induces an isomorphism $\alpha\colon \mathcal{K}_{(L,K)} \xrightarrow{\sim} \mathcal{K}_{(L_0,K_0)}$ of groups.*

The same holds for $\mathcal{K}_{(K,L)}$.

(3.9) Lemma. *For the twisted cyclic k-algebra (A_0, L_0, K_0) we have the explicit description:*

$$\begin{aligned}
\mathcal{K}_{(L_0,K_0)} &= \{\zeta X_0(\zeta') : \zeta, \zeta' \in \mu_n\} \\
&= \{\xi^i X_0(\xi)^j : i, j = 0, \ldots, n-1\} \\
\mathcal{K}_{(K_0,L_0)} &= \{\zeta Y_0^j : \zeta \in \mu_n,\, j = 0, \ldots, n-1\} \\
&= \{\xi^i Y_0^j : i, j = 0, \ldots, n-1\} \;,
\end{aligned}$$

where $\xi \in \mu_n$ is any primitive n-th root of unity.

Proof: Let $X \in \mathcal{K}_{(L_0,K_0)}$, then $X\bar{K}_0X^{-1} = \bar{K}_0$, especially

$$XY_0X^{-1} \;=\; a_0Y_0^0 + a_1Y_0^1 + \cdots + a_{n-1}Y_0^{n-1}$$

for some $a_i \in \bar{k}$. Since X is diagonal we must have $a_i = 0$ for $i \neq 1$: $XY_0X^{-1} \;=\; aY_0$ for some $a \in \bar{k}^*$, i.e., $X = aY_0XY_0^{-1}$, and one observes that X has the form

$$X \;=\; \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix} ,$$

where $\alpha_i \in \bar{k}^*$ and $\alpha_{i+1} = a\alpha_i$ for all i (seen modulo n), i.e., $\alpha_i = a^i\alpha$ for $\alpha := \alpha_n$, hence $a^n = 1$ (thus $a = \zeta \in \mu_n$) and $X = \alpha X_0(\zeta)$. Finally $X^n = \alpha^n = 1$, and that means $\alpha \in \mu_n$. On the other hand the elements $\zeta X_0(\zeta')$ obviously lie in $\mathcal{K}_{(L_0,K_0)}$
The second part follows from the first if one uses the isomorphism

$$\begin{aligned} \kappa_{Z_0(\xi)}\colon \mathcal{K}_{(L_0,K_0)} &\;\xrightarrow{\sim}\; \mathcal{K}_{(K_0,L_0)} \\ \xi^iX_0(\xi)^j &\;\longmapsto\; \xi^iY_0^j \ . \end{aligned}$$

mentioned in (3.7), and (3.8)(iv). □

(3.10) Proposition. *For any twisted cyclic k-algebra (A, L, K) of degree n, the groups $\mathcal{K}_{(L,K)}/\mu_n$ and $\mathcal{K}_{(K,L)}/\mu_n$ are cyclic groups of order n and they are Γ-modules.*

Proof: The last part is clear. The first part is certainly true for (A_0, L_0, K_0) as one can see at the explicit description given in (3.9). But the induced isomorphisms (of groups)

$$\begin{aligned} \alpha\colon \mathcal{K}_{(L,K)}/\mu_n &\;\xrightarrow{\sim}\; \mathcal{K}_{(L_0,K_0)}/\mu_n \\ \alpha\colon \mathcal{K}_{(K,L)}/\mu_n &\;\xrightarrow{\sim}\; \mathcal{K}_{(K_0,L_0)}/\mu_n \end{aligned}$$

show the general case. □

(3.11) Remark. We immediately get for any two generators (of the cyclic groups) $[X] \in \mathcal{K}_{(L,K)}/\mu_n$ and $[Y] \in \mathcal{K}_{(K,L)}/\mu_n$:

$$\mathcal{K}_{(L,K)} \;=\; \{\zeta X^j : \zeta \in \mu_n,\, j = 0, \ldots, n-1\}$$

and

$$\mathcal{K}_{(K,L)} \;=\; \{\zeta Y^j : \zeta \in \mu_n,\, j = 0, \ldots, n-1\} \ .$$

X and Y are any representatives of the classes $[X]$ and $[Y]$.

(3.12) Corollary. *For a twisted cyclic k-algebra (A, L, K) of degree n let $[X] \in \mathcal{K}_{(L,K)}/\mu_n$ and $[Y] \in \mathcal{K}_{(K,L)}/\mu_n$ be generators of the cyclic groups. Then*

$$\bar{L} \;=\; \bar{k}[X] \;=\; \bigoplus_{\nu=0}^{n-1} \bar{k}X^\nu \quad \text{and} \quad \bar{K} \;=\; \bar{k}[Y] \;=\; \bigoplus_{\nu=0}^{n-1} \bar{k}Y^\nu \ .$$

Proof: Again, we only have to prove this for our standard triple (A_0, L_0, K_0). In this situation it is clear that

$$X \;=\; \xi X_0(\zeta) \quad \text{and} \quad Y = \xi' Y_0^j$$

for $\zeta \in \mu_n$ primitive and $\xi, \xi' \in \mu_n$; and the claim is obvious. □

§ 3. Twisted cyclic algebras

By definition, $\mathcal{K}_{(K,L)}$ resp. $\mathcal{K}_{(L,K)}$ are sets of elements of $\bar{K}$ resp. $\bar{L}$ which act on $\bar{L}$ resp. $\bar{K}$ by conjugation. Since μ_n lies in the center of $\bar{A}$ we get the maps

$$\begin{aligned} \rho_L\colon \mathcal{K}_{(K,L)}/\mu_n &\longrightarrow \mathrm{Aut}_{\bar{k}}(\bar{L}) \\ [Y] &\longmapsto \kappa_Y \end{aligned}$$

and

$$\begin{aligned} \rho_K\colon \mathcal{K}_{(L,K)}/\mu_n &\longrightarrow \mathrm{Aut}_{\bar{k}}(\bar{K}) \\ [X] &\longmapsto \kappa_X \ . \end{aligned}$$

About these maps one knows:

(3.13) Remark. Let (A, K, L) and (A', L', K') be twisted cyclic k-algebras of degree n. Let $\alpha\colon \bar{A} \xrightarrow{\sim} \bar{A}'$ be an isomorphism of $\bar{k}$-algebras such that $\alpha(\bar{L}) = \bar{L}'$ and $\alpha(\bar{K}) = \bar{K}'$, then we have the commutative diagram

$$\begin{array}{ccc} \mathcal{K}_{(K,L)}/\mu_n & \xrightarrow{\rho_L} & \mathrm{Aut}_{\bar{k}}(\bar{L}) \\ \wr\downarrow\alpha & & \wr\downarrow\alpha \\ \mathcal{K}_{(K',L')}/\mu_n & \xrightarrow{\rho_{L'}} & \mathrm{Aut}_{\bar{k}}(\bar{L}') \ . \end{array}$$

The same holds for ρ_K and $\rho_{K'}$.

(3.14) Proposition. *Let (A, L, K) be a twisted cyclic k-algebra. Then (L, ρ_L) and (K, ρ_K) are $\mathcal{K}_{(K,L)}/\mu_n$- and $\mathcal{K}_{(L,K)}/\mu_n$-extensions.*

Proof: The map ρ_L is Γ-equivariant since for any $Y \in \mathcal{K}_{(K,L)}$ and $\gamma \in \Gamma$

$$\kappa_{(\mathrm{id}_K \otimes\gamma)Y} \ = \ \varphi_L(\gamma) \circ \kappa_Y \circ \varphi_L(\gamma)^{-1} \ = \ (\mathrm{id}_L \otimes\gamma) \circ \kappa_Y \circ (\mathrm{id}_L \otimes\gamma)^{-1} \ .$$

In fact we evaluate in any $X \in \bar{L}$:

$$\begin{aligned} \kappa_{(\mathrm{id}_K \otimes\gamma)Y}(X) \ &= \ \big((\mathrm{id}_A \otimes\gamma)Y\big)X\big((\mathrm{id}_A \otimes\gamma)Y\big)^{-1} \\ &= \ (\mathrm{id}_L \otimes\gamma)\big(Y\big((\mathrm{id}_L \otimes\gamma)^{-1}X\big)Y^{-1}\big) \\ &= \ \big((\mathrm{id}_L \otimes\gamma) \circ \kappa_Y \circ (\mathrm{id}_L \otimes\gamma)^{-1}\big)(X) \ . \end{aligned}$$

ρ_L is injective:
Regarding (3.13) it is enough to consider (A_0, L_0, K_0). Therefore Y_0 is a generator of $\mathcal{K}_{(K_0,L_0)}/\mu_n$. Now if $\rho_L([Y_0]^j) = \mathrm{id}_{\bar{L}}$, then $X_0 = Y_0^j X_0 Y_0^{-j} = \zeta^{-j} X_0$ ($X_0 = X_0(\zeta)$ and ζ some primitive n-th root of unity) therefore $n|j$. It is easy to see that $\mathrm{im}(\rho_L)$ is a transitive subgroup.—Analogously one proves the same fact about about ρ_K. □

(3.15) Proposition. *For a twisted cyclic k-algebra (A, L, K) one has the isomorphism*

$$\begin{aligned} \mathfrak{c}_{(A,L,K)}\colon \mathcal{K}_{(K,L)}/\mu_n \otimes_{\mathbb{Z}} \mathcal{K}_{(L,K)}/\mu_n &\xrightarrow{\sim} \mu_n \subseteq \bar{k}^* \\ [Y] \otimes [X] &\longmapsto XYX^{-1}Y^{-1} \ . \end{aligned}$$

of Γ-modules.

Proof: Let $X \in \mathcal{K}_{(L,K)}$ and $Y \in \mathcal{K}_{(K,L)}$, then $XYX^{-1}Y^{-1} \in \bar{K}^* \cap \bar{L}^* = \bar{k}^*$. Therefore $\mathfrak{c} := \mathfrak{c}_{(A,L,K)}$ is well defined as a map going to $\bar{k}^*$. Obviously $\mathfrak{c}$ is Γ-equivariant. $\mathfrak{c}$ is a

homomorphism of groups: e.g., let $[X] \in \mathcal{K}_{(L,K)}/\mu_n$ and $[Y] \in \mathcal{K}_{(K,L)}/\mu_n$ be generators and $a, b \in \mathbb{Z}$, then

$$\begin{aligned}\mathfrak{c}([Y^{a+b}] \otimes [X]) &= XY^{a+b}X^{-1}Y^{-a-b} \\ &= XY^aX^{-1}(XY^bX^{-1}Y^{-b})Y^{-a} \\ &= (XY^aX^{-1}Y^{-a})(XY^bX^{-1}Y^{-b}) \\ &= \mathfrak{c}([Y^a] \otimes [X])\mathfrak{c}([Y^b] \otimes [X])\ .\end{aligned}$$

The object on the left hand side of the arrow is as an abelian group isomorphic to $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$, and therefore $\mathfrak{c}$ factors through μ_n, the subgroup of $\bar{k}^*$ of the elements of order dividing n. In order to show that $\mathfrak{c}$ is an isomorphism one has to show that $\mathfrak{c}$ is surjective. Let $\zeta \in \mu_n$. With the isomorphism α: $\bar{A} \xrightarrow{\sim} \bar{A}_0$ of (3.3) we have the commutative diagram

$$\begin{array}{ccc} \mathcal{K}_{(K,L)}/\mu_n \otimes \mathcal{K}_{(L,K)}/\mu_n & & \\ \Big\downarrow \alpha & \searrow^{\mathfrak{c}_{(A,L,K)}} & \\ & & \mu_n \\ \mathcal{K}_{(K_0,L_0)}/\mu_n \otimes \mathcal{K}_{(L_0,K_0)}/\mu_n & \nearrow_{\mathfrak{c}_{(A_0,L_0,K_0)}} & \end{array}$$

All we have to show is $\zeta \in \mathrm{im}(\mathfrak{c}_{(A_0,L_0,K_0)})$. But $X_0(\zeta)Y_0X_0(\zeta)^{-1}Y_0^{-1} = \zeta$. □

Now, one easily gets the following descriptions of the ρ's.

(3.16) Corollary. *For a twisted cyclic k-algebra (A, L, K) we know about ρ_L and ρ_K the following description: Let $X \in \mathcal{K}_{(L,K)}$ and $Y \in \mathcal{K}_{(K,L)}$, then*

$$\rho_L([Y])(X) = \xi^{-1}X \quad \text{and} \quad \rho_K([X])(Y) = \xi Y\ ,$$

where $\xi = \mathfrak{c}_{(A,L,K)}([Y] \otimes [X]) \in \mu_n$.

(3.17) Remark. For any twisted cyclic k-algebra (A, L, K) there is a commutative diagram

$$\begin{array}{ccc} \mathcal{K}_{(K,L)}/\mu_n \otimes \mathcal{K}_{(L,K)}/\mu_n & \xrightarrow[\sim]{\mathfrak{c}_{(A,L,K)}} & \mu_n \\ \Big\downarrow \text{switch} & & \Big\downarrow \text{inverse} \\ \mathcal{K}_{(L,K)}/\mu_n \otimes \mathcal{K}_{(K,L)}/\mu_n & \xrightarrow[\mathfrak{c}_{(A,K,L)}]{\sim} & \mu_n\ . \end{array}$$

Starting from a twisted cyclic k-algebra (A, L, K) we got two twisted cyclic extensions (L, C) and (K, D), where we denote $C := C_{(A,L,K)} := \mathrm{im}(\rho_L)$ and $D := D_{(A,L,K)} := \mathrm{im}(\rho_K)$.
Observe the (almost) tautology $C_{(A,L,K)} = D_{(A,K,L)}$ and $D_{(A,L,K)} = C_{(A,K,L)}$.
Additionally we got an isomorphism $\mathfrak{c}_{(A,L,K)}$: $\mathcal{K}_{(K,L)}/\mu_n \otimes \mathcal{K}_{(L,K)}/\mu_n \xrightarrow{\sim} \mu_n$. This factorizes through $\rho_L \otimes \rho_K$ in the form

$$\begin{array}{ccc} \mathcal{K}_{(K,L)}/\mu_n \otimes \mathcal{K}_{(L,K)}/\mu_n & & \\ & \searrow^{\mathfrak{c}_{(A,K,L)}} & \\ \Big\downarrow \rho_L \otimes \rho_K & & \\ C \otimes D & \xrightarrow{\mathfrak{c}_{(A,K,L)}} & \mu_n\ . \end{array}$$

(3.18) Definition. *A* **pair of twisted cyclic extensions** *(of degree n) is a tuple $\big((L,C),(K,D),\mathfrak{c}\big)$, where (L,C) and (K,D) are twisted cyclic extensions (of degree n) and $\mathfrak{c}$: $C \otimes_{\mathbb{Z}} D \xrightarrow{\sim} \mu_n$ is an isomorphism of Γ-modules.*

Now we can say: There is a map from the twisted cyclic k-algebras to the pairs of twisted cyclic extensions of k (of degree n)

$$(A,L,K) \longmapsto \big((L,C_{(A,L,K)}),(K,D_{(A,L,K)}),\mathfrak{c}_{(A,L,K)}\big) .$$

In the next section we will ask the question, if every pair of twisted cyclic extensions comes from a twisted cyclic algebra.
If we have a pair of twisted cyclic extension, associated to a twisted cyclic algebra, we immediately get back A as a k-module, namely $L \otimes_k K$ (cf. (3.5)).
How about the multiplication, i.e., what are the relations of the elements of L and K by multiplication? At least we know it for the elements $\mathcal{K}_{(L,K)} \subseteq \bar{L}$ and $\mathcal{K}_{(K,L)} \subseteq \bar{K}$, since $\mathfrak{c}_{(A,L,K)}$ gives us the rule, and that is enough. But since we have only C and D, we first have to get back the groups $\mathcal{K}_{(L,K)}$ and $\mathcal{K}_{(K,L)}$.

(3.19) Lemma. *Let (A,L,K) be a twisted cyclic k-algebra and let C and D be the associated twisted cyclic structures on L and K. Then we have the following description:*

$$\mathcal{K}_{(L,K)} \;=\; \left\{ \zeta' \sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e) : \zeta',\zeta \in \mu_n \right\}$$

for any generator $c \in C$ and any primitive idempotent $e \in M_L$;

$$\mathcal{K}_{(K,L)} \;=\; \left\{ \zeta' \sum_{\nu=0}^{n-1} \zeta^\nu d^\nu(f) : \zeta',\zeta \in \mu_n \right\}$$

for any generator $d \in D$ and any primitive idempotent $f \in M_K$.

Proof: First observe that the sets on the right side are independent of the choices! Let α: $\bar{A} \to \bar{A}_0$ be an isomorphism of $\bar{k}$-algebras as in (3.3). Then α maps bijectively $\mathcal{K}_{(A,L,K)}$ to $\mathcal{K}_{(A_0,L_0,K_0)}$, $\mathrm{im}(\rho_L)$ to $\mathrm{im}(\rho_{L_0})$, M_L to M_{L_0} ... .
So we just have to prove the claim in this case: It is easy to see that $\kappa_{Y_0} \in \mathrm{Aut}_{\bar{k}}(\bar{L})$ generates $C = C_{(A_0,L_0,K_0)}$ and that E_{11} (we denote with E_{ij} the $n \times n$-matrix which has just one non-zero entry: a "1"at the place (i,j)) is a primitive idempotent of $\bar{L}_0$, in fact $M_{L_0} = \{E_{11}, E_{22}, \ldots, E_{nn}\}$. Furthermore

$$\kappa_{Y_0^\nu}(E_{11}) \;=\; Y_0^\nu E_{11} Y_0^{-\nu} \;=\; E_{1+\nu,1+\nu} .$$

thus

$$\zeta' \sum_{\nu=0}^{n-1} \zeta^\nu {\kappa_{Y_0}}^\nu(E_{11}) \;=\; \zeta' \sum_{\nu=0}^{n-1} \zeta^\nu E_{1+\nu,1+\nu} \;=\; \zeta'\zeta^{-1} X_0(\zeta) .$$

Now compare with (3.9). The second part is proved analogously. □

Now we can give an intrinsic description of (the inverse of) ρ_L and ρ_K without using the embeddings of L and K in A.

(3.20) Proposition. *Let (A, L, K) be a twisted cyclic k-algebra and ρ_L, ρ_K, $\mathfrak{c} = \mathfrak{c}_{(A,L,K)}$ the associated data. Then the inverse maps of ρ_K and ρ_L can be described in the following way:*

$$\begin{aligned} \lambda_K\colon D &\longrightarrow \mathcal{K}_{(L,K)}/\mu_n \\ d &\longmapsto \left[\sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e)\right] , \end{aligned}$$

where $c \in C$ is any generator of C, $\zeta := \mathfrak{c}(c \otimes d)$ and $e \in M_L$;

$$\begin{aligned} \lambda_L\colon C &\longrightarrow \mathcal{K}_{(K,L)}/\mu_n \\ c &\longmapsto \left[\sum_{\nu=0}^{n-1} \zeta^{-\nu} d^\nu(f)\right] , \end{aligned}$$

where $d \in D$ is any generator of D, $\zeta := \mathfrak{c}(c \otimes d)$ and $f \in M_K$.

Proof: First observe that the maps are well defined and independent of the various choices, e. g., let's prove it for λ_K.
Let c' be another generator of C, $c' = c^\omega$ for some integer ω with $(\omega, n) = 1$. Then $\zeta' := \mathfrak{c}(c' \otimes d) = \zeta^\omega$.

$$\left[\sum_{\nu=0}^{n-1} \zeta' c'^\nu(e)\right] = \left[\sum_{\nu=0}^{n-1} \zeta^{\omega\nu} c^{\omega\nu}(e)\right] = \left[\sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e)\right] .$$

Let $e' = c^\omega(e) \in M_L$ be any other primitive idempotent, then

$$\begin{aligned} \left[\sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e')\right] &= \left[\sum_{\nu=0}^{n-1} \zeta^\nu c^{\nu+\omega}(e)\right] \\ &= \left[\zeta^{-\omega} \sum_{\nu=0}^{n-1} \zeta^{\nu+\omega} c^{\nu+\omega}(e)\right] \\ &= \left[\zeta^{-\omega} \sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e)\right] \\ &= \left[\sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e)\right] . \end{aligned}$$

The same holds for λ_L. Also λ_K is a homomorphism. Let $\alpha, \beta \in \mathbb{Z}$

$$\begin{aligned} \lambda_K(d^\alpha d^\beta) &= \left[\sum_{\nu=0}^{n-1} \zeta^{(\alpha+\beta)\nu} c^\nu(e)\right] \\ &= \left[\sum_{\nu=0}^{n-1} \zeta^{\alpha\nu} \zeta^{\beta\nu} c^\nu(e)\right] \\ &= \left[\sum_{\nu=0}^{n-1} \zeta^{\alpha\nu} c^\nu(e)\right] \left[\sum_{\nu=0}^{n-1} \zeta^{\beta\nu} c^\nu(e)\right] \\ &= \lambda_K(d^\alpha)\lambda_K(d^\beta) \ ; \end{aligned}$$

the proof for λ_L is similar.
In order to show that $\lambda_K = \rho_K^{-1}$ we only need to prove $\lambda_K\big(\rho_K([X])\big) = [X]$ for $X \in \mathcal{K}_{(L,K)}$. Again by reasons of "functoriality"(cf. (3.13)) it is enough to consider the case (A_0, L_0, K_0), so we will show $\lambda_{K_0}\big(\rho_{K_0}([X_0])\big) = [X_0]$ for any $X_0 = X_0(\zeta) \in \mathcal{K}_{(L,K)}$:

$$\begin{aligned}
\lambda_{K_0}\big(\rho_{K_0}([X_0])\big) &= \lambda_{K_0}(\kappa_{X_0}) \\
&= \left[\sum_{\nu=0}^{n-1} \zeta^\nu Y_0^\nu E_{11} Y_0^{-\nu}\right] \\
&= \left[\sum_{\nu=0}^{n-1} \zeta^\nu E_{1+\nu,1+\nu}\right] \\
&= \left[\zeta^{-1} \sum_{\nu=0}^{n-1} \zeta^\nu E_{\nu\nu}\right] \\
&= [\zeta^{-1} X_0] \;=\; [X_0]\;;
\end{aligned}$$

note that $\zeta = \mathfrak{c}_{(A_0,L_0,K_0)}([Y_0] \otimes [X_0])$. Using (3.7) together with (3.17) the claim for λ_L follows from the proven one. Alternatively one can prove it directly like above. □

3. Twisted Cyclic Algebras associated to Pairs of Twisted Cyclic Extensions

Now we want to go the other direction. Given a pair of twisted cyclic extensions $\big((L,C),(K,D),\mathfrak{c}\big)$ of degree n we ask: Is there a central simple k-algebra A of degree n together with embeddings $L \hookrightarrow A$, $K \hookrightarrow A$ such that (A,L,K) is a twisted cyclic k-algebra and the associated pair $\big((L,C_{(A,L,K)}),(K,D_{(A,L,K)}),\mathfrak{c}_{(A,L,K)}\big)$ is the given one? If there is one it must be $L \otimes_k K$ by (3.5) and C, D, $\mathfrak{c}$ will give us the right multiplication on it.

(3.21) Lemma. *Given a pair $\big((L,C),(K,D),\mathfrak{c}\big)$ of twisted cyclic extensions of degree n then the following maps are well defined injective morphisms of Γ-modules, independent of the various choices:*

$$\begin{aligned}
\lambda_K\colon D &\longrightarrow \bar{L}^*/\mu_n \\
d &\longmapsto \left[\sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e)\right]\;,
\end{aligned}$$

where $c \in C$ is any generator of C, $\zeta := \mathfrak{c}(c \otimes d)$ and $e \in M_L$;

$$\begin{aligned}
\lambda_L\colon C &\longrightarrow \bar{K}^*/\mu_n \\
c &\longmapsto \left[\sum_{\nu=0}^{n-1} \zeta^{-\nu} d^\nu(f)\right]\;,
\end{aligned}$$

where $d \in D$ is any generator of D, $\zeta := \mathfrak{c}(c \otimes d)$ and $f \in M_K$.

Proof: The independence of the choices are proved exactly the same way as in the proof of (3.20).

The injectivity and the fact that the maps go to the units of $\bar{L}$ and $\bar{K}$: Taking the identification $\bar{L} \cong \bar{k}^n$ of $\bar{k}$-algebras, observe that the matrix, given by (representatives of) the vectors of $\lambda_K(d)$, $d \in D$ is (up to some elementary row and column operations) the Vandermonde matrix $(\zeta^{ij})_{i,j=0,\dots,n-1}$ for some primitive n-th root of unity ζ, and this matrix is invertible. □

Now define

$$\mathcal{K}_{(K,L),\mathfrak{c}} := \operatorname{im}(\lambda_L) \quad \text{and} \quad \mathcal{K}_{(L,K),\mathfrak{c}} := \operatorname{im}(\lambda_K) \ .$$

They are cyclic groups of order n.
Again with the Vandermonde determinant one sees

(3.22) Lemma. *If $c \in C$ is a generator of C, then the element $\lambda_L(c)$ (better: any representative) is a generator of $\mathcal{K}_{(K,L),\mathfrak{c}}$ and it is a generator of $\bar{K}$ as a $\bar{k}$-algebra, i.e., $\bar{K} = \bar{k}[\lambda_L(c)]$. Mutatis mutandis for $d \in D$ and $\bar{L}$.*

(3.23) Theorem. *Let $\big((L,C),(K,D),\mathfrak{c}\big)$ be a pair of twisted cyclic extensions of k. Then there exists a—up to a unique k-isomorphism—unique twisted cyclic k-algebra (A,L,K) such that $C = C_{(A,L,K)}$, $D = D_{(A,L,K)}$, $\mathfrak{c} = \mathfrak{c}_{(A,L,K)}$.*

Proof: *Existence:* Define A to be $L \otimes_k K$ as k-module. We have to give a multiplication on A. But this is the same as giving a—the Γ-action respecting—multiplication on $\bar{A} = \bar{L} \otimes_{\bar{k}} \bar{K}$. Choose any primitive idempotents $e \in M_L$ and $f \in M_K$ and some generators $c \in C$ and $d \in D$, then (because $\mathfrak{c}$ is an isomorphism) $\zeta := \mathfrak{c}(c \otimes d) \in \mu_n$ is a primitive n-th root of unity. Set

$$\ell_K := \sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e) \quad \text{and} \quad \ell_L := \sum_{\nu=0}^{n-1} \zeta^{-\nu} d^\nu(f) \ ,$$

then $\lambda_K(d) = [\ell_K] \in \bar{L}^*/\mu_n$, and $\lambda_L(c) = [\ell_L] \in \bar{K}^*/\mu_n$ and from (3.22) we know

$$\bar{L} \ = \ \bar{k}[\ell_K] \ = \ \bigoplus_{\nu=0}^{n-1} \bar{k} \cdot \ell_K^\nu \quad \text{and} \quad \bar{K} \ = \ \bar{k}[\ell_L] \ = \ \bigoplus_{\nu=0}^{n-1} \bar{k} \cdot \ell_L^\nu \ .$$

There is a well defined isomorphism

$$\begin{aligned} \bar{L} \otimes_{\bar{k}} \bar{K} \ &\xrightarrow{\sim}\ \bar{A}_0 \\ \ell_K^i \otimes \ell_L^j \ &\longmapsto\ X_0(\zeta)^i Y_0^j \end{aligned}$$

of $\bar{k}$-modules.
The two restrictions $\bar{L} \hookrightarrow \bar{L} \otimes_{\bar{k}} \bar{K} \to \bar{A}_0$ and $\bar{K} \hookrightarrow \bar{L} \otimes_{\bar{k}} \bar{K} \to \bar{A}_0$ are monomorphisms of $\bar{k}$-algebras, and we can define (by structure transport via this isomorphism) on $\bar{L} \otimes_{\bar{k}} \bar{K}$ a $\bar{k}$-algebra structure such that $\bar{L}$ and $\bar{K}$ are $\bar{k}$-subalgebras. The semilinear action of Γ on $\bar{L} \otimes_{\bar{k}} \bar{K}$ is even an action on the new $\bar{k}$-algebra: For that, all we have to consider is that Γ respects the multiplication of the pair ℓ_K and ℓ_L. We know $\ell_K \ell_L \ell_K^{-1} \ell_L^{-1} = \zeta$ since $X_0(\zeta) Y_0 X_0(\zeta)^{-1} Y_0^{-1} = \zeta$. For an element $\gamma \in \Gamma$ we have ${}^\gamma c = c^i$ and ${}^\gamma d = d^j$ for some integers i, j which are prime to n. Hence

$${}^\gamma\zeta \ = \ {}^\gamma\mathfrak{c}(c \otimes d) \ = \ \mathfrak{c}({}^\gamma c \otimes {}^\gamma d) \ = \ \mathfrak{c}(c^i \otimes d^j) \ = \ \zeta^{ij} \ ,$$

and this implies ${}^{\gamma}\ell_K {}^{\gamma}\ell_L {}^{\gamma}\ell_K^{-1} {}^{\gamma}\ell_L^{-1} = {}^{\gamma}\zeta$. In fact

$$\begin{aligned}
{}^{\gamma}\ell_K &= \sum_{\nu=0}^{n-1} ({}^{\gamma}\zeta)^{\nu} ({}^{\gamma}c)^{\nu}(\gamma e) \\
&= \sum_{\nu=0}^{n-1} \zeta^{ij\nu} c^{i\nu}(\gamma e) \\
&= \sum_{\nu=0}^{n-1} \zeta^{j\nu} c^{\nu}(\gamma e) \\
&= \left(\sum_{\nu=0}^{n-1} \zeta^{\nu} c^{\nu}(\gamma e) \right)^{j} \\
&= \left(\sum_{\nu=0}^{n-1} \zeta^{\nu} c^{\nu+p}(e) \right)^{j} \\
&= \left(\zeta^{-p} \sum_{\nu=0}^{n-1} \zeta^{\nu} c^{\nu}(e) \right)^{j} \\
&= \zeta^{-pj} \ell_K^j \ ,
\end{aligned}$$

where p is an integer such that $\gamma e = c^p(e)$.
Analogously ${}^{\gamma}\ell_L = \zeta^{qi}\ell_L^i$ for some integer q such that $\gamma f = d^q(f)$.
So from $\ell_K \ell_L = \zeta \ell_L \ell_K$ follows $\ell_K^j \ell_L^i = \zeta^{ij} \ell_L^i \ell_K^j$, i.e.,

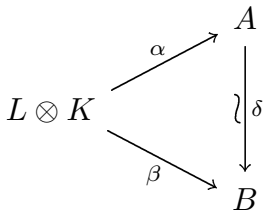
$${}^{\gamma}\ell_K {}^{\gamma}\ell_L {}^{\gamma}\ell_K^{-1} {}^{\gamma}\ell_L^{-1} \ = \ \ell_K^j \ell_L^i \ell_K^{-j} \ell_L^{-i} \ = \ \zeta^{ij} \ = \ {}^{\gamma}\zeta$$

Now we have a k-algebra structure on A. Finally we have to show that $C = C_{(A,L,K)}$, $D = D_{(A,L,K)}$ and $\mathfrak{c} = \mathfrak{c}_{(A,L,K)}$.
Claim: $\rho_L(\ell_L) = c$, i.e., $\kappa_{\ell_L} = c$: $\bar{L} \to \bar{L}$. It suffices to prove it for evaluation in $\ell_K \in \bar{L}$:

$$\begin{aligned}
\kappa_{\ell_L}(\ell_K) &= \ell_L \ell_K \ell_L^{-1} \ = \ \zeta^{-1} \ell_K \\
&= \zeta^{-1} \sum_{\nu=0}^{n-1} \zeta^{\nu} c^{\nu}(e) \\
&= \sum_{\nu=0}^{n-1} \zeta^{\nu-1} c^{\nu}(e) \\
&= \sum_{\nu=0}^{n-1} \zeta^{\nu} c^{\nu+1}(e) \\
&= c \sum_{\nu=0}^{n-1} \zeta^{\nu} c^{\nu}(e) \\
&= c\, \ell_K \ ;
\end{aligned}$$

analogously $\rho_K(\ell_K) = d$.—The claim $\mathfrak{c} = \mathfrak{c}_{(A,L,K)}$ is obvious.
Uniqueness: Let (A, L, K) and (B, L, K) be two twisted cyclic k-algebras such that

$C_{(A,L,K)} = C_{(B,L,K)}$, $D_{(A,L,K)} = D_{(B,L,K)}$ and $\mathfrak{c}_{(A,L,K)} = \mathfrak{c}_{(B,L,K)}\colon C \otimes D \to \mu_n$. Then the isomorphisms of (3.5) yield an isomorphism δ of k-modules such that



commutes. Here α and β denote the multiplication morphisms. We have to show that δ is a morphism of k-algebras. We verify it after the base extension $\bar{k}|k$. Let $\ell_K \in \bar{L}$ and $\ell_L \in \bar{K}$ be—as above—elements representing $\lambda_K(d)$, $\lambda_L(c)$, then we know

$$\bar{A} \;=\; \bigoplus_{i,j=0}^{n-1} \bar{k} \cdot \alpha(\ell_K)^i \alpha(\ell_L)^j \quad \text{and} \quad \bar{B} \;=\; \bigoplus_{i,j=0}^{n-1} \bar{k} \cdot \beta(\ell_K)^i \beta(\ell_L)^j \;.$$

Now we have to show only

$$\delta\big(\alpha(\ell_K)\alpha(\ell_L)\alpha(\ell_K)^{-1}\alpha(\ell_L)^{-1}\big) \;=\; \beta(\ell_K)\beta(\ell_L)\beta(\ell_K)^{-1}\beta(\ell_L)^{-1} \;.$$

But the two groups $\mathcal{K}_{(L,K)}$ derived from the two twisted cyclic algebras are equal (cf. (3.19)), and also the two groups $\mathcal{K}_{(K,L)}$. Also $\ell_K \in \mathcal{K}_{(L,K)}$, $\ell_L \in \mathcal{K}_{(K,L)}$, hence

$$\begin{aligned} \alpha(\ell_K)\alpha(\ell_L)\alpha(\ell_K)^{-1}\alpha(\ell_L)^{-1} \;&=\; \mathfrak{c}_{(A,L,K)}([\ell_L] \otimes [\ell_K]) \\ &=\; \mathfrak{c}_{(B,L,K)}([\ell_L] \otimes [\ell_K]) \\ &=\; \beta(\ell_K)\beta(\ell_L)\beta(\ell_K)^{-1}\beta(\ell_L)^{-1} \;. \end{aligned}$$

□

(3.24) Notation. *In the following we will denote the algebra A constructed in the proof of (3.23) with $A\big((L,C),(K,D),\mathfrak{c}\big)$.*

4. A Cohomological Classification of Twisted Cyclic Algebras

We want to classify the twisted cyclic k-algebras of degree n.
Since the twisted cyclic k-algebras are exactly the objects which become—after the base field extension $\bar{k}|k$—isomorphic to our standard model (A_0, L_0, K_0), the set of isomorphism classes of twisted cyclic k-algebras of degree n is the first Galois cohomology group over k with values in the automorphism group of our standard model. Cf. chapter X, §2 in [SeLF] or chapter VII, 29.A in [BI].

(3.25) Definition. *An* **isomorphism of twisted cyclic k-algebras** $f\colon (A,L,K) \xrightarrow{\sim} (A',L',K')$ *is an isomorphism $f\colon A \xrightarrow{\sim} A'$ of k-algebras such that $f(L) = L'$ and $f(K) = K'$. The set of the automorphisms of a twisted cyclic k-algebra (A,L,K) will be denoted by* $\mathrm{Aut}(A,L,K)$.

(3.26) Remark. As we have seen earlier, an isomorphism $f\colon (A,L,K) \xrightarrow{\sim} (A',L',K')$ of twisted cyclic k-algebras induces isomorphisms

$$f\colon \mathcal{K}_{(L,K)} \xrightarrow{\sim} \mathcal{K}_{(L',K')} \quad \text{and} \quad f\colon \mathcal{K}_{(K,L)} \xrightarrow{\sim} \mathcal{K}_{(K',L')}$$

as well as

$$f\colon \mathcal{K}_{(L,K)}/\mu_n \xrightarrow{\sim} \mathcal{K}_{(L',K')}/\mu_n \quad \text{and} \quad f\colon \mathcal{K}_{(K,L)}/\mu_n \xrightarrow{\sim} \mathcal{K}_{(K',L')}/\mu_n \ .$$

So in the case of an automorphism $f \in \mathrm{Aut}(A, L, K)$ we get the induced automorphisms

$$f_{(L,K)} := f\colon \mathcal{K}_{(L,K)}/\mu_n \xrightarrow{\sim} \mathcal{K}_{(L,K)}/\mu_n \quad \text{and} \quad f_{(K,L)} := f\colon \mathcal{K}_{(K,L)}/\mu_n \xrightarrow{\sim} \mathcal{K}_{(K,L)}/\mu_n \ ,$$

i.e., $f_{(L,K)} \in \mathrm{Aut}(\mathcal{K}_{(L,K)}/\mu_n)$ and $f_{(K,L)} \in \mathrm{Aut}(\mathcal{K}_{(K,L)}/\mu_n)$.
From (3.10) we know that $\mathcal{K}_{(L,K)}/\mu_n$ and $\mathcal{K}_{(K,L)}/\mu_n$ are cyclic groups of order n. Therefore we have the canonical identifications

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^* &= \mathrm{Aut}(\mathcal{K}_{(L,K)}/\mu_n) \\ (\nu \bmod n\mathbb{Z}) &\longmapsto ([X] \mapsto [X^\nu]) \end{aligned}$$

and

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^* &= \mathrm{Aut}(\mathcal{K}_{(K,L)}/\mu_n) \\ (\nu \bmod n\mathbb{Z}) &\longmapsto ([Y] \mapsto [Y^\nu]) \end{aligned}$$

where here $[X]$ and $[Y]$ stand for $(X \bmod \mu_n)$ and $(Y \bmod \mu_n)$. So we will view $f_{(L,K)}$ and $f_{(K,L)}$ also as elements of $(\mathbb{Z}/n\mathbb{Z})^*$.

(3.27) Lemma. *With these identifications we have*

$$f_{(L,K)} \cdot f_{(K,L)} \ = \ (1 \bmod n\mathbb{Z}) \in (\mathbb{Z}/n\mathbb{Z})^*$$

for any automorphism $f \in \mathrm{Aut}(A, L, K)$ of a twisted cyclic k-algebra (A, L, K) of degree n.

Proof: We may assume that $k = \bar{k}$ and hence that $(A, L, K) = (A_0, L_0, K_0)$ is our standard triple. Regarding $f_{(L,K)} = (\nu \bmod n\mathbb{Z})$ and $f_{(K,L)} = (\nu' \bmod n\mathbb{Z})$ as elements of $(\mathbb{Z}/n\mathbb{Z})^*$, then

$$\begin{aligned} f_{(L,K)}\colon \mathcal{K}_{(L,K)}/\mu_n &\xrightarrow{\sim} \mathcal{K}_{(L,K)}/\mu_n \\ [X_0(\xi)] &\longmapsto [X_0(\xi)^\nu] \end{aligned}$$

for any $\xi \in \mu_n$, and

$$\begin{aligned} f_{(K,L)}\colon \mathcal{K}_{(K,L)}/\mu_n &\xrightarrow{\sim} \mathcal{K}_{(K,L)}/\mu_n \\ [Y_0^m] &\longmapsto [Y_0^{m\nu'}] \end{aligned}$$

for any $m \in \mathbb{Z}$.
Now for any primitive n-th root $\zeta \in \mu_n$ of unity

$$\begin{aligned} \zeta &= f(\zeta) \\ &= f\big(X_0(\zeta)Y_0X_0(\zeta)^{-1}Y_0^{-1}\big) \\ &= X_0(\zeta)^\nu Y_0^{\nu'} X_0(\zeta)^{-\nu} Y_0^{-\nu'} \\ &= \zeta^{\nu\nu'} \ . \end{aligned}$$

Therefore $\nu\nu' \equiv 1 \pmod n$. □

Now we assume that $\mu_n = \mu(\bar{k}) \subseteq k$.

(3.28) Lemma. *If $\zeta \in \mu_n$ is a primitive n-th root of unity, then for an automorphism $f \in \mathrm{Aut}(A_0, L_0, K_0)$, the following conditions are equivalent*

(i) $f(Y_0) \in \mu_n \cdot Y_0$

(ii) $f\big(X_0(\zeta)\big) \in \mu_n \cdot X_0(\zeta)$

(iii) $f\big(X_0(\xi)\big) \in \mu_n \cdot X_0(\xi)$ *for all* $\xi \in \mu_n$

(iv) $f_{(L_0,K_0)} = (1 \bmod n\mathbb{Z})$ *is the identity*

(v) $f_{(K_0,L_0)} = (1 \bmod n\mathbb{Z})$ *is the identity.*

Proof: The equivalence of (i) and (v) as well as (ii) and (iv) is trivial since $[X_0(\zeta)]$ and $[Y_0]$ are generators of the cyclic groups $\mathcal{K}_{(L_0,K_0)}/\mu_n$ and $\mathcal{K}_{(K_0,L_0)}/\mu_n$.
The equivalence of (iv) and (v) is just (3.27).
The equivalence of (ii) and (iii) is clear. □

(3.29) Lemma. *There is an injective morphism*

$$\begin{aligned} \mu_n \times (\mathbb{Z}/n\mathbb{Z}) &\hookrightarrow \mathrm{Aut}(A_0, L_0, K_0) \\ (\xi, \bar{m}) &\longmapsto \kappa_{(\xi,\bar{m})} \end{aligned}$$

where

$$\begin{aligned} \kappa_{(\xi,\bar{m})} := \kappa_{X_0(\xi)Y_0^m} \colon A_0 &\xrightarrow{\sim} A_0 \\ Z &\longmapsto X_0(\xi)Y_0^m Z Y_0^{-m} X_0(\xi)^{-1} \ . \end{aligned}$$

—We write $\bar{m}$ for $(m \bmod n\mathbb{Z})$.
The image of this injection is the set of all automorphisms $f \in \mathrm{Aut}(A_0, L_0, K_0)$ which fulfill the conditions of (3.28).

Proof: The map is a morphism since

$$\kappa_{X_0(\xi)Y_0^m} \circ \kappa_{X_0(\xi')Y_0^{m'}} = \kappa_{X_0(\xi\xi')Y_0^{(m+m')}}$$

for ξ, $\xi' \in \mu_n$ and m, $m' \in \mathbb{Z}$. This follows from the fact that

$$X_0(\xi')Y_0^m = \xi'^m Y_0^m X_0(\xi')$$

and hence $\kappa_{X_0(\xi')} \circ \kappa_{Y_0^m} = \kappa_{Y_0^m} \circ \kappa_{X_0(\xi')}$.
Injectivity: Let $(\xi, \bar{m}) \in \mu_n \times (\mathbb{Z}/n\mathbb{Z})$ such that $\kappa_{(\xi,\bar{m})}$ is the identity. Then

$$\begin{aligned} X_0(\zeta) &= \kappa_{(\xi,\bar{m})}\big(X_0(\xi)\big) \\ &= X_0(\xi)Y_0^m X_0(\zeta) Y_0^{-m} X_0(\xi)^{-1} \\ &= \zeta^{-m} X_0(\zeta) \end{aligned}$$

for any $\zeta \in \mu_n$, hence $m \equiv 0 \pmod n$.

$$\begin{aligned} Y_0 &= \kappa_{(\xi,\bar{m})}(Y_0) \\ &= X_0(\xi)Y_0^m Y_0 Y_0^{-m} X_0(\xi)^{-1} \\ &= X_0(\xi) Y_0 X_0(\xi)^{-1} \\ &= \xi Y_0 \ , \end{aligned}$$

hence $\xi = 1$.
For the last statement, first note that for any $(\xi, \bar{m}) \in \mu_n \times (\mathbb{Z}/n\mathbb{Z})$, the induced

morphism

$$(\kappa_{(\xi,\bar{m})})_{(L_0,K_0)}\colon \mathcal{K}_{(L_0,K_0)}/\mu_n \xrightarrow{\sim} \mathcal{K}_{(L_0,K_0)}/\mu_n$$

is the identity, since

$$\kappa_{(\xi,\bar{m})}\big(X_0(\zeta)\big) \;=\; \zeta^{-m}X_0(\zeta)$$

for any $\zeta \in \mu_n$. Cf. (3.28).
On the other hand let $f \in \mathrm{Aut}(A_0, L_0, K_0)$ such that the conditions of (3.28) hold for f. Then $f(Y_0) = \xi Y_0$ for some $\xi \in \mu_n$. Choose a primitive n-th root of unity $\zeta \in \mu_n$, then we also have by (3.28) $f\big(X_0(\zeta)\big) = \zeta^{-m}X_0(\zeta)$ for some $m \in \mathbb{Z}$.
Obviously now $f = \kappa_{(\xi,\bar{m})}$, since both automorphisms are equal on the generators of A_0,—$X_0(\zeta)$ and Y_0. □

As a consequence we get

(3.30) Proposition. *There are two short exact sequences*

$$\begin{aligned} 0 \longrightarrow \mu_n \times (\mathbb{Z}/n\mathbb{Z}) \hookrightarrow \mathrm{Aut}(A_0, L_0, K_0) &\longrightarrow \mathrm{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n) \longrightarrow 1 \\ f &\longmapsto f_{(L_0,K_0)} \end{aligned}$$

and

$$\begin{aligned} 0 \longrightarrow \mu_n \times (\mathbb{Z}/n\mathbb{Z}) \hookrightarrow \mathrm{Aut}(A_0, L_0, K_0) &\longrightarrow \mathrm{Aut}(\mathcal{K}_{(K_0,L_0)}/\mu_n) \longrightarrow 1 \\ f &\longmapsto f_{(K_0,L_0)}\ . \end{aligned}$$

The surjective morphisms on the right hand side have the following sections:

$$\begin{aligned} \mathrm{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n) = (\mathbb{Z}/n\mathbb{Z})^* &\longrightarrow \mathrm{Aut}(A_0, L_0, K_0) \\ \bar{\nu} = (\nu \bmod n\mathbb{Z}) &\longmapsto f_{\bar{\nu}} \end{aligned}$$

and

$$\begin{aligned} \mathrm{Aut}(\mathcal{K}_{(K_0,L_0)}/\mu_n) = (\mathbb{Z}/n\mathbb{Z})^* &\longrightarrow \mathrm{Aut}(A_0, L_0, K_0) \\ \bar{\nu} = (\nu \bmod n\mathbb{Z}) &\longmapsto g_{\bar{\nu}} \end{aligned}$$

where $f_{\bar{\nu}}$ and $g_{\bar{\nu}}$ are given by

$$\begin{aligned} f_{\bar{\nu}}\colon A_0 &\xrightarrow{\sim} A_0 \\ X_0(\xi) &\longmapsto X_0(\xi)^{\nu} \\ Y_0 &\longmapsto Y_0^{(\nu^{-1})} \end{aligned}$$

and

$$\begin{aligned} g_{\bar{\nu}}\colon A_0 &\xrightarrow{\sim} A_0 \\ X_0(\xi) &\longmapsto X_0(\xi)^{(\nu^{-1})} \\ Y_0 &\longmapsto Y_0^{\nu} \end{aligned}$$

for any $\xi \in \mu_n$; and ν^{-1} denotes any integer such that $\nu\nu^{-1} \equiv 1 \pmod{n}$.

Proof: The first part of the proposition—except for the surjectivity in the sequences—is just (3.28) and (3.29).

The surjectivity follows with the sections: For the fact that $f_{\bar\nu}$ and $g_{\bar\nu}$ are well defined automorphisms of (A_0, L_0, K_0) observe that they conserve the relation of the two generators $X_0(\zeta)$ (for any primitive n-th root $\zeta \in \mu_n$), Y_0 and their images, e.g., for $f_{\bar\nu}$:

$$X_0(\zeta)^\nu Y_0^{(\nu^{-1})} X_0(\zeta)^{-\nu} Y_0^{-(\nu^{-1})} \;=\; \zeta^{\nu\nu^{-1}} \;=\; \zeta \;=\; X_0(\zeta) Y_0 X_0(\zeta)^{-1} Y_0^{-1} \;.$$

It is obvious that the applications $\bar\nu \mapsto f_{\bar\nu}$ and $\bar\nu \mapsto g_{\bar\nu}$ are morphisms and sections. □

(3.31) Remark. For every $\bar\nu \in (\mathbb{Z}/n\mathbb{Z})^*$ the automorphisms $f_{\bar\nu}$ and $g_{\bar\nu}$ are inverse to each other, i.e., $f_{\bar\nu} \circ g_{\bar\nu} = g_{\bar\nu} \circ f_{\bar\nu} = \mathrm{id}_{A_0}$.

In our situation of (3.30), the right hand side objects of the short exact sequences act on the left hand side objects, in a well known manner: E.g., in the first case, one takes a preimage $\varphi \in \mathrm{Aut}(A_0, L_0, K_0)$ of an element $\bar\nu \in \mathrm{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n) = (\mathbb{Z}/n\mathbb{Z})^*$ (one may take $\varphi = f_{\bar\nu}$) and, after identification of $\mu_n \times (\mathbb{Z}/n\mathbb{Z})$ with its image in $\mathrm{Aut}(A_0, L_0, K_0)$, the action of $\bar\nu$ on $\mu_n \times (\mathbb{Z}/n\mathbb{Z})$ is given by conjugation with φ. One knows that this is in fact a well defined action.

How do these actions look like in our case?

(3.32) Lemma. *The actions of the groups* $\mathrm{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n)$ *and* $\mathrm{Aut}(\mathcal{K}_{(K_0,L_0)}/\mu_n)$ *on the group* $\mu_n \times (\mathbb{Z}/n\mathbb{Z})$ *from above can be described in the following way:*
After the identification $\mathrm{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n) = (\mathbb{Z}/n\mathbb{Z})^*$, *the action of this group is*

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^* \times \big(\mu_n \times (\mathbb{Z}/n\mathbb{Z})\big) &\longrightarrow \mu_n \times (\mathbb{Z}/n\mathbb{Z}) \\ \big(\bar\nu, (\xi, \bar m)\big) &\longmapsto (\xi^\nu, \bar\nu^{-1}\bar m) \;. \end{aligned}$$

After the identification $\mathrm{Aut}(\mathcal{K}_{(K_0,L_0)}/\mu_n) = (\mathbb{Z}/n\mathbb{Z})^*$, *the action of this group is*

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^* \times \big(\mu_n \times (\mathbb{Z}/n\mathbb{Z})\big) &\longrightarrow \mu_n \times (\mathbb{Z}/n\mathbb{Z}) \\ \big(\bar\nu, (\xi, \bar m)\big) &\longmapsto (\xi^{(\nu^{-1})}, \bar\nu\bar m) \end{aligned}$$

where ν^{-1} *is any integer such that* $\nu\nu^{-1} \equiv 1 \pmod n$.

Proof: For the first case we choose $\varphi = f_{\bar\nu}$ and we have to prove

$$f_{\bar\nu} \circ \kappa_{(\xi,\bar m)} \;=\; \kappa_{(\xi^\nu, \bar\nu^{-1}\bar m)} \circ f_{\bar\nu} \;.$$

It is enough to verify this equation after evaluation in $X_0(\zeta)$ (for any $\zeta \in \mu_n$) and Y_0:

$$\begin{aligned} (f_{\bar\nu} \circ \kappa_{(\xi,\bar m)})\big(X_0(\zeta)\big) &= f_{\bar\nu}\big(\kappa_{(\xi,\bar m)}\big(X_0(\zeta)\big)\big) \\ &= f_{\bar\nu}\big(\zeta^{-m} X_0(\zeta)\big) \\ &= \zeta^{-m} X_0(\zeta)^\nu \\ &= \zeta^{-m} X_0(\zeta^\nu) \\ &= \kappa_{(\xi^\nu, \bar\nu^{-1}\bar m)}\big(X_0(\zeta^\nu)\big) \\ &= (\kappa_{(\xi^\nu, \bar\nu^{-1}\bar m)} \circ f_{\bar\nu})\big(X_0(\zeta)\big) \end{aligned}$$

and

$$\begin{aligned}(f_{\bar\nu}\circ\kappa_{(\xi,\bar m)})(Y_0^\nu) &= f_{\bar\nu}\big(\kappa_{(\xi,\bar m)}(Y_0^\nu)\big)\\ &= f_{\bar\nu}(\xi^\nu Y_0^\nu)\\ &= \xi^\nu Y_0\\ &= \kappa_{(\xi^\nu,\bar\nu^{-1}\bar m)}(Y_0)\\ &= \kappa_{(\xi^\nu,\bar\nu^{-1}\bar m)}\big(f_{\bar\nu}(Y_0^\nu)\big)\\ &= (\kappa_{(\xi^\nu,\bar\nu^{-1}\bar m)}\circ f_{\bar\nu})(Y_0^\nu)\ .\end{aligned}$$

The description of the other action follows from the fact that $g_{\bar\nu} = f_{\bar\nu}^{-1}$ for every $\bar\nu\in(\mathbb{Z}/n\mathbb{Z})^*$. □

From the last points now follows:

(3.33) Proposition. *With these actions we can construct the following semidirect products and get the isomorphisms*

$$\begin{aligned}\big(\mu_n\times(\mathbb{Z}/n\mathbb{Z})\big)\rtimes\mathrm{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n) = \big(\mu_n\times(\mathbb{Z}/n\mathbb{Z})\big)\rtimes(\mathbb{Z}/n\mathbb{Z})^* &\xrightarrow{\sim} \mathrm{Aut}(A_0,L_0,K_0)\\ \big((\xi,\bar m),\bar\nu\big) &\longmapsto \kappa_{(\xi,\bar m)}\circ f_{\bar\nu}\end{aligned}$$

and

$$\begin{aligned}\big(\mu_n\times(\mathbb{Z}/n\mathbb{Z})\big)\rtimes\mathrm{Aut}(\mathcal{K}_{(K_0,L_0)}/\mu_n) = \big(\mu_n\times(\mathbb{Z}/n\mathbb{Z})\big)\rtimes(\mathbb{Z}/n\mathbb{Z})^* &\xrightarrow{\sim} \mathrm{Aut}(A_0,L_0,K_0)\\ \big((\xi,\bar m),\bar\nu\big) &\longmapsto \kappa_{(\xi,\bar m)}\circ g_{\bar\nu}\ .\end{aligned}$$

Now let again k be a field *not necessarily* with $\mu_n\subseteq k$, and let (A,L,K) be a twisted cyclic k-algebra of degree n. We still have a separable algebraic closure $\bar k$ of k and $\Gamma=\mathrm{Gal}(\bar k|k)$.
Then Γ acts on $\mathrm{Aut}(\bar A,\bar L,\bar K)$ via conjugation

$$\begin{aligned}\Gamma\times\mathrm{Aut}(\bar A,\bar L,\bar K) &\longrightarrow \mathrm{Aut}(\bar A,\bar L,\bar K)\\ (\gamma,f) &\longmapsto (\mathrm{id}_A\otimes\gamma)\circ f\circ(\mathrm{id}_A\otimes\gamma)^{-1}\ .\end{aligned}$$

In an analogous way Γ acts by conjugation on $\mathrm{Aut}(\mathcal{K}_{(L,K)}/\mu_n)$ and $\mathrm{Aut}(\mathcal{K}_{(K,L)}/\mu_n)$. On $\mu_n\times(\mathbb{Z}/n\mathbb{Z})$ the group Γ may act in the obvious way.

(3.34) Lemma. *The actions of* Γ *on the groups* $\mathrm{Aut}(\mathcal{K}_{(L,K)}/\mu_n)$ *and* $\mathrm{Aut}(\mathcal{K}_{(K,L)}/\mu_n)$ *are trivial, so their identification with* $(\mathbb{Z}/n\mathbb{Z})^*$ *are even* Γ*-isomorphisms.*

Proof: Let $f\in\mathrm{Aut}(\mathcal{K}_{(L,K)}/\mu_n)$, i.e., there is a $\bar\nu\in(\mathbb{Z}/n\mathbb{Z})^*$ such that

$$\begin{aligned}f\colon \mathcal{K}_{(L,K)}/\mu_n &\xrightarrow{\sim} \mathcal{K}_{(L,K)}/\mu_n\\ [X] &\longmapsto [X^\nu]\ .\end{aligned}$$

Then for any $\gamma\in\Gamma$

$$\begin{aligned}(\mathrm{id}_A\otimes\gamma)\circ f\circ(\mathrm{id}_A\otimes\gamma)^{-1}([X]) &= (\mathrm{id}_A\otimes\gamma)\circ f\big([(\mathrm{id}_A\otimes\gamma)^{-1}X]\big)\\ &= (\mathrm{id}_A\otimes\gamma)\big([(\mathrm{id}_A\otimes\gamma)^{-1}X^\nu]\big)\\ &= [X^\nu]\\ &= f([X])\ .\end{aligned}$$

Analogous for the other action. □

(3.35) Lemma. *The injective morphism*

$$\begin{aligned} \mu_n \times (\mathbb{Z}/n\mathbb{Z}) &\hookrightarrow \operatorname{Aut}(\bar{A}_0, \bar{L}_0, \bar{K}_0) \\ (\xi, \bar{m}) &\longmapsto \kappa_{(\xi,\bar{m})} \end{aligned}$$

is Γ*-equivariant.*

Proof: For $\gamma \in \Gamma$, $\xi \in \mu_n$, $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ we have to show

$$(\mathrm{id} \otimes \gamma) \circ \kappa_{(\xi,\bar{m})} \circ (\mathrm{id} \otimes \gamma)^{-1} \;=\; \kappa_{(\gamma\xi,\bar{m})} \ .$$

For any $Z \in \bar{A}_0$ we have

$$\begin{aligned} \big((\mathrm{id} \otimes \gamma) \circ \kappa_{(\xi,\bar{m})} \circ (\mathrm{id} \otimes \gamma)^{-1}\big)(Z) \;&=\; (\mathrm{id} \otimes \gamma)\big(X_0(\xi) Y_0^m ((\mathrm{id} \otimes \gamma)^{-1} Z) Y_0^{-m} X_0(\xi)^{-1}\big) \\ &=\; (\mathrm{id} \otimes \gamma)\big(X_0(\xi) Y_0^m\big) \cdot Z \cdot (\mathrm{id} \otimes \gamma)\big(Y_0^{-m} X_0(\xi)^{-1}\big) \\ &=\; X_0(\gamma\xi) Y_0^m Z Y_0^{-m} X_0(\gamma\xi)^{-1} \\ &=\; \kappa_{(\gamma\xi,\bar{m})}(Z) \ , \end{aligned}$$

and we are done. □

Now we apply the former propositions to $(\bar{A}_0, \bar{L}_0, \bar{K}_0)$ and we get

(3.36) Theorem. *The short exact sequences from (3.30)*

$$0 \longrightarrow \mu_n \times (\mathbb{Z}/n\mathbb{Z}) \hookrightarrow \operatorname{Aut}(\bar{A}_0, \bar{L}_0, \bar{K}_0) \longrightarrow \operatorname{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n) \longrightarrow 1$$

and

$$0 \longrightarrow \mu_n \times (\mathbb{Z}/n\mathbb{Z}) \hookrightarrow \operatorname{Aut}(\bar{A}_0, \bar{L}_0, \bar{K}_0) \longrightarrow \operatorname{Aut}(\mathcal{K}_{(K_0,L_0)}/\mu_n) \longrightarrow 1$$

are sequences of Γ*-groups and the morphisms are* Γ*-equivariant. The two induced isomorphisms from (3.33)*

$$\beta\colon \big(\mu_n \times (\mathbb{Z}/n\mathbb{Z})\big) \rtimes \operatorname{Aut}(\mathcal{K}_{(L_0,K_0)}/\mu_n) = \big(\mu_n \times (\mathbb{Z}/n\mathbb{Z})\big) \rtimes (\mathbb{Z}/n\mathbb{Z})^* \xrightarrow{\sim} \operatorname{Aut}(A_0, L_0, K_0)$$

and

$$\beta'\colon \big(\mu_n \times (\mathbb{Z}/n\mathbb{Z})\big) \rtimes \operatorname{Aut}(\mathcal{K}_{(K_0,L_0)}/\mu_n) = \big(\mu_n \times (\mathbb{Z}/n\mathbb{Z})\big) \rtimes (\mathbb{Z}/n\mathbb{Z})^* \xrightarrow{\sim} \operatorname{Aut}(A_0, L_0, K_0)$$

are isomorphisms of Γ*-groups.*

Now, by the general theory of Galois cohomology we know that the first cohomology group over k with coefficients in $\operatorname{Aut}(\bar{A}_0, \bar{L}_0, \bar{K}_0)$ classify the twisted objects of (A_0, L_0, K_0):

(3.37) Remark. There is an isomorphism, i.e., bijection,

$$\begin{aligned} \{\text{Twisted cyclic } k\text{-algebras of degree } n\}/\cong \;&\xrightarrow{\sim}\; H^1\big(k, \operatorname{Aut}(\bar{A}_0, \bar{L}_0, \bar{K}_0)\big) \\ (A, L, K) \;&\longmapsto\; [c_\gamma] \ , \end{aligned}$$

where a representing cocycle $\Gamma \to \operatorname{Aut}(\bar{A}_0, \bar{L}_0, \bar{K}_0)\big)$, $\gamma \mapsto c_\gamma$ is given by

$$c_\gamma \;=\; \alpha \circ (\mathrm{id}_A \otimes \gamma) \circ \alpha^{-1} \circ (\mathrm{id}_{A_0} \otimes \gamma)^{-1} \ ;$$

α is any isomorphism as in the definition (3.3).

Now we fix (e.g.) the first action of $(\mathbb{Z}/n\mathbb{Z})^*$ on $\mu_n \times (\mathbb{Z}/n\mathbb{Z})$ described in (3.32) and the theorem (3.36) yields the

(3.38) Corollary. *There is an isomorphism*

$$\begin{aligned} \{\text{Twisted cyclic } k\text{-algebras of degree } n\}/\cong \ &\xrightarrow{\sim}\ H^1\big(k, \big(\mu_n \times (\mathbb{Z}/n\mathbb{Z})\big) \rtimes (\mathbb{Z}/n\mathbb{Z})^*\big) \\ (A, L, K) \ &\longmapsto\ [\beta^{-1} c_\gamma] \ . \end{aligned}$$

§ 4. Existence of Twisted Cyclic Decompositions of Central Simple Algebras

In §3, 3., we considered the question if—expressed in a sloppy manner—we can fill in the gap in $(?, L, K)$. Now we want to fill the gap in $(A, L, ?)$, i.e., we ask if we can complete L to a twisted cyclic decomposition of A.

The way we are going to find some K is the following: We transfer our situation to $\bar{A}_0$, i.e., instead of looking for a K in A, we are looking for a Γ-invariant $\bar{K}$ in $\bar{A}$—but for computational reasons we work in $\bar{A}_0$. And all we have to do is pushing the action of Γ on $\bar{A}$ to an action of Γ on $\bar{A}_0$, which is not necessarily the canonical action.
The main ingredient however is a cohomological one, which we will discuss in the first part.

1. A Cohomological Lemma

Let (L, C) be a twisted cyclic extension of k of degree n. As always Γ denotes the absolute Galois group of k—with respect to a chosen separable algebraic closure $\bar{k}$ of k. We assume that L is a field.
There is a canonical morphism of Γ-modules

$$\begin{aligned} \Xi\colon \operatorname{Hom}_{\mathbb{Z}}(C, \mu_n) &\longrightarrow \bar{L}^*/\bar{k}^* \\ u &\longmapsto \left[\textstyle\sum_{c\in C} u(c)\cdot c(e)\right] \end{aligned}$$

for any primitive idempotent $e \in M_L$ of $\bar{L}$: Γ acts on the left group in the usual way. Ξ is independent of the choice of e: Let $e' = c'(e)$ be any other primitive idempotent, $c' \in C$, then

$$\begin{aligned} \sum_{c\in C} u(c)\cdot c(e') &= \sum_{c\in C} u(c)\cdot cc'(e) \\ &= \sum_{c\in C} u(cc'^{-1})\cdot c(e) \\ &= u(c')^{-1}\sum_{c\in C} u(c)\cdot c(e)\ . \end{aligned}$$

Ξ is Γ-equivariant. Let $\gamma \in \Gamma$, then giving heed to (1.10)

$$\begin{aligned} \Xi({}^{\gamma}u) &= \Xi\big(\gamma\circ u\circ {\kappa_{\varphi_L(\gamma)}}^{-1}\big) \\ &= \left[\sum_{c\in C} \gamma u\big(\varphi_L(\gamma)^{-1}c\varphi_L(\gamma)\big)\cdot c(e)\right] \\ &= \left[\sum_{c'\in C} \gamma\big(u(c')\big)\cdot(\mathrm{id}_L\otimes\gamma)\big(c'\big((\mathrm{id}_L\otimes\gamma)^{-1}e\big)\big)\right] \\ &= (\mathrm{id}_L\otimes\gamma)\big(\Xi(u)\big)\ . \end{aligned}$$

Taking cohomology, this morphism induces the morphism

$$\Xi_* := H^1(\Gamma, \Xi)\colon H^1\big(\Gamma, \operatorname{Hom}_{\mathbb{Z}}(C, \mu_n)\big) \longrightarrow H^1(\Gamma, \bar{L}^*/\bar{k}^*)\ .$$

§ 4. Existence of twisted cyclic decompositions

(4.1) Lemma. *The cohomology group $H^1(\Gamma, \bar{L}^*/\bar{k}^*)$ is isomorphic to the relative Brauer group $\mathrm{Br}(L|k)$, and therefore it is an n-torsion group.*

Proof: First we may assume that L is embedded in $\bar{k}$, i.e., $k \subseteq L \subseteq \bar{k}$. Let $\Gamma' := \mathrm{Gal}(\bar{k}|L)$ be the absolute Galois group of L which is an open subgroup of Γ of index n. Note: $\bar{L}$ does *not* denote an algebraic closure of L but still the base extension $L \otimes_k \bar{K}$.
Claim: $\bar{L}^*$ is an induced module for $\Gamma' \subseteq \Gamma$.
The morphism of Γ-modules

$$\begin{aligned} \psi\colon \bar{L}^* = (L \otimes_k \bar{k})^* &\xrightarrow{\sim} \mathrm{Map}_{\Gamma'}(\Gamma, \bar{k}^*) \\ \textstyle\sum_\nu l_\nu \otimes x_\nu &\longmapsto \big(\tau \mapsto \textstyle\sum_\nu l_\nu \tau(x_\nu)\big) \end{aligned}$$

is an isomorphism. In fact it is the composition of the obviously bijective morphisms of Γ-modules

$$\begin{aligned} \bar{L}^* = (L \otimes_k \bar{k})^* &\xrightarrow{\sim} \prod_{\bar\sigma \in \Gamma/\Gamma'} \bar{k}^* \\ \textstyle\sum_\nu (l_\nu \otimes x_\nu) &\longmapsto \big(\textstyle\sum_\nu \sigma(l_\nu) x_\nu\big)_{\bar\sigma} \end{aligned}$$

and

$$\begin{aligned} \prod_{\bar\sigma \in \Gamma/\Gamma'} \bar{k}^* &\xrightarrow{\sim} \mathrm{Map}_{\Gamma'}(\Gamma, \bar{k}^*) \\ (a_{\bar\sigma})_{\bar\sigma} &\longmapsto \big(\tau \mapsto \tau a_{\bar\tau^{-1}}\big) \\ \big(\sigma w(\sigma^{-1})\big)_{\bar\sigma} &\longmapsto w\ . \end{aligned}$$

Here $\bar\sigma$ stands for $(\sigma \bmod \Gamma')$ and σ is any representative.
Applying cohomology to the short exact sequence

$$1 \longrightarrow \bar{k}^* \longrightarrow \bar{L}^* \longrightarrow \bar{L}^*/\bar{k}^* \longrightarrow 1$$

of Γ-modules yields, as part of the long exact cohomology sequence, the exact sequence

$$H^1(\Gamma, \bar{L}^*) \longrightarrow H^1(\Gamma, \bar{L}^*/\bar{k}^*) \xrightarrow{\delta} H^2(\Gamma, \bar{k}^*) \longrightarrow H^2(\Gamma, \bar{L}^*)\ .$$

Hilbert's Theorem 90 and Shapiro's lemma—via ψ—(cf. [ShPG], II, §2, Theorem 8, p. 31) shows

$$H^1(\Gamma, \bar{L}^*) \cong H^1\big(\Gamma, \mathrm{Map}_{\Gamma'}(\Gamma, \bar{k}^*)\big) \cong H^1(\Gamma', \bar{k}^*) = 1\ .$$

Therefore δ identifies $H^1(\Gamma, \bar{L}^*/\bar{k}^*)$ with the kernel of the right arrow of the latter sequence. We have the commutative diagram

$$\begin{array}{ccc} H^2(\Gamma, \bar{k}^*) & \longrightarrow & H^2(\Gamma, \bar{L}^*) \\ & \searrow^{(\epsilon_{\bar{k}^*})_*} & \big\downarrow \psi_* \\ & & H^2\big(\Gamma, \mathrm{Map}_{\Gamma'}(\Gamma, \bar{k}^*)\big)\ , \end{array}$$

where $\epsilon_{\bar{k}^*}$ is the composition

$$\bar{k}^* = (k \otimes_k \bar{k})^* \hookrightarrow (L \otimes_k \bar{k})^* \xrightarrow{\psi} \mathrm{Map}_{\Gamma'}(\Gamma, \bar{k}^*)\ ,$$

$\epsilon_{\bar{k}^*}(x)(\tau) = \tau(x)$ for $x \in \bar{k}^*$ and $\tau \in \Gamma$,—in concordance with the notation in [ShPG], II, §3, Proposition 7, p. 33—gives the commutative diagram

$$\begin{array}{ccc} H^2(\Gamma, \bar{k}^*) & \xrightarrow{(\epsilon_{\bar{k}^*})_*} & H^2\big(\Gamma, \mathrm{Map}_{\Gamma'}(\Gamma, \bar{k}^*)\big) \\ & \searrow^{\mathrm{res}} & \big\downarrow{\scriptstyle \wr\,\mathrm{shapiro}} \\ & & H^2(\Gamma', \bar{k}^*) \end{array}$$

Therefore our kernel is equal to the kernel of the restriction, given in the last diagram. This kernel is known to be the relative Brauer group $\mathrm{Br}(L|k)$ and this is n-torsion since the composition

$$H^2(\Gamma, \bar{k}^*) \xrightarrow{\mathrm{res}} H^2(\Gamma', \bar{k}^*) \xrightarrow{\mathrm{cor}} H^2(\Gamma, \bar{k}^*)$$

restricted to $\mathrm{Br}(L|k)$ is on the one hand zero, and on the other hand it is the multiplication with n. □

(4.2) Lemma. *Assume that Γ acts trivially on C, i.e., (L, C) is a cyclic extension, then*

$$\Xi_*\colon H^1\big(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(C, \mu_n)\big) \longrightarrow H^1(\Gamma, \bar{L}^*/\bar{k}^*)$$

is surjective.

Proof: In this case we have the isomorphism $\mathrm{ev}_\pi\colon \mathrm{Hom}_{\mathbb{Z}}(C, \mu_n) \xrightarrow{\sim} \mu_n$, $u \mapsto u(\pi)$ of Γ-modules; here we have chosen a generator $\pi \in C$ of the cyclic group $C(\subseteq \mathrm{Aut}_{\bar{k}}(\bar{L}))$. We will show the surjectivity of the composition

$$\Xi^\pi_* := \Xi_* \circ (\mathrm{ev}_\pi^{-1})_*\colon H^1(\Gamma, \mu_n) \longrightarrow H^1(\Gamma, \bar{L}^*/\bar{k}^*)\ ,$$

where this morphism is induced by

$$\begin{array}{rcl} \Xi^\pi := \Xi \circ \mathrm{ev}_\pi^{-1}\colon \mu_n & \longrightarrow & \bar{L}^*/\bar{k}^* \\ \zeta & \longmapsto & \Big[\sum_{\nu=0}^{n-1} \zeta^\nu \pi^\nu(e)\Big] \end{array}$$

for any primitive idempotent $e \in M_L$, which we want to fix.
Let us apply cohomology to the two short exact sequences

$$1 \longrightarrow \mu_n \longrightarrow \bar{k}^* \xrightarrow{n} \bar{k}^* \longrightarrow 1$$

and

$$\begin{array}{rcl} 1 \longrightarrow \bar{L}^*/\bar{k}^* \xrightarrow{1-\pi} \bar{L}^* \xrightarrow{\mathrm{N}} \bar{k}^* \longrightarrow 1\ , & & \\ l & \longmapsto & \frac{l}{\pi(l)} \end{array}$$

where N is the morphism

$$\begin{array}{rcl} \mathrm{N}\colon \bar{L}^* = \bigoplus_{e' \in M_L} \bar{k}^* \cdot e' & \longrightarrow & \bar{k}^* \\ (a_{e'}) & \longmapsto & \prod_{e' \in M_L} a_{e'}\ , \end{array}$$

induced by the Norm map $\mathrm{N}_{L|k}$. Then we get the exact sequences

$$k^* \xrightarrow{n} k^* \xrightarrow{\delta} H^1(\Gamma, \mu_n) \longrightarrow H^1(\Gamma, \bar{k}^*)$$

and

$$L^* \xrightarrow{\mathrm{N}_{L|k}} k^* \xrightarrow{\delta} H^1(\Gamma, \bar{L}^*/\bar{k}^*) \longrightarrow H^1(\Gamma, \bar{L}^*) \ .$$

But $H^1(\Gamma, \bar{k}^*) = 1$ by Hilbert's Theorem 90 and $H^1(\Gamma, \bar{L}^*) = 1$ as we have seen in the proof of (4.1). Therefore we get isomorphisms

$$\begin{aligned} \delta\colon k^*/k^{*n} &\xrightarrow{\sim} H^1(\Gamma, \mu_n) \\ (a \bmod k^{*n}) &\longmapsto [h_\alpha] \ , \end{aligned}$$

where $h_\alpha(\gamma) = \frac{\alpha}{\gamma(\alpha)}$, with some $\alpha \in \bar{k}^*$ such that $\alpha^n = a$, and

$$\begin{aligned} \delta\colon k^*/\mathrm{N}_{L|k}(L^*) &\xrightarrow{\sim} H^1(\Gamma, \bar{L}^*/\bar{k}^*) \\ \big(a \bmod \mathrm{N}_{L|k}(L^*)\big) &\longmapsto [h_\beta] \ , \end{aligned}$$

where for $\gamma \in \Gamma$ the element $h_\beta(\gamma) \in \bar{L}^*/\bar{k}^*$ is given by $(1-\pi)h_\beta(\gamma) = \frac{\beta}{\gamma(\beta)}$, with some $\beta \in \bar{L}^*$ such that $\mathrm{N}(\beta) = a$. For example one may choose $\beta = \sum_{c\in C} \alpha \cdot c(e)$ for some $\alpha \in \bar{k}^*$ with $\alpha^n = a$. Then $\frac{\beta}{\gamma(\beta)} = \sum_{c\in C}(\frac{\alpha}{\gamma(\alpha)}) \cdot c(e)$ and therefore

$$h_\beta(\gamma) \ = \ \left[\sum_{\nu=0}^{n-1} \left(\frac{\alpha}{\gamma(\alpha)}\right)^\nu \pi^\nu(e)\right] \ .$$

The diagram

$$\begin{array}{ccc} H^1(\Gamma, \mu_n) & \xrightarrow{\Xi_*^\pi} & H^1(\Gamma, \bar{L}^*/\bar{k}^*) \\ \delta\uparrow\wr & & \delta\uparrow\wr \\ k^*/k^{*n} & \xrightarrow{\mathrm{proj}} & k^*/\mathrm{N}_{L|k}\, L^* \end{array}$$

is commutative: For any a, α and β as above,

$$\begin{aligned} \Xi^\pi \circ h_\alpha(\gamma) \ &= \ \Xi^\pi \left(\frac{\alpha}{\gamma(\alpha)}\right) \\ &= \ \left[\sum_{\nu=0}^{n-1} \left(\frac{\alpha}{\gamma(\alpha)}\right)^\nu \pi^\nu(e)\right] \\ &= \ h_\beta(\gamma) \ . \end{aligned}$$

The claim follows immediately. □

(4.3) Proposition. *If $\big(n, \varphi(n)\big) = 1$, then the morphism*

$$\Xi_*\colon H^1\big(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(C, \mu_n)\big) \longrightarrow H^1(\Gamma, \bar{L}^*/\bar{k}^*)$$

is surjective.

Proof: For any $e \in M_L$ we have the factorization from (1.15)

$$\varphi_L\colon \Gamma \xrightarrow{\tau_e} C \rtimes \mathrm{Aut}(C) \xrightarrow{\sigma_e} \mathrm{Aut}_{\bar{k}}(\bar{L}) \ .$$

Set $\Gamma' := \tau_e^{-1}(C \rtimes \{1\})$ (this group is independent of the choice of e), then we see that Γ' acts trivially on C. The field extension $k' := \bar{k}^{\Gamma'}|k$ has the degree $n' := (\Gamma : \Gamma')$,

which divides $\varphi(n)$ and thus is prime to n. Therefore (4.2) says that

$$\Xi'_*\colon H^1\big(\Gamma', \mathrm{Hom}_{\mathbb{Z}}(C, \mu_n)\big) \longrightarrow H^1(\Gamma', \bar{L}^*/\bar{k}^*)$$

is surjective. Consider that in this case—the situation of k' as base field—we have $(L' := L \otimes_k k', C)$ as (twisted) cyclic extension of degree n, $\bar{k'} = \bar{k}$, $\bar{L}' = L' \otimes_{k'} \otimes \bar{k} = L \otimes_k \bar{k} = \bar{L}$ and $M_{L'} = M_L$, especially $\bar{L}'^*/\bar{k}'^* = \bar{L}^*/\bar{k}^*$. Now there is the commutative diagram

$$\begin{array}{ccc} H^1\big(\Gamma', \mathrm{Hom}_{\mathbb{Z}}(C, \mu_n)\big) & \xrightarrow{\Xi'_*} & H^1(\Gamma', \bar{L}^*/\bar{k}^*) \\ \big\downarrow \mathrm{cor} & & \big\downarrow \mathrm{cor} \\ H^1\big(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(C, \mu_n)\big) & \xrightarrow{\Xi_*} & H^1(\Gamma, \bar{L}^*/\bar{k}^*)\ . \end{array}$$

Since $H^1(\Gamma, \bar{L}^*/\bar{k}^*)$ is n-torsion the multiplication with n' is surjective, but this is also $\mathrm{cor} \circ \mathrm{res}$, therefore cor is surjective. Since now $\mathrm{cor} \circ \Xi'_* = \Xi_* \circ \mathrm{cor}$ is surjective, this is also true for Ξ_*. □

2. Galois Actions on $\bar{A}_0$

In this section we are interested in the following problem: Given a k-algebra A such that $\bar{A} \cong \bar{A}_0$ as $\bar{k}$-algebras. How does the action $(\mathrm{id}_A \otimes \gamma)$ of $\gamma \in \Gamma$ on $\bar{A}$ look like, after "transporting" it to $\bar{A}_0$? Especially in the case when we have additional structures like twisted cyclic decompositions of A.

(4.4) Notation. *Let $\sigma \in S_n$ be a permutation, then we denote by E_σ the "permutational matrix" in $\mathrm{GL}_n(k)$, which is defined by the condition that it maps the i-th canonical basis vector $e_i \in k^n$ to $e_{\sigma(i)}$.*
For example, if $\pi_0 := (1\ 2\ \ldots\ n) \in S_n$, then we have $Y_0 = E_{\pi_0}$ and more general ${Y_0}^\nu = E_{\pi_0^\nu}$ for any $\nu \in \mathbb{Z}$.

(4.5) Lemma. *Let $X \in \mathrm{GL}_n(k)$ be an invertible matrix such that the inner automorphism $\kappa_X\colon A_0 \xrightarrow{\sim} A_0$ maps L_0 to L_0. Then X has the form*

$$X \ = \ D \cdot E_\sigma\ ,$$

where D is a diagonal matrix, i.e., $D \in L_0$, and $\sigma \in S_n$ is uniquely defined by

$$\kappa_X(E_{ii}) \ = \ E_{\sigma(i),\sigma(i)}\ .$$

This decomposition of X into a product of a diagonal matrix and a permutational matrix is therefore unique.

Proof: Since κ_X is also an automorphism of the k-algebra L_0 it permutes the primitive idempotents $E_{11}, \ldots, E_{nn}$. Hence define $\sigma \in S_n$ by $\kappa_X(E_{ii}) = E_{\sigma(i),\sigma(i)}$.
So we have $X \cdot E_{ii} = E_{\sigma(i),\sigma(i)} \cdot X$ for all $i = 1, 2, \ldots, n$, and the image of the right-hand-side endomorphism is $k \cdot e_{\sigma(i)}$ whereas the image of the left-hand-side endomorphism is $X(k \cdot e_i)$. Therefore X must map $k \cdot e_i$ onto $k \cdot e_{\sigma(i)}$. So $X \circ E_{\sigma^{-1}}$ maps $k \cdot e_{\sigma(i)}$ onto itself, and that means that it is a diagonal matrix. □

(4.6) Lemma. *Additionally to the situation in (4.5) we assume that κ_X maps K_0 to K_0. Then D has the form*

$$D \;=\; \eta \cdot X_0(\zeta)$$

for a n-th root of unity $\zeta \in \mu_n(k)$ and $\eta \in k^*$. Moreover $\sigma \in N_{\langle \pi_0 \rangle} \subseteq S_n$ is an element of the normalizer subgroup of $\langle \pi_0 \rangle$, where again $\pi_0 = (1\ 2\ \ldots\ n) \in S_n$.

Proof: Since $\kappa_X(Y_0) = XY_0X^{-1} = DE_\sigma E_{\pi_0} E_\sigma^{-1} D^{-1} = DE_{\sigma\pi_0\sigma^{-1}} D^{-1} \in K_0 = k[Y_0]$ there exists a $\lambda \in k^*$ and $(i \bmod n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$ such that $\kappa_X(Y_0) = \lambda Y_0^i$, i.e., $E_{\sigma\pi_0\sigma^{-1}} = Y_0^i$ or equivalently $\sigma\pi_0\sigma^{-1} = \pi_0^i$ —hence the last claim follows. Since the order of Y_0 is n, the same holds for the order of $\kappa_X(Y_0)$ and that means $(i \bmod n\mathbb{Z}) \in (\mathbb{Z}/n\mathbb{Z})^*$. Furthermore $(\lambda Y_0^i)^n = \kappa_X(Y_0)^n = E$ we have $\lambda \in \mu_n(k)$.
Let $(j \bmod n\mathbb{Z}) \in (\mathbb{Z}/n\mathbb{Z})^*$, such that $ji \equiv 1 \pmod{n\mathbb{Z}}$. We have

$$XE_\sigma^{-1} e_n \;=\; De_n \;=\; \eta e_n$$

for some $\eta \in k^*$.
Claim: $D = \eta X_0(\zeta)$ with $\zeta = \lambda^j$.
All we have to check is $De_\nu = \eta\zeta^\nu e_\nu$. For e_n this is the definition of η. Now we know

$$XY_0 \;=\; \lambda Y_0^i X \quad \text{and} \quad E_\sigma Y_0 E_\sigma^{-1} \;=\; Y_0^i$$

and the latter can be written as $E_\sigma Y_0^j E_\sigma^{-1} = Y_0$, i.e., $E_\sigma^{-1} Y_0 = Y_0^j E_\sigma^{-1}$. Therefore

$$\begin{aligned} De_\nu \;&=\; (XE_\sigma^{-1})(Y_0^\nu e_n) \\ &=\; XE_\sigma^{-1} Y_0^\nu e_n \\ &=\; XY_0^{\nu j} E_\sigma^{-1} e_n \\ &=\; \lambda^{\nu j} Y_0^{\nu ji} XE_\sigma^{-1} e_n \\ &=\; \zeta^\nu Y_0^\nu \eta e_n \\ &= \eta\zeta^\nu e_\nu \ . \end{aligned}$$

□

(4.7) Remark. Of course both lemmas also go into the other direction, i.e., if $X = D \cdot E_\sigma$ or $X = \eta X_0(\zeta) E_\sigma$ with $\sigma \in N_{\langle \pi_0 \rangle}$, then κ_X leaves L_0, or both L_0 and K_0 respectively, invariant.

Now let A be a central simple k-algebra of degree n and $L \subseteq A$ a separable commutative k-subalgebra of k-dimension n. Then L is a maximal commutative k-subalgebra of A. We fix an isomorphism $\alpha\colon \bar{A} \xrightarrow{\sim} \bar{A}_0$ of $\bar{k}$-algebras with $\alpha(\bar{L}) = \bar{L}_0$. Such an isomorphism always exist: If $\alpha'\colon \bar{A} \xrightarrow{\sim} \bar{A}_0$ is any isomorphism of $\bar{k}$-algebras, then the set $\alpha(M_L)$ is a set of—as projectors—diagonalizable and commuting endomorphisms in $\bar{A}_0 = \mathrm{M}_n(\bar{k})$. Therefore they are simultaneously diagonalizable by say $G \in \mathrm{GL}_n(\bar{k})$. Now define $\alpha := \kappa_G \circ \alpha'$.

(4.8) Claim. *We endow the group $\mathrm{PGL}_n(\bar{k}) = \mathrm{GL}_n(\bar{k})/\bar{k}^*$ with the canonical Γ-action (or we just say $\mathrm{PGL}_n(\bar{k}) := \bar{A}_0^*/\bar{k}^*$.) For every $\gamma \in \Gamma$ there exists a unique element*

$$(X_\gamma \bmod \bar{k}^*) \in \mathrm{PGL}_n(\bar{k})$$

such that the diagram

$$\begin{array}{ccc} \bar{A} & \xrightarrow{(\mathrm{id}_A \otimes\gamma)} & \bar{A} \\ {\scriptstyle\alpha}\big\downarrow\wr & & \wr\big\downarrow{\scriptstyle\alpha} \\ \bar{A}_0 & \xrightarrow{\kappa_{X_\gamma}\circ(\mathrm{id}_{A_0}\otimes\gamma)} & \bar{A}_0 \end{array}$$

is commutative, i.e., $\alpha_*(\mathrm{id}_A \otimes\gamma) := \alpha \circ (\mathrm{id}_A \otimes\gamma) \circ \alpha^{-1} = \kappa_{X_\gamma} \circ (\mathrm{id}_{A_0} \otimes\gamma)$. *Moreover* $(X_\gamma \bmod \bar{k}^*)$ *defines a* 1*-cocycle*

$$(X_\gamma \bmod \bar{k}^*) \in \mathscr{Z}^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big) \ .$$

Proof: Since the morphism $\alpha_*(\mathrm{id}_A \otimes\gamma) \circ (\mathrm{id}_{A_0} \otimes\gamma)^{-1}$: $\bar{A}_0 \xrightarrow{\sim} \bar{A}_0$ is obviously $\bar{k}$-linear we get by Skolem-Noether's theorem a unique element $(X_\gamma \bmod \bar{k}^*) \in \mathrm{PGL}_n(\bar{k})$ such that $\kappa_{X_\gamma} = \alpha_*(\mathrm{id}_A \otimes\gamma)\circ(\mathrm{id}_{A_0} \otimes\gamma)^{-1}$, hence $\kappa_{X_\gamma}\circ(\mathrm{id}_{A_0} \otimes\gamma) = \alpha_*(\mathrm{id}_A \otimes\gamma)$. Let $\gamma, \gamma' \in \Gamma$, then

$$\begin{aligned} \kappa_{X_{\gamma\gamma'}} &= \alpha \circ (\mathrm{id}_A \otimes\gamma\gamma') \circ \alpha^{-1} \circ (\mathrm{id}_{A_0} \otimes\gamma\gamma')^{-1} \\ &= \alpha \circ (\mathrm{id}_A \otimes\gamma) \circ \alpha^{-1} \circ \alpha \circ (\mathrm{id}_A \otimes\gamma') \circ \alpha^{-1} \circ (\mathrm{id}_{A_0} \otimes\gamma')^{-1} \circ (\mathrm{id}_{A_0} \otimes\gamma)^{-1} \\ &= \alpha \circ (\mathrm{id}_A \otimes\gamma) \circ \alpha^{-1} \circ \kappa_{X_{\gamma'}} \circ (\mathrm{id}_{A_0} \otimes\gamma)^{-1} \\ &= \kappa_{X_\gamma} \circ (\mathrm{id}_{A_0} \otimes\gamma) \circ \kappa_{X_{\gamma'}} \circ (\mathrm{id}_{A_0} \otimes\gamma)^{-1} \\ &= \kappa_{X_\gamma} \circ \kappa_{(\mathrm{id}_{A_0} \otimes\gamma)(X_{\gamma'})} \\ &= \kappa_{X_\gamma (\mathrm{id}_{A_0} \otimes\gamma)(X_{\gamma'})} \ , \end{aligned}$$

hence $X_{\gamma\gamma'} \equiv X_\gamma(\mathrm{id}_{A_0} \otimes\gamma)(X_{\gamma'}) \pmod{\bar{k}^*}$, and $(X_\gamma \bmod \bar{k}^*)$ is a crossed homomorphism. □

(4.9) Notation. *If there is no way of misunderstanding we will write* γ *instead of* $(\mathrm{id}_A \otimes\gamma)$ *and* $(\mathrm{id}_{A_0} \otimes\gamma)$*, and we will write* $\alpha_*(\gamma)$ *for* $\alpha_*(\mathrm{id}_A \otimes\gamma)$.

(4.10) Remark. This is the first step (of two steps) in the definition of a morphism—which will be the opposite of the standard morphism—from the Brauer group $\mathrm{Br}(k)$ to the cohomology group $H^2(k, \bar{k}^*)$; cf. [SeLF], X, §2 and §5.

(4.11) Notation. *The set of the primitive idempotents of* L_0 *is*

$$M_{L_0} = \{E_{11}, E_{22}, \ldots, E_{nn}\} \ .$$

We identify this set with the set $\{1, \ldots, n\}$ *via* $i \mapsto E_{ii}$*, such that we also can easily identify* $S(M_{L_0})$ *with* S_n.
The isomorphism α: $\bar{L} \xrightarrow{\sim} \bar{L}_0$ *gives a bijection* α: $M_L \xrightarrow{\sim} M_{L_0} = \{1, \ldots, n\}$. *This gives rise to the composition*

$$\Gamma \xrightarrow{\varphi_L} S(M_L) \xrightarrow{\alpha_*} S(M_{L_0}) = S_n \ ,$$

and we will denote for any $\gamma \in \Gamma$,

$$\tilde{\gamma} := \alpha_*\big(\varphi_L(\gamma)\big) \in S_n \ .$$

In other words we have the commutative diagram

$$\begin{array}{ccc} M_L & \xrightarrow{\varphi_L(\gamma)=(\mathrm{id}_A\otimes\gamma)} & M_L \\ \wr\downarrow\alpha & & \wr\downarrow\alpha \\ M_{L_0} & \longrightarrow & M_{L_0} \\ \| & & \| \\ \{1,\dots,n\} & \xrightarrow{\tilde\gamma} & \{1,\dots,n\} \end{array}$$

and the middle horizontal arrow is defined by $E_{ii} \mapsto E_{\tilde\gamma(i),\tilde\gamma(i)}$. *We have*

$$E_{\tilde\gamma(i),\tilde\gamma(i)} = \alpha_*(\mathrm{id}_A\otimes\gamma)(E_{ii}) = \alpha_*(\mathrm{id}_A\otimes\gamma)(\mathrm{id}_{A_0}\otimes\gamma)^{-1}(E_{ii}) = \kappa_{X_\gamma}(E_{ii})\ .$$

(4.12) Remark. Since both $\alpha_*(\mathrm{id}_A\otimes\gamma)$ and $(\mathrm{id}_{A_0}\otimes\gamma)$ leave $\bar L_0$ invariant we know by (4.5) about the matrix X_γ, that it has the form $X_\gamma = D_\gamma\cdot E_{\tilde\gamma}$, where D_γ is a diagonal matrix and $(D_\gamma \bmod \bar k^*) \in \bar L_0^*/\bar k^*$ is unique. But we can say more about D_γ:

(4.13) Proposition. *There is a unique* 1*-cocycle*

$$(\widetilde D_\gamma \bmod \bar k^*) \in \mathscr{Z}^1(\Gamma, \bar L^*/\bar k^*)$$

such that

$$D_\gamma \ \equiv\ \alpha(\widetilde D_\gamma) \pmod{\bar k^*}\ .$$

Proof: Since $\alpha\colon \bar A \xrightarrow{\sim} \bar A_0$ yields am isomorphism $\alpha\colon \bar L^*/\bar k^* \xrightarrow{\sim} \bar L_0^*/\bar k^*$ just define

$$\widetilde D_\gamma \bmod \bar k^* \ :=\ \alpha^{-1}(D_\gamma \bmod \bar k^*)\ .$$

All we have to prove is that $(\widetilde D_\gamma \bmod \bar k^*)$ is a 1-cocycle, i.e., for $\gamma,\gamma'\in\Gamma$,

$$\widetilde D_{\gamma\gamma'} \ \equiv\ \widetilde D_\gamma\cdot(\mathrm{id}_A\otimes\gamma)(\widetilde D_{\gamma'}) \pmod{\bar k^*}\ .$$

Applying α_* this is equivalent to showing

$$D_{\gamma\gamma'} \ \equiv\ D_\gamma\cdot\alpha_*(\mathrm{id}_A\otimes\gamma)(D_{\gamma'}) \pmod{\bar k^*}\ .$$

We know from (4.8) and (4.12)

$$\begin{aligned} D_{\gamma\gamma'}E_{\tilde\gamma\tilde\gamma'} &\equiv X_{\gamma\gamma'} \\ &\equiv X_\gamma(\mathrm{id}_{A_0}\otimes\gamma)(X_{\gamma'}) \\ &\equiv D_\gamma E_{\tilde\gamma}(\mathrm{id}_{A_0}\otimes\gamma)(D_{\gamma'}E_{\tilde\gamma'}) \\ &\equiv D_\gamma E_{\tilde\gamma}(\mathrm{id}_{A_0}\otimes\gamma)(D_{\gamma'})E_{\tilde\gamma'} \pmod{\bar k^*}\ ; \end{aligned}$$

and this is equivalent to

$$D_{\gamma\gamma'} \ \equiv\ D_\gamma\kappa_{E_{\tilde\gamma}}\big((\mathrm{id}_{A_0}\otimes\gamma)(D_{\gamma'})\big) \pmod{\bar k^*}\ .$$

But the latter equivalence shows that $\kappa_{E_{\tilde\gamma}}\big((\mathrm{id}_{A_0}\otimes\gamma)(D_{\gamma'})\big)$ is diagonal, so it is equal to

$$\kappa_{D_\gamma}\circ\kappa_{E_{\tilde\gamma}}\big((\mathrm{id}_{A_0}\otimes\gamma)(D_{\gamma'})\big) = \alpha_*(\mathrm{id}_A\otimes\gamma)(D_{\gamma'})\ .$$

Replacing this in the last equation we get our cocycle condition. □

3. The Existence of a Twisted Cyclic Decomposition

Again, let A be a central simple k-algebra of degree n, let (L, C) be a twisted cyclic extension of k of degree n and assume that $L \subseteq A$ is a subalgebra of A. Choose a generator $\pi \in C$ of C and an isomorphism $\alpha\colon \bar{A} \xrightarrow{\sim} \bar{A}_0$ of $\bar{k}$-algebras such that $\alpha(\bar{L}) = \bar{L}_0$.
We may assume that $\alpha_*(\pi) = \alpha \circ \pi \circ \alpha^{-1} \in S(M_{L_0}) = S_n$ is the permutation $\pi_0 := (1\ 2\ \ldots\ n) \in S_n$, i.e., $(\alpha \circ \pi \circ \alpha^{-1})(E_{ii}) = E_{i+1,i+1}$. The index is viewed modulo n.
If this is not already the case, then there exists a $\sigma \in S_n$ such that $\sigma\alpha_*(\pi)\sigma^{-1} = \pi_0$. If we change α to $\kappa_{E_\sigma} \circ \alpha$, then we have our desired property.

(4.14) Lemma. *In this situation, the composition*

$$\mathrm{Hom}_{\mathbb{Z}}(C, \mu_n) \xrightarrow{\Xi} \bar{L}^*/\bar{k}^* \xrightarrow{\alpha} \bar{L}_0^*/\bar{k}^*$$

can be described as

$$(\alpha \circ \Xi)(u) \;=\; \big[X_0\big(u(\pi)\big)\big]\ .$$

Proof: We choose for the primitive idempotent $e \in M_L$ the element $e := \alpha^{-1}(E_{nn})$. Then

$$\begin{aligned}(\alpha \circ \Xi)(u) \;&=\; \alpha\left[\sum_{\nu=0}^{n-1} u(\pi^\nu)\pi^\nu(e)\right]\\ &=\; \left[\sum_{\nu=0}^{n-1} u(\pi)^\nu \alpha_*(\pi)^\nu(E_{nn})\right]\\ &=\; \left[\sum_{\nu=0}^{n-1} u(\pi)^\nu E_{\pi_0^\nu(n),\pi_0^\nu(n)}\right]\\ &=\; \left[\sum_{\nu=0}^{n-1} u(\pi)^\nu E_{\nu,\nu}\right]\\ &=\; \big[X_0\big(u(\pi)\big)\big]\ .\end{aligned}$$

□

(4.15) Theorem. *Assume that L is a field and $\big(n, \varphi(n)\big) = 1$. Then there exists a separable k-subalgebra K of A of degree n such that (A, L, K) is a twisted cyclic k-algebra of degree n. Moreover $C = C_{(A,L,K)}$.*

Proof: Let $(X_\gamma \bmod \bar{k}^*) \in \mathscr{Z}^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big)$ be the 1-cocycle constructed in (4.8). (This, of course, depends on the choice of α—we take the α from above.) Then, with $D_\gamma := X_\gamma E_{\tilde{\gamma}}^{-1}$, by (4.13) there exists a 1-cocycle $(\widetilde{D}_\gamma \bmod \bar{k}^*) \in \mathscr{Z}^1(\Gamma, \bar{L}^*/\bar{k}^*)$ such that $D_\gamma \equiv \alpha(\widetilde{D}_\gamma) \pmod{\bar{k}^*}$.
Because of (4.3) there is a 1-cocycle

$$u_\gamma \in \mathscr{Z}^1\big(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(C, \mu_n)\big)$$

such that

$$[\Xi \circ u_\gamma] \;=\; [\tilde{D}_\gamma] \in H^1(\Gamma, \bar{L}^*/\bar{k}^*)\ ,$$

i.e., there is a $\Delta \in \bar{L}^*$ such that

$$\widetilde{D}_\gamma \;\equiv\; (\Xi \circ u_\gamma) \cdot {}^\gamma\Delta \cdot \Delta^{-1} \pmod{\bar{k}^*}$$

for all $\gamma \in \Gamma$. Applying α and defining $\Delta_0 := \alpha(\Delta)$ we get with (4.14)

$$D_\gamma \;\equiv\; X_0\big(u_\gamma(\pi)\big) \cdot \alpha_*(\mathrm{id}_A \otimes\gamma)(\Delta_0) \cdot \Delta_0^{-1} \pmod{\bar{k}^*} \;,$$

For all $\gamma \in \Gamma$. But

$$\alpha_*(\mathrm{id}_A \otimes\gamma) \;=\; E_{\tilde{\gamma}} \cdot (\mathrm{id}_{A_0} \otimes\gamma)(\Delta_0) \cdot E_{\tilde{\gamma}}^{-1} \pmod{\bar{k}^*} \;,$$

since $\Delta_0 \in \bar{L}_0$ is diagonal. Therefore

$$\Delta_0 \cdot D_\gamma \cdot E_{\tilde{\gamma}} \;\equiv\; X_0\big(u_\gamma(\pi)\big) \cdot E_{\tilde{\gamma}} \cdot (\mathrm{id}_{A_0} \otimes\gamma)(\Delta_0) \pmod{\bar{k}^*} \;;$$

in other words: The diagram

$$\begin{array}{ccc} \bar{A}_0 & \xrightarrow{\kappa_{(D_\gamma E_{\tilde{\gamma}})} \circ (\mathrm{id}_{A_0} \otimes\gamma)} & \bar{A}_0 \\ {\scriptstyle \kappa_{\Delta_0}}\big\downarrow & & \big\downarrow{\scriptstyle \kappa_{\Delta_0}} \\ \bar{A}_0 & \xrightarrow{\kappa_{(X_0(u_\gamma(\pi)) E_{\tilde{\gamma}})} \circ (\mathrm{id}_{A_0} \otimes\gamma)} & \bar{A}_0 \end{array}$$

is commutative. If we replace α by $\kappa_{\Delta_0} \circ \alpha$, then

$$X_\gamma \;=\; X_0\big(u_\gamma(\pi)\big) \cdot E_{\tilde{\gamma}}$$

and (4.7) says that κ_{X_γ}, and also $\kappa_{X_\gamma} \circ (\mathrm{id}_{A_0} \otimes\gamma)$, leaves $\bar{L}_0$ and $\bar{K}_0$ invariant. Define $\bar{K} := \alpha^{-1}(\bar{K}_0)$, then $\bar{K} \subseteq \bar{A}$ is Γ-invariant. Define K to be $\bar{K}^\Gamma$, and we are done. The last statement of the theorem follows, e.g., from the uniqueness of C, cf. (1.30). □

§ 5. A Cohomological Description of Twisted Cyclic Algebras

In this section we fix a twisted cyclic k-algebra (A, L, K) of degree n—or equivalently—a pair of twisted cyclic extensions $\big((L,C),(K,D),\mathfrak{c}\big)$ of degree n (which is associated to this algebra.)
The well known isomorphism between the Brauer group $\mathrm{Br}(k)$ of k and the cohomology group $H^2(k,\bar{k}^*)$ gives us a two-dimensional cohomology class $[A]$, associated to the central simple k-algebra A.
On the other hand we constructed in §2 the one-dimensional cohomology classes $[L,C]$ and $[K,D]$.
In this rather technical section we will show how these three classes are related.

1. The Theorem

In §2 we constructed the cohomology classes

$$[L,C] \in H^1(\Gamma, C) \quad \text{and} \quad [K,D] \in H^1(\Gamma, D)\ .$$

Their cup-product is a two-dimensional cohomology class

$$[L,C] \cup [K,D] \in H^2(\Gamma, C \otimes_{\mathbb{Z}} D)\ .$$

The isomorphism $\mathfrak{c}\colon C \otimes_{\mathbb{Z}} D \xrightarrow{\sim} \mu_n$ of Γ-modules induces the isomorphism

$$\mathfrak{c}_*\colon H^2(\Gamma, C \otimes_{\mathbb{Z}} D) \xrightarrow{\sim} H^2(\Gamma, \mu_n)$$

of the cohomology groups, and the right-hand-side group can canonically be identified with the n-torsion part of $H^2(\Gamma,\bar{k}^*)$. (Apply cohomology to the short exact sequence $1 \to \mu_n \longrightarrow \bar{k}^* \xrightarrow{n} \bar{k}^* \to 1$ and use Hilbert's Theorem 90 to get the exact sequence $1 \xrightarrow{\delta} H^2(\Gamma,\mu_n) \longrightarrow H^2(\Gamma,\bar{k}^*) \xrightarrow{n} H^2(\Gamma,\bar{k}^*)$.) Therefore

$$\mathfrak{c}_*\big([L,C] \cup [K,D]\big) \in H^2(\Gamma, \bar{k}^*)\ .$$

If we use the well known identification $H^2(\Gamma,\bar{k}^*) = \mathrm{Br}(\bar{k})$—we will use the construction of Serre in [SeLF], X, which is the opposite of the standard morphism, constructed by means of "crossed products"—we can see this class as an element of the Brauer group of k. On the other hand we have the element $[A] \in \mathrm{Br}(k)$. They are connected in the following way:

(5.1) Theorem. *Let $\big((L,C),(K,D),\mathfrak{c}\big)$ be a pair of twisted cyclic extensions of degree n and assume that Γ acts transitively on M_L, then*

$$\mathfrak{c}_*\big([L,C] \cup [K,D]\big) \;=\; -\big[A\big((L,C),(K,D),\mathfrak{c}\big)\big]\ .$$

(5.2) Remark. The additional assumption is true, e.g., if L is a field. Of course for reasons of symmetry, one can alternatively assume that Γ acts transitively on M_K.

We will show the theorem by a—lengthy—direct computation with cocycles. In order to do that we first have to compute a 2-cocycle which represents the cohomology class

$[A] \in \mathrm{Br}(k) = H^2(\Gamma, \bar{k}^*)$ and two 1-cocycles representing the cohomology classes $[L, C] \in H^1(\Gamma, C)$ and $[K, D] \in H^1(\Gamma, D)$.

Recall that the construction given in [SeLF], X, §2 and §5 has two steps: Starting with a central simple algebra of degree n, one first gets (as shown in (4.8)) a cohomology class in $H^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big)$. By virtue of the connecting morphism δ: $H^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big) \longrightarrow H^2(\Gamma, \bar{k}^*)$ that appears in the long exact cohomology sequence which is associated to the short exact sequence

$$1 \longrightarrow \bar{k}^* \longrightarrow \mathrm{GL}_n(\bar{k}) \longrightarrow \mathrm{PGL}_n(\bar{k}) \longrightarrow 1$$

of (non-abelian) Γ-groups, we get the cohomology class $[A]$.

Actually, we will not go all the way but compare the cohomology class of A with the cup-product in the left-hand group $H^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big)$. In order to do that we have to find a pre-image of the cup-product.

Moreover we are not working with the classes $[L, C]$ and $[K, D]$ but—and this is equivalent because of (2.12) and the remark before (3.18)—with the more explicit $[h_{(L,\rho_L)}] \in H^1(\Gamma, \mathcal{K}_{(K,L)}/\mu_n)$ and $[h_{(K,\rho_K)}] \in H^1(\Gamma, \mathcal{K}_{(L,K)}/\mu_n)$ constructed in §2, 2.

2. Cocycles Associated to a Twisted Cyclic Algebra

For our twisted cyclic k-algebra (A, L, K) choose an isomorphism α: $\bar{A} \xrightarrow{\sim} \bar{A}_0$ of $\bar{k}$-algebras as in (3.3). We adopt the notations of (4.11) and set again $\pi_0 := (1\ 2\ \ldots\ n) \in S_n = S(M_{L_0})$. Let $Y := \alpha^{-1}(Y_0) \in \mathcal{K}_{(K,L)}$ and $e := \alpha^{-1}(E_{nn}) \in M_L$.
Then define $\pi := \rho_L([Y]) \in C$. Since Y and Y_0 have order n the cyclic group C is generated by π.

(5.3) Lemma. *The morphism*

$$\alpha_*\colon S(M_L) \longrightarrow S(M_{L_0}) = S_n$$

maps π to π_0.

Proof: Let $i = 1, \ldots, n$, then

$$\begin{aligned} \alpha_*(\pi)^i(E_{nn}) &= \alpha\big(\pi^i(e)\big) \\ &= \alpha(Y^i e Y^i) \\ &= Y_0^i E_{nn} Y_0^{-i} \\ &= E_{ii}\ . \end{aligned}$$

This implies our claim. □

Now we want to describe the cohomology class in $H^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big)$ assigned to the algebra A, which is mapped to $[A]$ by the morphism δ: $H^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big) \longrightarrow H^2(\Gamma, \bar{k}^*)$ mentioned above.

§ 5. A cohomological description of twisted cyclic algebras

We have done this already in §4, 2.: The cohomology class is given by

$$[X_\gamma \bmod \bar{k}^*] \in H^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big) \ ,$$

where X_γ is the cocycle we got in (4.8). Now (4.6) tells us that we can write

$$X_\gamma \ = \ X_0(\xi_\gamma) \cdot E_{\tilde{\gamma}} \ ,$$

where $\xi_\gamma \in \mu_n$ for every $\gamma \in \Gamma$. Let us denote the pre-image of $X_0(\xi_\gamma)$ via α by

$$X(\xi_\gamma) := \alpha^{-1}\big(X_0(\xi_\gamma)\big) \in \mathcal{K}_{(L,K)} \ .$$

For the proof we want to write $\mathrm{PGL}_n(\bar{k})$ in a different way: Define the k-vector space V to be

$$V := \bigoplus_{e' \in M_L} k \cdot e'$$

and $\bar{V} := V \otimes_k \bar{k}$ with the canonical Γ-action: Γ does not permute the components. So the linear map

$$\begin{aligned} \beta\colon \bar{k}^n \ &\longrightarrow \ \bar{V} \\ e_i \ &\longmapsto \ 1 \cdot \pi^i(e) \end{aligned}$$

for $i = 1, \cdots, n$, is an isomorphism of Γ-modules and it induces an isomorphism

$$\beta_*\colon \mathrm{PGL}_n(\bar{k}) = \big(\mathrm{GL}_n(k) \otimes_k \bar{k}\big)/\bar{k}^* \ \xrightarrow{\sim} \ \mathrm{PGL}(\bar{V}) = \big(\mathrm{GL}(V) \otimes_k \bar{k}\big)/\bar{k}^* \ .$$

of Γ-groups.
Let now $[q_\gamma \bmod \bar{k}^*]$ denote the image of $[X_\gamma \bmod \bar{k}^*]$ under the induced isomorphism

$$\beta_*\colon H^1\big(\Gamma, \mathrm{PGL}_n(\bar{k})\big) \ \xrightarrow{\sim} \ H^1\big(\Gamma, \mathrm{PGL}(\bar{V})\big) \ ,$$

i.e., $q_\gamma \in \mathrm{GL}(\bar{V})$ is some automorphism of $\bar{V}$ for every $\gamma \in \Gamma$.
In order to describe q_γ better let us make some conventions on notations:

(5.4) Notation. *If $e', e'' \in M_L$ are some primitive idempotents of $\bar{L}$, then there a unique $c \in C$ such that $e'' = c(e')$. We will write*

$$\frac{e''}{e'} := c \ .$$

Furthermore, if $c = \pi^\nu$ for some $\bar{\nu} \in \mathbb{Z}/n\mathbb{Z}$, then we will write

$$\log_\pi(c) := \bar{\nu} \ .$$

(5.5) Lemma. *A representative q_γ of the class $[q_\gamma \bmod \bar{k}^*] \in H^1\big(\Gamma, \mathrm{PGL}(\bar{V})\big)$ is given by*

$$\begin{aligned} q_\gamma\colon \bigoplus_{e' \in M_L} \bar{k} \cdot e' \ &\longrightarrow \ \bigoplus_{e' \in M_L} \bar{k} \cdot e' \\ e' \ &\longmapsto \ \xi_\gamma^{\log_\pi(\frac{\gamma(e')}{e})} \cdot \gamma(e') \ , \end{aligned}$$

where $\gamma(e')$ is an abbreviation for $(\mathrm{id}_A \otimes \gamma)(e') = \varphi_L(\gamma)(e')$, which we will use in the following in connection with the action on the idempotents; cf. (4.9).

Proof: We denote the linear morphism defined in the lemma by q'_γ. We have to show for $\gamma \in \Gamma$,

$$\beta_*^{-1}(q'_\gamma) \equiv D_\gamma E_{\tilde{\gamma}} \pmod{\bar{k}^*} ,$$

and we will show

$$q'_\gamma\big(\beta(e_i)\big) = \beta\big(D_\gamma E_{\tilde{\gamma}}(e_i)\big)$$

for $i = 1, \dots, n$, and e_i is still the i-th basis vector of $\bar{k}^n$.
First we claim: $\tilde{\gamma}(i) = \log_\pi(\frac{\gamma\pi^i(e)}{e})$.
Since α maps e to $E_{nn} \in M_{L_0}$ or—equivalently in our convention of identifying M_{L_0} with the set $\{1, \dots, n\}$—to $n \in \{1, \dots, n\}$ and since $\alpha_*\colon S(M_L) \to S_n$ maps $\gamma\pi^i$ to $\tilde{\gamma}\pi_0^i$ we have

$$\alpha\big(\gamma\pi^i(e)\big) = \alpha_*(\gamma\pi^i)\alpha(e) = \tilde{\gamma}\pi_0^i(n) = \tilde{\gamma}(i) = \pi_0^{\tilde{\gamma}(i)}(n) = \alpha\big(\pi^{\tilde{\gamma}(i)}(e)\big) .$$

Hence $\gamma\pi^i(e) = \pi^{\tilde{\gamma}(i)}(e)$—the claim. Now

$$\begin{aligned}
\beta(D_\gamma E_{\tilde{\gamma}} e_i) &= \beta\big(X_0(\xi_\gamma) e_{\tilde{\gamma}(i)}\big) \\
&= \xi_\gamma^{\tilde{\gamma}(i)} \cdot \beta(e_{\tilde{\gamma}(i)}) \\
&= \xi_\gamma^{\tilde{\gamma}(i)} \cdot \pi^{\tilde{\gamma}(i)}(e) \\
&= \xi_\gamma^{\tilde{\gamma}(i)} \cdot \gamma\pi^i(e) \\
&= \xi_\gamma^{\tilde{\gamma}(i)} \cdot \gamma\big(\beta(e_i)\big) \\
&= q'_\gamma\big(\beta(e_i)\big) ,
\end{aligned}$$

since $\tilde{\gamma}(i) = \log_\pi(\frac{\gamma\pi^i(e)}{e}) = \log_\pi(\frac{\gamma\beta(e_i)}{e})$. □

(5.6) Remark. If—in the description of the map q_γ—one replaces the idempotent e by any other primitive idempotent, then one gets the same 1-cocycle in $\mathscr{Z}^1\big(\Gamma, \mathrm{PGL}(\bar{V})\big)$. If one changes π to some other generator of C one gets a different cocycle, but the new one still represents the same cohomology class.

3. The 1-Cocycles Associated to the Pairs (L, ρ_L) and (K, ρ_K)

We still keep the notations from above.
For the 1-cocycle $h_L := h_{(L,\rho_L)}$ which represents the cohomology class $[h_{(L,\rho_L)}] \in H^1(\Gamma, \mathcal{K}_{(K,L)}/\mu_n)$, constructed in §2, we know by (2.8) that it is given by the formula

$$(\mathrm{id}_A \otimes \gamma)(e) = \rho_L\big(h_L(\gamma)\big)(e)$$

for all $\gamma \in \Gamma$.

(5.7) Lemma. *A 1-cocycle $h_L\colon \Gamma \longrightarrow \mathcal{K}_{(K,L)}/\mu_n$ representing the class $[h_{(L,\rho_L)}]$ is given by*

$$h_L(\gamma) = \big(Y^{\log_\pi(\frac{\gamma(e)}{e})} \bmod \mu_n\big)$$

for all $\gamma \in \Gamma$.

Proof: We have to check the formula from above. It suffices to prove this formula after applying α to it, i.e., we have to prove

$$\alpha_*(\mathrm{id}_A \otimes \gamma)(\alpha e) \;=\; \rho_{L_0}(Y_0^{\log_\pi(\frac{\gamma(e)}{e})} \bmod \mu_n)(\alpha e) \;.$$

First we claim

$$\log_\pi(\frac{\gamma(e)}{e}) \;=\; \tilde{\gamma}(n) \;.$$

Let $\gamma(e) = \pi^i(e)$ for some $i = 1, \ldots, n$, then

$$\tilde{\gamma}(n) \;=\; \alpha_*\big(\gamma(e)\big) \;=\; \alpha_*\big(\pi^i(e)\big) \;=\; \pi_0^i(n) \;=\; i \;.$$

Now with (4.8)

$$\begin{aligned}
\alpha_*(\mathrm{id}_A \otimes \gamma)(\alpha e) \;&=\; \kappa_{X_\gamma} \circ (\mathrm{id}_{A_0} \otimes \gamma)(E_{nn}) \\
&=\; X_0(\xi_\gamma) E_{\tilde{\gamma}} E_{nn} E_{\tilde{\gamma}}^{-1} X_0(\xi_\gamma)^{-1} \\
&=\; X_0(\xi_\gamma) E_{\tilde{\gamma}(n),\tilde{\gamma}(n)} X_0(\xi_\gamma)^{-1} \\
&=\; E_{\tilde{\gamma}(n),\tilde{\gamma}(n)} \\
&=\; Y_0^{\tilde{\gamma}(n)} E_{nn} Y_0^{-\tilde{\gamma}(n)} \\
&=\; \rho_{L_0}(Y_0^{\tilde{\gamma}(n)} \bmod \mu_n)(E_{nn}) \;.
\end{aligned}$$

□

(5.8) Lemma. *The action of Γ on $Y = \alpha^{-1}(Y_0)$ can be described as follows:*

$$(\mathrm{id}_A \otimes \gamma)(Y) \;=\; (\xi_\gamma \cdot Y)^{\log_\pi(\frac{\gamma\pi(e)}{\gamma(e)})}$$

for all $\gamma \in \Gamma$.

Proof: Again the formula will be verified after we applied α.
Let $\varphi_L(\gamma)\pi\varphi_L(\gamma)^{-1} = \pi^i$ for some $i = 1, \ldots, n$, then $\tilde{\gamma}\pi_0\tilde{\gamma}^{-1} = \pi_0^i$ and $\gamma\pi(e) = \gamma\pi\gamma^{-1}(\gamma e) = \pi^i\gamma(e)$, hence $i = \log_\pi(\frac{\gamma\pi(e)}{\gamma(e)})$. Now since

$$X_0(\xi_\gamma) E_{\pi_0} X_0(\xi_\gamma)^{-1} \;=\; X_0(\xi_\gamma) Y_0 X_0(\xi_\gamma)^{-1} \;=\; \xi_\gamma Y_0$$

we have

$$\begin{aligned}
\alpha_*(\mathrm{id}_A \otimes \gamma)(Y_0) \;&=\; \kappa_{X_\gamma} \circ (\mathrm{id}_{A_0} \otimes \gamma) E_{\pi_0} \\
&=\; X_0(\xi_\gamma) E_{\tilde{\gamma}} E_{\pi_0} E_{\tilde{\gamma}}^{-1} X_0(\xi_\gamma)^{-1} \\
&=\; X_0(\xi_\gamma) E_{\tilde{\gamma}\pi_0\tilde{\gamma}^{-1}} X_0(\xi_\gamma)^{-1} \\
&=\; X_0(\xi_\gamma) E_{\pi_0^i} X_0(\xi_\gamma)^{-1} \\
&=\; X_0(\xi_\gamma) E_{\pi_0}^i X_0(\xi_\gamma)^{-1} \\
&=\; (\xi_\gamma Y_0)^i \;.
\end{aligned}$$

□

Like in the first case we can describe a 1-cocycle $h_K := h_{(K,\rho_K)}$ which represents the cohomology class $[h_{(K,\rho_K)}] \in H^1(\Gamma, \mathcal{K}_{(L,K)}/\mu_n)$ by the formula

$$(\mathrm{id}_A \otimes \gamma)(g) \;=\; \rho_K\big(h_K(\gamma)\big)(g)\ ,$$

where $g \in M_K$ is any primitive idempotent of $\bar{K}$.

Recall the isomorphism $\kappa_{Z_0}\colon \bar{L}_0 \xrightarrow{\sim} \bar{K}_0$ defined in the proof of (3.7). This induces a bijection $\kappa_{Z_0}\colon M_{L_0} \longrightarrow M_{K_0}$ and explicit computation yields

$$M_{K_0} \;=\; \left\{ \frac{1}{n} \sum_{\nu=0}^{n-1} \zeta^\nu Y_0^\nu : \zeta \in \mu_n \right\}\ .$$

We will choose for g the easiest case $\zeta = 1$, i.e., $g := \alpha^{-1}\big(\frac{1}{n}\sum_{\nu=0}^{n-1} Y_0^\nu\big) = \frac{1}{n}\sum_{\nu=0}^{n-1} Y^\nu$.

(5.9) Lemma. *A 1-cocycle $h_K\colon \Gamma \longrightarrow \mathcal{K}_{(L,K)}/\mu_n$ representing the class $[h_{(K,\rho_K)}]$ is given by*

$$h_K(\gamma) \;=\; \big(X(\xi_\gamma) \bmod \mu_n\big)$$

for all $\gamma \in \Gamma$.

Proof: We have $X(\xi_\gamma) Y X(\xi_\gamma)^{-1} = \xi_\gamma Y$ and therefore

$$\begin{aligned}
(\mathrm{id}_A \otimes \gamma)(g) \;&=\; (\mathrm{id}_A \otimes \gamma)\big(\frac{1}{n}\sum_{\nu=0}^{n-1} Y^\nu\big) \\
&=\; \frac{1}{n}\sum_{\nu=0}^{n-1} (\mathrm{id}_A \otimes \gamma) Y^\nu \\
&=\; \frac{1}{n}\sum_{\nu=0}^{n-1} (\xi_\gamma \cdot Y)^{\nu \log_\pi(\frac{\gamma\pi(e)}{\gamma(e)})} \\
&=\; \frac{1}{n}\sum_{\nu=0}^{n-1} (\xi_\gamma \cdot Y)^{\nu} \\
&=\; \frac{1}{n}\sum_{\nu=0}^{n-1} \big(X(\xi_\gamma) Y X(\xi_\gamma)^{-1}\big)^{\nu} \\
&=\; X(\xi_\gamma) g X(\xi_\gamma)^{-1} \\
&=\; \rho_K\big(X(\xi_\gamma) \bmod \mu_n\big)(g)\ .
\end{aligned}$$

Note that

$$i := \log_\pi(\frac{\gamma\pi(e)}{\gamma(e)}) \;=\; \log_\pi(\frac{\gamma\pi\gamma^{-1}(e)}{e}) \in (\mathbb{Z}/n\mathbb{Z})^*\ ,$$

since $\gamma\pi\gamma^{-1} = \pi^i$ has order n. □

4. Proof of the Theorem

We now want to prove the Theorem, i.e., the equation

$$\mathfrak{c}\big([h_L]\cup[h_K]\big) \;=\; -[A]\ .$$

The cohomology class

$$[h_L]\cup[h_K]\in H^2(\Gamma,\mathcal{K}_{(K,L)}/\mu_n\otimes_{\mathbb{Z}}\mathcal{K}_{(L,K)}/\mu_n)$$

has the 2-cocycle $b_{\sigma,\tau}:=h_L(\sigma)\otimes(\mathrm{id}_A\otimes\sigma)h_K(\tau)$ as a representative.
Because of the anticommutativity of the cup-product of one-dimensional cohomology classes we will actually show

$$(\mathfrak{c}\circ\mathrm{switch})([h_K]\cup[h_L]) \;=\; [A]\ .$$

A 2-cocycle which represents the left side is then

$$\begin{aligned} a_{\sigma,\tau} \;&=\; \mathfrak{c}\big(\big((\mathrm{id}_A\otimes\sigma)h_L(\tau)\big)\otimes h_K(\sigma)\big)\\ &=\; \widehat{h_K(\sigma)}\cdot(\mathrm{id}_A\otimes\sigma)\big(\widehat{h_L(\tau)}\big)\cdot\widehat{h_K(\sigma)}^{\,-1}\cdot(\mathrm{id}_A\otimes\sigma)\big(\widehat{h_L(\tau)}\big)^{-1}\in\mu_n\ , \end{aligned}$$

Where $\widehat{h_K(\sigma)}$ and $\widehat{h_L(\tau)}$ are representatives of $h_K(\sigma)$ and $h_L(\tau)$ respectively. In order to compare $[a_{\sigma,\tau}]\in H^2(\Gamma,\bar{k}^*)$ with $[q_\gamma \bmod \bar{k}^*]\in H^1\big(\Gamma,\mathrm{PGL}(\bar{V})\big)$ we first take a pre-image of $[a_{\sigma,\tau}]$ under the composition

$$H^1\big(\Gamma,\mathrm{PGL}(\bar{V})\big)\ \xrightarrow{\beta_*^{-1}}\ H^1\big(\Gamma,\mathrm{PGL}_n(\bar{k}^*)\big)\ \xrightarrow{\ \delta\ }\ H^2(\Gamma,\bar{k}^*)\ .$$

(5.10) Lemma. *A pre-image $[p_\gamma \bmod \bar{k}^*]\in H^1\big(\Gamma,\mathrm{PGL}(\bar{V})\big)$ of $[a_{\sigma,\tau}]$ under $\delta\circ\beta_*^{-1}$ is given by*

$$\begin{aligned} p_\gamma\colon \bigoplus_{e'\in M_L}\bar{k}e' \;&\longrightarrow\; \bigoplus_{e'\in M_L}\bar{k}e'\\ \tau(e)\;&\longmapsto\; a_{\gamma,\tau}\cdot\gamma\tau(e) \end{aligned}$$

for $\tau\in\Gamma$.

(5.11) Remark. p_γ is well defined:
If for two elements $\tau,\tau'\in\Gamma$ we suppose $\tau(e)=\tau'(e)$, then $a_{\gamma,\tau}=a_{\gamma,\tau'}$, since the assumption implies $(\mathrm{id}_A\otimes\tau)(e)=(\mathrm{id}_A\otimes\tau')(e)$ and thus $h_L(\tau)=h_L(\tau')$, by (2.8).
Moreover $M_L=\{\tau(e):\tau\in\Gamma\}$ since in (5.1) we assumed that Γ acts transitively on the set M_L of the primitive idempotents of $\bar{L}$.

Proof: (of (5.10)). We have to show that $a_{\sigma,\tau}$ is cohomologous to $p_\sigma\circ{}^\sigma p_\tau\circ p_{\sigma\tau}^{-1}$. In fact we will show that they are equal: Let $\sigma,\tau,\omega\in\Gamma$, then

$$\begin{aligned} p_\sigma\circ{}^\sigma p_\tau\big(\omega(e)\big) \;&=\; p_\sigma\big(\sigma(a_{\tau,\omega})\cdot(\tau\omega)(e)\big)\\ &=\; a_{\sigma,\tau\omega}\cdot\sigma(a_{\tau,\omega})\cdot(\sigma\tau\omega)(e)\\ &=\; a_{\sigma,\tau}\cdot a_{\sigma\tau,\omega}\cdot(\sigma\tau)\big(\omega(e)\big)\\ &=\; a_{\sigma,\tau}\cdot p_{\sigma\tau}\big(\omega(e)\big)\ . \end{aligned}$$

In the third equality we used the cocycle property of $a_{\sigma,\tau}$. □

(5.12) Lemma. *For any $\sigma, \tau \in \Gamma$ we have the formula*

$$\log_\pi\left(\frac{\tau(e)}{e}\right) \cdot \log_\pi\left(\frac{\sigma\pi(e)}{\sigma(e)}\right) \;=\; \log_\pi\left(\frac{\sigma\tau(e)}{\sigma(e)}\right) .$$

Proof: Let $\varphi_L(\sigma)\pi\varphi_L(\sigma)^{-1} = \pi^i$, i.e., $\log_\pi(\frac{\sigma\pi(e)}{\sigma(e)}) = i$ and set $j := \log_\pi(\frac{\tau(e)}{e})$. Then $\tau(e) = \pi^j(e)$ and we get $\sigma\tau(e) = \sigma\pi^j(e) = \pi^{ij}\sigma(e)$. □

We come to the proof of our theorem:

Proof: (of (5.1)). Now what remains to show is

$$[q_\gamma \bmod \bar{k}^*] \;=\; [p_\gamma \bmod \bar{k}^*] \in H^1\big(\Gamma, \mathrm{PGL}(\bar{V})\big) .$$

We will show for every $\gamma \in \Gamma$,

$$\xi_\gamma^{\log_\pi(\frac{e}{\gamma(e)})} \cdot q_\gamma = p_\gamma$$

for the representatives from above. Let $\gamma, \tau \in \Gamma$, then

$$\xi_\gamma^{\log_\pi(\frac{e}{\gamma(e)})} \cdot q_\gamma\big(\tau(e)\big) \;=\; \xi_\gamma^{\log_\pi(\frac{e}{\gamma(e)})} \cdot \xi_\gamma^{\log_\pi(\frac{\gamma\tau(e)}{e})} \cdot \gamma\tau(e) \;=\; \xi_\gamma^{\log_\pi(\frac{\gamma\tau(e)}{\gamma(e)})} \cdot \gamma\tau(e)$$

by (5.5). And

$$p_\gamma\big(\tau(e)\big) \;=\; a_{\gamma,\tau} \cdot \gamma\tau(e) ,$$

where

$$\begin{aligned} a_{\gamma,\tau} \;&=\; \widehat{h_K(\gamma)} \cdot (\mathrm{id}_A \otimes\gamma)\big(\widehat{h_L(\tau)}\big) \cdot \widehat{h_K(\gamma)}^{-1} \cdot (\mathrm{id}_A \otimes\gamma)\big(\widehat{h_L(\tau)}\big)^{-1} \\ &=\; X(\xi_\gamma) \cdot Y^{\log_\pi(\frac{\gamma\tau(e)}{\gamma(e)})} \cdot X(\xi_\gamma)^{-1} \cdot Y^{-\log_\pi(\frac{\gamma\tau(e)}{\gamma(e)})} \\ &=\; \xi_\gamma^{\log_\pi(\frac{\gamma\tau(e)}{\gamma(e)})} , \end{aligned}$$

where for the representatives $\widehat{h_K(\gamma)}$ and $\widehat{h_L(\tau)}$ we used $X(\xi_\gamma)$ and $Y^{\log_\pi(\frac{\tau(e)}{e})}$ respectively. Further we used in the second equation

$$\begin{aligned} (\mathrm{id}_A \otimes\gamma)\big(\widehat{h_L(\tau)}\big) \;&=\; (\mathrm{id}_A \otimes\gamma)(Y^{\log_\pi(\frac{\tau(e)}{e})}) \\ &=\; (\xi_\gamma \cdot Y)^{\log_\pi(\frac{\gamma\pi(e)}{\gamma(e)})\cdot\log_\pi(\frac{\tau(e)}{e})} \\ &=\; (\xi_\gamma \cdot Y)^{\log_\pi(\frac{\gamma\tau(e)}{\gamma(e)})} \\ &=\; Y^{\log_\pi(\frac{\gamma\tau(e)}{\gamma(e)})} . \end{aligned}$$

We are done. □

Chapter III

The Notion of Chain Equivalence

§ 6. Kummer Elements and Kummer Relation

In §3 we have seen that a twisted cyclic k-algebra (A, L, K) gives rise to elements $X \in \mathcal{K}_{(L,K)}$ and $Y \in \mathcal{K}_{(K,L)}$ which are in a—what we are going to call—*Kummer relation*, i.e., $XY = \zeta YX$, where $\zeta \in \mu_n = \mu_n(\bar{k})$ is a primitive n-th root of unity. Since these elements generate $\bar{L}$ and $\bar{K}$, they already give rise to our twisted cyclic decomposition of A. We are going to use these *Kummer elements* in order to describe twisted cyclic decompositions.

In this section we fix a field k and a positive integer $n \geq 2$ which is prime to the characteristic of k, and ζ denotes a primitive n-th root of unity in $\bar{k}$. Let A be a central simple k-algebra of degree n.

1. Kummer Elements

For every element $X \in A$ we have its *reduced characteristic polynomial*

$$\mathrm{Prd}(X,t) \;=\; t^n - \mathrm{Srd}_1(X)t^{n-1} + \cdots + (-1)^n \,\mathrm{Srd}_n(X) \in k[t] \;,$$

especially the *reduced trace* $\mathrm{Trd}(X) = \mathrm{Srd}_1(X) \in k$ and the *reduced norm* $\mathrm{Nrd}(X) = \mathrm{Srd}_n(X) \in k$.
If A is a matrix algebra, then $\mathrm{Nrd}(X)$ and $\mathrm{Trd}(X)$ are just *determinant* and *trace* of the matrix X. (Cf. [SchQH], chap. 8, §8, p. 296, or [BI]).
The condition $\mathrm{Nrd}(X) \neq 0$ is equivalent to $X \in A^*$.
If $A = \mathrm{M}_n(k)$, then $\mathrm{Srd}_\nu(X)$ is a homogeneous polynomial of degree ν in the n^2 entries of the matrix X. The coefficients lie in $\mathbb{Z}$ (or better: in the image of $\mathbb{Z}$ in k).

(6.1) Definition. *A* **Kummer Element** *in A is an element $X \in A$ such that*

$$\mathrm{Prd}(X,t) \;=\; t^n - a \;,$$

where $a \in k^*$; or equivalently $X \in A^*$, $\mathrm{Srd}_\nu(X) = 0$ for all $\nu = 1, \ldots, n-1$.

(6.2) Notation. *We denote the set of all Kummer elements of A by*

$$\mathcal{W}(A) \;:=\; \{X \in A^* : \mathrm{Prd}(X,t) = t^n - a\} \;.$$

Since $\mathcal{W}(A)$ is stable under scaling by elements of k^*, we also call the "projective version"

$$\mathrm{W}(A) \;:=\; \mathcal{W}(A)/k^* \;=\; \{[X] \in A^*/k^* : X \in \mathcal{W}(A)\}$$

the **set of Kummer elements** *or more accurate* **Kummer lines**.

(6.3) Example. In $A = \mathrm{M}_n(\bar{k})$, we have the Kummer elements $X_0(\zeta)$, where ζ is any primitive n-th root of unity, and Y_0:

$$\mathrm{Prd}\big(X_0(\zeta), t\big) \;=\; \mathrm{Prd}(Y_0, t) \;=\; t^n - 1 \;.$$

In fact, we have

$$\mathrm{W}\big(\mathrm{M}_n(\bar{k})\big) \;=\; \big\{[GX_0(\zeta)G^{-1}] : G \in \mathrm{GL}_n(\bar{k})\big\} \;,$$

since an $X \in \mathcal{W}(A)$, scaled such that $\det(X) = 1$, has eigenvalues $\mathrm{EigVal}(X) = \mu_n(\bar{k})$ and therefore is similar to $X_0(\zeta)$ or Y_0.

(6.4) Remark. For a Kummer element $X \in \mathcal{W}(A)$ the reduced characteristic polynomial $\mathrm{Prd}(X, t) = t^n - a$ has n distinct roots. Hence $\mathrm{Prd}(X, t)$ is also the minimal polynomial of X.

(6.5) Lemma. *We assume that $(n!)$ is prime to the characteristic of k. For any $X \in A$ the following conditions are equivalent:*

(i) $\mathrm{Prd}(X, t) = t^n - a$,

(ii) $\mathrm{Trd}(X) = \mathrm{Trd}(X^2) = \ldots = \mathrm{Trd}(X^{n-1}) = 0$.

Proof: We may assume $k = \bar{k}$ and $A = \mathrm{M}_n(\bar{k})$. Furthermore we can assume that X is a triangular matrix with the diagonal elements $\alpha_1, \ldots, \alpha_n \in k$. Then (i) is equivalent to

$$\sigma_\nu(\alpha_1, \ldots, \alpha_n) \;=\; 0 \quad \text{for all } \nu = 1, \ldots, n-1 \;,$$

where $\sigma_\nu(T_1, \ldots, T_n) \in \mathbb{Z}[T_1, \ldots, T_n]$ is the *elementary symmetric polynomial* of degree ν. The condition (ii) is equivalent to

$$\tau_\nu(\alpha_1, \ldots, \alpha_n) \;=\; 0 \quad \text{for all } \nu = 1, \ldots, n-1 \;,$$

where $\tau_\nu(T_1, \ldots, T_n) := T_1^\nu + \cdots + T_n^\nu \in \mathbb{Z}[T_1, \ldots, T_n]$.
The equivalence of these conditions immediately follows from Newton's formula (cf. [WaAL],§33, Aufgabe 1)

$$\tau_\nu - \tau_{\nu-1}\sigma_1 + \tau_{\nu-2}\sigma_2 - \cdots + (-1)^{\nu-1}\tau_1\sigma_{\nu-1} + (-1)^\nu \nu\sigma_\nu \;=\; 0$$

for $1 \le \nu \le n$, using the fact that $\nu = 1, \ldots, n-1$ is invertible in k. □

(6.6) Proposition. *If $n = 2, 3$, then $\mathcal{W}(A) \neq \emptyset$.*

Proof: $n = 2$: We may assume A is a division algebra. (Otherwise $A \cong \mathrm{M}_2(k)$ and Y_0 is a Kummer element.) Take any $X' \in A - k \cdot 1_A$ and set

$$X \;:=\; X' - \frac{\mathrm{Trd}(X')}{2} \cdot 1_A \;.$$

Then $X \in \mathcal{W}(A)$, since $\mathrm{Trd}(X) = 0$.
$n = 3$: Cf. (19.2) in [BI]. □

(6.7) Lemma. *If $X, Y \in \mathrm{GL}_n(\bar{k})$ are invertible matrices such that $XY = \zeta YX$, then there are $\alpha, \beta \in \bar{k}^*$ such that we have for the eigenvalues of X and Y:*

$$\mathrm{EigVal}(X) \;=\; \alpha \cdot \mu_n \quad \text{and} \quad \mathrm{EigVal}(Y) \;=\; \beta \cdot \mu_n \;,$$

and $\alpha^n = (-1)^{n-1}\det(X)$, $\beta^n = (-1)^{n-1}\det(Y)$.

Proof: From $Y^{-1}XY = \zeta X$ we see

$$\zeta \cdot \mathrm{EigVal}(X) \;=\; \mathrm{EigVal}(\zeta X) \;=\; \mathrm{EigVal}(Y^{-1}XY) \;=\; \mathrm{EigVal}(X) \;.$$

Let $\alpha \in \mathrm{EigVal}(X) - \{0\}$, then $\zeta\alpha$, $\zeta^2\alpha, \ldots \in \mathrm{EigVal}(X)$. We have

$$\begin{aligned} \det(X) \;&=\; \prod_{\xi \in \mu_n} \xi\alpha \\ &=\; \Big(\prod_{\xi \in \mu_n} \xi\Big)\alpha^n \\ &=\; (-1)^{n-1}\alpha^n \;. \end{aligned}$$

The same holds for Y. □

(6.8) Proposition. *If $X, Y \in A^*$ are invertible elements such that $XY = \zeta YX$, then $X, Y \in \mathcal{W}(A)$ are Kummer elements.*

Proof: Since the reduced characteristic polynomial remains stable under base field extension we may assume that $k = \bar{k}$ and $A = \mathrm{M}_n(\bar{k})$. Because of (6.7) there is an $\alpha \in \bar{k}^*$ such that X is similar to $\alpha X_0(\zeta) \in \mathcal{W}(A)$. The same holds for Y. □

(6.9) Corollary. *If $X, Y \in A^*$ are invertible elements such that $XY = \zeta YX$, then also $XY \in \mathcal{W}(A)$ is a Kummer element.*

Proof: $XY = \zeta YX$ implies $(XY)Y = \zeta Y(XY)$. □

(6.10) Lemma. *If $X, Y \in \mathcal{W}(A)$ such that $XY = \zeta YX$, then for $X', Y' \in A$:*

$$\begin{aligned} XY' \;=\; \zeta Y'X \quad &\Longleftrightarrow \quad Y' \in k[X]\cdot Y \;=\; Y \cdot k[X] \\ X'Y \;=\; \zeta YX' \quad &\Longleftrightarrow \quad X' \in k[Y]\cdot X \;=\; X \cdot k[Y] \end{aligned}$$

Proof: The direction "⇐" is clear since the elements of $k[X]$ commute with X and the elements of $k[Y]$ commute with Y.
"⇒": Let $XY' = \zeta Y'X$, then

$$Y^{-1}Y'X \;=\; \zeta Y^{-1}XY' \;=\; XY^{-1}Y' \;,$$

i.e., $Y^{-1}Y'$ commutes with X. Therefore $Y^{-1}Y' \in k[X]$, since $k[X]$ is a maximal commutative subalgebra of A.—Analogous for X'. □

2. Description of Twisted Cyclic Algebras via Elements in Kummer Relation

We start with an important technical lemma:

(6.11) Lemma. *Let $X, Y \in \mathrm{GL}_n(k)$ such that $\det(X) = \det(Y) = (-1)^{n-1}$ and $XY = \zeta YX$. Then the pair (X, Y) is similar to $\big(X_0(\zeta), Y_0\big)$, i.e., there exists a matrix $G \in \mathrm{GL}_n(k)$ such that*

$$GXG^{-1} \;=\; X_0(\zeta) \quad \text{and} \quad GYG^{-1} \;=\; Y_0 \;.$$

Proof: Because of $\det(X) = \det(Y) = (-1)^{n-1}$ and (6.7) we know $\mathrm{EigVal}(X) = \mathrm{EigVal}(Y) = \mu_n$. Therefore there exists a $G_1 \in \mathrm{GL}_n(k)$ such that $G_1 X G_1^{-1} = X_0(\zeta)$.— Note that $\zeta \in k$ because $\zeta = XYX^{-1}Y^{-1}$. Since conjugation by G_1 does not change our assumption, we may for the proof assume that actually $X = X_0(\zeta)$. Since

$$XY \;=\; \zeta YX \quad \text{and} \quad XY_0 \;=\; \zeta Y_0 X \;,$$

we know by (6.10) that $Y^{-1}Y_0 = D \in k[X_0(\zeta)] = L_0$ is a diagonal matrix. Let $D = \mathrm{diag}(d_1, \ldots, d_n)$ for $d_1, \ldots, d_n \in k^*$, then we know, since $\det(Y^{-1}Y_0) = 1$, that $d_1 \cdots d_n = 1$. Define (we now use the "Hilbert's Theorem 90-trick")

$$G \;:=\; \mathrm{diag}(1, d_1, d_1 d_2, \ldots, d_1 \cdots d_{n-1}) \;.$$

Then

$$Y_0^{-1} G Y_0 \;=\; \mathrm{diag}(d_1, d_1 d_2, \ldots, d_1 \cdots d_n) \;,$$

hence

$$G^{-1}(Y_0^{-1} G Y_0) \;=\; \mathrm{diag}(d_1, d_2, \ldots, d_n) \;=\; Y^{-1} Y_0 \;,$$

i.e.,

$$GYG^{-1} \;=\; Y_0 \;.$$

But since $G \in L_0$ is diagonal, we still have $GXG^{-1} = X = X_0(\zeta)$ and we are done. □

As an immediate consequence we get:

(6.12) Corollary. *Let $X, Y \in \mathrm{GL}_n(k)$ with $XY = \zeta YX$, then there exists a $G \in \mathrm{GL}_n(\bar{k})$ and $\alpha, \beta \in \bar{k}^*$ such that*

$$GXG^{-1} \;=\; \alpha X_0(\zeta) \quad \text{and} \quad GXG^{-1} \;=\; \beta Y_0 \;.$$

In this case $\alpha^n = (-1)^{n-1}\det(X), \beta^n = (-1)^{n-1}\det(Y)$.

(6.13) Definition. *Let A be a central simple k-algebra of degree n and $X, Y \in A^*$. Then we say (X, Y) is a ζ-**pair**, or X and Y are in (ζ-)**Kummer relation** if*

$$XY \;=\; \zeta YX \;,$$

where ζ is a primitive n-th root of unity. We will also denote this fact by the symbol

$$X \xrightarrow{\zeta} Y \;.$$

(6.14) Proposition. *Let A be a central simple k-algebra of degree n and (X, Y) a ζ-pair in A. Then X and Y generate A, we even have*

$$A \;=\; \bigoplus_{i,j=0,\dots,n-1} k \cdot X^i Y^j \;.$$

If there are elements $\alpha, \beta \in k^*$ in the ground field such that $\alpha^n = (-1)^{n-1}\mathrm{Nrd}(X) = X^n$ and $\beta^n = (-1)^{n-1}\mathrm{Nrd}(Y) = Y^n$, then the morphism of k-algebras, given by

$$\begin{aligned} A &\xrightarrow{\sim} A_0 \\ X^i Y^j &\longmapsto \big(\alpha X_0(\zeta)\big)^i (\beta Y_0)^j \end{aligned}$$

for i, $j = 1, \dots, n-1$, is an isomorphism.

Proof: There is an isomorphism of $\bar{k}$-algebras

$$\bar{A} \;=\; A \otimes_k \bar{k} \;\xrightarrow{\sim}\; \bar{A}_0 \;= \mathrm{M}_n(\bar{k}) \;,$$

which maps X to $\alpha X_0(\zeta)$ and Y to βY_0: Take any isomorphism $\varphi\colon \bar{A} \to \bar{A}_0$. Since (X, Y) is a ζ-pair $\big(\varphi(X), \varphi(Y)\big)$ is also one. Now, take the $G \in \mathrm{GL}_n(\bar{k})$ of (6.12) and compose φ with κ_G. Obviously

$$\bar{A}_0 \;=\; \bigoplus_{i,j=0,\dots,n-1} \bar{k} \cdot X_0(\zeta)^i Y_0^j \;=\; \bigoplus_{i,j=0,\dots,n-1} \bar{k} \cdot \big(\alpha X_0(\zeta)\big)^i \big(\beta Y_0\big)^j \;,$$

therefore

$$\bar{A} \;=\; \bigoplus_{i,j=0,\dots,n-1} \bar{k} \cdot X^i Y^j \;.$$

Now, in order to show the first part of the proposition, it is enough to prove it after the (faithfully flat) base extension $\bar{k}|k$; what we have done above.
The second part also follows, since the isomorphism $\kappa_G \circ \varphi$ is already defined over k. □

Now we can characterize twisted cyclic algebras by ζ-pairs:

(6.15) Proposition. *Let A be a central simple k-algebra of degree n and $L, K \subseteq A$ two commutative k-subalgebras of degree n. Then the following conditions are equivalent:*

(i) *(L, K) is a twisted cyclic decomposition of A,*

(ii) *There exist $X \in \bar{L}$ and $Y \in \bar{K}$ such that (X, Y) is a ζ-pair.*

In this case

$$\bar{L} \;=\; \bar{k}[X] \quad \text{and} \quad \bar{K} \;=\; \bar{k}[Y] \;.$$

and

$$\begin{aligned} X \in \mathcal{K}_{(L,K)} \;&=\; \{\zeta^i X^j : i, j = 0, \dots, n-1\} \\ Y \in \mathcal{K}_{(K,L)} \;&=\; \{\zeta^i Y^j : i, j = 0, \dots, n-1\} \;. \end{aligned}$$

Proof: Let (A, L, K) be a twisted cyclic k-algebra and $\alpha\colon \bar{A} \xrightarrow{\sim} \bar{A}_0$ a Γ-isomorphism as in the definition (3.3). Then take $X := \alpha^{-1}\big(X_0(\zeta)\big)$ and $Y := \alpha^{-1}(Y_0)$.
The other direction follows with the isomorphism of (6.14) in the case $k = \bar{k}$. □

In (6.6) we said something about the existence of Kummer elements. Now we ask for the existence of ζ-pairs.

(6.16) Proposition. *Assume that $\mu_n = \mu_n(\bar{k}) \subseteq k$. If A is a division algebra and $X \in \mathcal{W}(A)$ a Kummer element in A, then there exist Kummer elements $Y \in \mathcal{W}(A)$ such that (X, Y) is a ζ-pair.*

Proof: $k[X]$ is a commutative subalgebra of A of dimension n. Therefore it is a field, in particular simple. The automorphism $k[X] \xrightarrow{\sim} k[X]$, $X \longmapsto \zeta^{-1}X$ can be extended by Skolem-Noether to an inner automorphism κ_Y for some $Y \in A^*$, i.e., we have $YXY^{-1} = \zeta^{-1}X$. □

3. Galois Action on Kummer Elements and Twisted Cyclic Decompositions

Let $k'|k$ be a Galois extension and A a central simple k-algebra. Then $G := \mathrm{Gal}(k'|k)$ acts on the central simple k'-algebra $A_{k'} = A \otimes_k k'$.
This action gives rise to actions on the set of Kummer elements and twisted cyclic decompositions.

(6.17) Remark. For $\sigma \in G$ and $X \in A_{k'}$ we have the identity

$$\mathrm{Prd}(\sigma X, t) \;=\; \sigma\,\mathrm{Prd}(X, t)\ ,$$

where σ acts on the coefficients of the polynomial. Therefore, if $X \in \mathcal{W}(A_{k'})$ is a Kummer element, then $\sigma X \in \mathcal{W}(A_{k'})$ is also one. The same holds for $\mathrm{W}(A_{k'})$.

(6.18) Proposition. *The map*

$$\mathcal{W}(A) \;\longrightarrow\; \mathcal{W}(A_{k'})\ ,\ X \;\longmapsto\; X$$

has Galois descent, i.e., it induces the bijection

$$\mathcal{W}(A) \;\xrightarrow{\sim}\; \mathcal{W}(A_{k'})^G\ .$$

Proof: This follows from the Galois descent of the map $A \longrightarrow A_{k'}$. □

The Galois group G acts in the following way on the set of twisted cyclic decompositions of $A_{k'}$.

(6.19) Lemma. *Let (L', K') be a twisted cyclic decomposition of the central simple k'-algebra $A_{k'}$. Then for $\sigma \in G$, the pair $(\sigma L', \sigma K')$ is also a twisted cyclic decomposition of $A_{k'}$.*

Proof: Because of (6.15) there are $X \in \bar{L}' = L' \otimes_{k'} \bar{k}$ and $Y \in \bar{K}' = K' \otimes_{k'} \bar{k}$ such that (X, Y) is a ζ-pair and $\bar{L}' = \bar{k}[X]$ and $\bar{K}' = \bar{k}[Y]$. But this implies that $(\sigma X, \sigma Y)$ is a $\sigma\zeta$-pair and $\overline{\sigma L'} = \bar{k}[\sigma X]$, $\overline{\sigma K'} = \bar{k}[\sigma Y]$. Again with (6.15) we are done. □

(6.20) Proposition. *The map*

$$\begin{aligned}\{\text{twisted cyclic decompositions of } A\} &\longrightarrow \{\text{twisted cyclic decompositions of } A_{k'}\}\\ (L,K) &\longmapsto (L\otimes_k k', K\otimes_k k')\end{aligned}$$

has Galois descent.

Proof: The map is obviously injective and well defined (cf. (3.4)). Let (L',K') be a decomposition which is invariant under G. Then G acts semilinear on L' and K'. Therefore we have for $L := L'^G$ and $K := K'^G$,

$$L' \;=\; L\otimes_k k' \quad\text{and}\quad K' \;=\; K\otimes_k k'\;;$$

cf. (18.1) in [BI]. □

4. Description of Split Twisted Cyclic Algebras

We will give a criterion for a triple (A,L,K) of k-algebras to be isomorphic to the standard one. This will be used to prove the last remark of (3.4).

(6.21) Lemma. *We assume $\mu_n \subseteq k$. Let (A,L,K) be a triple, where A is a k-algebra, L and K are commutative k-subalgebras of A. Then the condition*

$$(A,L,K) \;\cong\; (A_0,L_0,K_0)$$

is equivalent to the following set of two conditions:

(i) *$A\cong A_0$, $L\cong L_0$, $K\cong K_0$ as k-algebras;*

(ii) *One can number the primitive idempotents $\{e_1,\dots,e_n\}$ of L and $\{f_1,\dots,f_n\}$ of K in a way such that the elements $X := \zeta^1 e_1+\zeta^2 e_2+\cdots+\zeta^n e_n \in L$ and $Y := \zeta^1 f_1+\zeta^2 f_2+\cdots+\zeta^n f_n \in K$ are in a Kummer relation.*

Note that the point (i) implies that $L\cong k^n$ and $K\cong k^n$ and therefore they have n primitive idempotents.

Proof: If $(A,L,K)\cong(A_0,L_0,K_0)$, the point (i) is clear. The point (ii) follows, since it is true for the case $(A,L,K)=(A_0,L_0,K_0)$; this we can see putting together (3.9) and (3.19).
The other direction follows with (6.14): Since $X^n=Y^n=1$, we can set in this proposition $\alpha=\beta=1$, and that gives the isomorphism $(A,k[X],k[Y])\cong(A_0,L_0,K_0)$. But for dimension reasons the inclusions $k[X]\subseteq L$ and $k[Y]\subseteq K$ are actually equalities. □

(6.22) Proposition. *Let (A,L,K) be a triple, where A is a k-algebra, L and K are commutative k-subalgebras of A and $k'|k$ is an algebraic (not necessarily separable) field extension. Then we have the equivalence:*
(A,L,K) is a twisted cyclic k-algebra of degree n $\Longleftrightarrow$ $(A,L,K)_{k'}$ is a twisted cyclic k'-algebra of degree n.

Proof: The direction "⇒"is clear.
For the other direction we may assume that $k' = \tilde{k}$ is an algebraic closure of k.

Furthermore—because of (3.4)—we may assume that $k = \bar{k}$ is separably closed.
The separable closure of $\tilde{k}$ is of course $\tilde{k}$, therefore $(\tilde{A}, \tilde{L}, \tilde{K}) := (A, L, K)_{\tilde{k}}$ is isomorphic to $(\tilde{A}_0, \tilde{L}_0, \tilde{K}_0) := (A_0, L_0, K_0)_{\tilde{k}}$, i.e., $\tilde{A}$ is isomorphic to a matrix algebra. Thus A is a central simple k-algebra; and hence, A is already split, since k is its own separable closure. So $A \cong \mathrm{M}_n(k) = A_0$.
Since $\tilde{L}_0 \cong \tilde{k}^n$ and $\tilde{K}_0 \cong \tilde{k}^n$ are diagonalizable, the same holds for $\tilde{L}$ and $\tilde{K}$, i.e., $\tilde{L}$ and $\tilde{K}$ are separable $\tilde{k}$-algebras of degree n. Since

$$n \;=\; \mathrm{Hom}_{\tilde{k}}(\tilde{L}, \tilde{k}) \;=\; \mathrm{Hom}_k(L, \tilde{k}) \quad \text{and} \quad n \;=\; \mathrm{Hom}_{\tilde{k}}(\tilde{K}, \tilde{k}) \;=\; \mathrm{Hom}_k(K, \tilde{k}) \;,$$

L and K are separable k-algebras. And since k is separably closed, we get

$$L \;\cong\; k^n \;\cong\; L_0 \quad \text{and} \quad K \;\cong\; k^n \;\cong\; K_0 \;;$$

in other words: The primitive idempotents $e_1, \ldots, e_n$ of $\tilde{L}$ and $f_1, \ldots, f_n$ of $\tilde{K}$ already lie in L and K respectively. Now

$$L \;=\; k \cdot e_1 \oplus \cdots \oplus k \cdot e_n \quad \text{and} \quad K \;=\; k \cdot f_1 \oplus \cdots \oplus k \cdot f_n$$

as well as

$$\tilde{L} \;=\; \tilde{k} \cdot e_1 \oplus \cdots \oplus \tilde{k} \cdot e_n \quad \text{and} \quad \tilde{K} \;=\; \tilde{k} \cdot f_1 \oplus \cdots \oplus \tilde{k} \cdot f_n \;.$$

Since $(\tilde{A}, \tilde{L}, \tilde{K}) \cong (\tilde{A}_0, \tilde{L}_0, \tilde{K}_0)$, we may, by (6.21), assume that the elements $X := \zeta^1 e_1 + \zeta^2 e_2 + \cdots + \zeta^n e_n$ and $Y := \zeta^1 f_1 + \zeta^2 f_2 + \cdots + \zeta^n f_n$ are in a Kummer relation. But X and Y already lie in L and K respectively. Using the other direction of (6.21) we get the claim. □

§ 7. Chains of Twisted Cyclic Extensions

In this section we establish the first version of chains, give some elementary properties and classify these by virtue of certain "structure morphisms".
We fix a field k and positive integers $n \geq 2$ and ℓ such that n is prime to the characteristic of k. Let A be a central simple k-algebra of degree n.

1. Definition of Chains

(7.1) Definition. *A* k**-chain** *in* A *of length* ℓ *is an* $(\ell+1)$*-tuple* $(L_0, \ldots, L_\ell)$ *of separable commutative* k*-subalgebras of* A *such that* (L_i, L_{i+1}) *is a twisted cyclic decomposition of* A *for all* $i = 0, \ldots, \ell - 1$.

(7.2) Notation. *We denote the set of all* k*-chains in* A *of length* ℓ *by the expression*

$$\mathrm{Chain}_\ell(A) \ .$$

(7.3) Remark. If $k'|k$ is a field extension, then we have a natural injective map

$$\begin{aligned} \mathrm{Chain}_\ell(A) &\longrightarrow \mathrm{Chain}_\ell(A \otimes_k k') \\ (L_0, \ldots, L_\ell) &\longmapsto (L_0, \ldots, L_\ell)_{k'} \ , \end{aligned}$$

where $(L_0, \ldots, L_\ell)_{k'} := (L_0 \otimes_k k', \ldots, L_\ell \otimes_k k')$; cf. (3.4).

Furthermore if $k'|k$ is a Galois extension, then $\mathrm{Gal}(k'|k)$ acts on $\mathrm{Chain}_\ell(A \otimes_k k')$, in the way of (6.19). Analogously to (6.20) we have:

(7.4) Proposition. *If* $k'|k$ *is a Galois extension, then the map*

$$\mathrm{Chain}_\ell(A) \longrightarrow \mathrm{Chain}_\ell(A_{k'}) \ ,$$

has Galois descent.

2. Chains with Fixed Starting and End Points

We fix two separable commutative k-subalgebras $L, K \subseteq A$ of degree n.
Since we are interested in the question if two separable commutative subalgebras can be connected by chains, we make the following definition.

(7.5) Definition. *Let* $k'|k$ *be a field extension. A* k'**-chain** *in* A *from* L *to* K *of length* ℓ *is a* k'*-chain* $(L'_0, \ldots, L'_\ell) \in \mathrm{Chain}_\ell(A_{k'})$ *such that*

$$L'_0 \ = \ L_{k'} \quad \text{and} \quad L'_\ell \ = \ K_{k'} \ .$$

(7.6) Notation. *We make the following notations*

$$\mathrm{Chain}_\ell(L,K;A)_{k'} \;:=\; \{(L'_0,\dots,L'_\ell)\in \mathrm{Chain}_\ell(A_{k'}) : L'_0 = L_{k'}, L'_\ell = K_{k'}\}$$

and

$$\mathrm{Chain}_\ell(L,-;A)_{k'} \;:=\; \{(L'_0,\dots,L'_\ell)\in \mathrm{Chain}_\ell(A_{k'}) : L'_0 = L_{k'}\}\ .$$

If $k'=k$, we leave the index "k".

(7.7) Remark. Obviously

$$\mathrm{Chain}_\ell(L,K;A)_{k'} \;=\; \mathrm{Chain}_\ell(L_{k'},K_{k'};A_{k'})\ .$$

If $k'|k$ is a Galois extension, then $\mathrm{Gal}(k'|k)$ acts on this set, since the Galois action leaves $L_{k'}$ and $K_{k'}$ fixed. An easy consequence of (7.4) is:

(7.8) Proposition. *We have the natural injective map*

$$\begin{aligned}\mathrm{Chain}_\ell(L,K;A) &\longrightarrow \mathrm{Chain}_\ell(L,K;A)_{k'}\\ (L_0,\dots,L_\ell) &\longmapsto (L_0,\dots,L_\ell)_{k'}\ .\end{aligned}$$

If $k'|k$ is a Galois extension, then this map has Galois descent.

We remind that we wrote $\Gamma = \mathrm{Gal}(\bar{k}|k)$ for the absolute Galois group of k.
Let $\mathscr{C}_n$ be the *category of the Γ-modules C which are cyclic groups of order n*. Then we have on $\mathscr{C}_n$ the following involutionary endo-functor

$$\begin{aligned}T := \mathrm{Hom}_{\mathbb{Z}}(-,\mu_n)\colon \mathscr{C}_n &\longrightarrow \mathscr{C}_n\\ C &\longmapsto \mathrm{Hom}_{\mathbb{Z}}(C,\mu_n)\ ,\end{aligned}$$

where $\mu_n = \mu_n(\bar{k})$. The natural transformation $\varphi\colon \mathrm{id} \xrightarrow{\sim} T\circ T$ is given by

$$\begin{aligned}\varphi_C\colon C &\longrightarrow \mathrm{Hom}_{\mathbb{Z}}\big(\mathrm{Hom}_{\mathbb{Z}}(C,\mu_n),\mu_n\big)\\ c &\longmapsto \mathrm{ev}_c\ ,\end{aligned}$$

the evaluation morphism. The following is well known.

(7.9) Lemma. *For any $C, D\in\mathscr{C}_n$ we have the identity*

$$\mathrm{Isom}_\Gamma(C\otimes_{\mathbb{Z}} D,\mu_n) \;=\!=\; \mathrm{Isom}_\Gamma\big(C,T(D)\big)\ .$$

Let $(L_0,\dots,L_\ell)\in\mathrm{Chain}_\ell(A)$ be a k-chain, then (A,L_i,L_{i+1}) is twisted cyclic k-algebra for $i=0,\dots,\ell-1$.
This induces the twisted cyclic structures

$$C_i \;:=\; C_{(A,L_i,L_{i+1})} \quad \text{on } L_i$$

and

$$D_{i+1} \;:=\; D_{(A,L_i,L_{i+1})} \quad \text{on } L_{i+1}$$

and the isomorphism of Γ-modules

$$\mathfrak{c}_i \;:=\; \mathfrak{c}_{(A_i,L_i,L_{i+1})}\colon C_i\otimes_{\mathbb{Z}} D_{i+1} \;\xrightarrow{\sim}\; \mu_n = \mu_n(\bar{k})\ ;$$

cf. §3, 2.

(7.10) Definition. *A* **coherent chain** *in A is a chain $(L_0, \dots, L_\ell) \in \mathrm{Chain}_\ell(A)$ with*

$$C_i \;=\; D_i \quad \text{for all } i = 1, \dots, \ell - 1 \ .$$

(7.11) Notation. *We write for the set of coherent chains of length ℓ,*

$$\text{c-Chain}_\ell(A) \;:=\; \{(L_0, \dots, L_\ell) \in \mathrm{Chain}_\ell(A) : (L_0, \dots, L_\ell) \text{ is coherent}\}$$

and

$$\text{c-Chain}_\ell(L, K; A) \;:=\; \text{c-Chain}_\ell(A) \cap \mathrm{Chain}_\ell(K, L; A) \ ,$$

and analogously for all other notations of this kind.

If $(L_0, \dots, L_\ell) \in \text{c-Chain}_\ell(A)$ is a coherent chain, then we can compose the Γ-morphisms, given by (7.9):

$$T^i(\mathfrak{c}_i)\colon T^i(C_i) \;\xrightarrow{\sim}\; T^{i+1}(D_{i+1}) \;=\; T^{i+1}(C_{i+1}) \ ,$$

and we get

$$C_0 \;\xrightarrow{\sim}\; T^1(C_1) \;\xrightarrow{\sim}\; T^2(C_2) \;\xrightarrow{\sim}\; \cdots \xrightarrow{\sim}\; T^{\ell-1}(C_{\ell-1}) \;\xrightarrow{\sim}\; T^\ell(D_\ell) \ ,$$

which we will denote by

$$\rho_{(L_0,\dots,L_\ell)}\colon C_0 \;\xrightarrow{\sim}\; T^\ell(D_\ell) \ .$$

Thus we can classify coherent chains by means of this isomorphism.

(7.12) Notation. *For $C, D \in \mathscr{C}_n$ and $\rho \in \mathrm{Isom}_\Gamma\big(C, T^\ell(D)\big)$ we define*

$$\mathrm{Chain}_\ell^\rho(L, K; A) := \\ \{(L_0, \dots, L_\ell) \in \text{c-Chain}_\ell(L, K; A) : C_0 = C, D_\ell = D, \rho_{(L_0,\dots,L_\ell)} = \rho\} \ .$$

(7.13) Remark. Obviously we have the disjoint union

$$\text{c-Chain}_\ell(L, K; A) \;= \coprod_{C,D} \coprod_{\rho} \mathrm{Chain}_\ell^\rho(L, K; A) \ ,$$

where C and D run through the set of twisted cyclic structures of L and K respectively and ρ runs through the set $\mathrm{Isom}_\Gamma\big(C, T^\ell(D)\big)$.

(7.14) Proposition. *If A is a division algebra and $\big(n, \varphi(n)\big) = 1$, then*

$$\text{c-Chain}_\ell(A) \;=\; \mathrm{Chain}_\ell(A) \ .$$

Proof: This follows immediately from the uniqueness of twisted cyclic structures, proven in (1.30). □

(7.15) Corollary. *If A is a division algebra and $\big(n, \varphi(n)\big) = 1$, and if we assume that $\mathrm{Chain}_\ell(L, K; A) \neq \emptyset$, then there are unique twisted cyclic structures C and D on L and K respectively, and we have the disjoint union*

$$\mathrm{Chain}_\ell(L, K; A) \;=\; \coprod_{\rho \in \mathrm{Isom}_\Gamma(C, T^\ell(D))} \mathrm{Chain}_\ell^\rho(L, K; A) \;.$$

(7.16) Definition. *Let C and D be some twisted cyclic structures on L and K respectively and let $\rho \in \mathrm{Isom}_\Gamma\big(C, T^\ell(D)\big)$, then we say that L and K are (ℓ, ρ)-**chain equivalent over** k', if the set*

$$\mathrm{Chain}_\ell^\rho(L, K; A)_{k'} \;=\; \mathrm{Chain}_\ell^\rho(L_{k'}, K_{k'}; A_{k'}) \;\neq\; \emptyset$$

is non-empty. (Note that C and D are also twisted cyclic structures on $L_{k'}$ and $K_{k'}$.)

(7.17) Proposition. *Let $k'|k$ be an algebraic field extension, then we have for any $(L_0, \ldots, L_\ell) \in \mathrm{Chain}_\ell(A)$ the equivalence*

$$(L_0, \ldots, L_\ell) \text{ is coherent} \quad \Longleftrightarrow \quad (L_0, \ldots, L_\ell)_{k'} \text{ is coherent} \;.$$

In particular, there is the injective map

$$\begin{aligned} \text{c-}\mathrm{Chain}_\ell(A) &\longrightarrow \text{c-}\mathrm{Chain}_\ell(A_{k'}) \\ (L_0, \ldots, L_\ell) &\longmapsto (L_0, \ldots, L_\ell)_{k'} \;, \end{aligned}$$

which has Galois descent, if $k'|k$ is a Galois extension.

Proof: One only has to observe that the associated twisted cyclic structures C_i and D_i do not change under base extension. □

Finally, we want to state a useful lemma, which we will need later.

(7.18) Lemma. *Let $(L_0, \ldots, L_\ell) \in \mathrm{Chain}_\ell(A)$ be a chain. Then $(L_0, \ldots, L_\ell)$ is coherent if and only if*

$$\mathcal{K}_{(L_i, L_{i-1})} \;=\; \mathcal{K}_{(L_i, L_{i+1})}$$

for $i = 1, \ldots, \ell - 1$.—More precisely: The last condition for i is equivalent to the condition $C_i = D_i$ for i.

Proof: We fix an $i \in \{1, \ldots, \ell - 1\}$. Let $d \in D_i$ and $c \in C_i$ be generators of the cyclic groups and $e \in M_{L_i}$ a primitive idempotent of $\bar{L}_i$. Then (3.19) says

$$\mathcal{K}_{(L_i, L_{i-1})} \;=\; \left\{ \zeta' \sum_{\nu=0}^{n-1} \zeta^\nu d^\nu(e) : \zeta', \zeta \in \mu_n \right\}$$

and

$$\mathcal{K}_{(L_i, L_{i+1})} \;=\; \left\{ \zeta' \sum_{\nu=0}^{n-1} \zeta^\nu c^\nu(e) : \zeta', \zeta \in \mu_n \right\} \;.$$

If $C_i = D_i$, then we may choose $c = d$ and the claim $\mathcal{K}_{(L_i,L_{i-1})} = \mathcal{K}_{(L_i,L_{i+1})}$ is clear. If $\mathcal{K}_{(L_i,L_{i-1})} = \mathcal{K}_{(L_i,L_{i+1})}$, then by the following lemma

$$\begin{aligned} D_i &= D_{(A,L_{i-1},L_i)} \\ &= C_{(A,L_i,L_{i-1})} \\ &= C_{(A,L_i,L_{i+1})} \\ &= C_i \ , \end{aligned}$$

where the first and last equality are the definitions, the second equality is the tautological one and the third equality follows from (7.19). □

(7.19) Lemma. *Let (A, L, K) be a twisted cyclic k-algebra of degree n, further $[X] \in \mathcal{K}_{(L,K)}/\mu_n$ and $[Y] \in \mathcal{K}_{(K,L)}/\mu_n$ generators of the cyclic groups. Then*

$$C_{(A,L,K)} = \{(\bar{L} \xrightarrow{\sim} \bar{L}, X \longmapsto \xi X) : \xi \in \mu_n\}$$

and

$$D_{(A,L,K)} = \{(\bar{K} \xrightarrow{\sim} \bar{K}, Y \longmapsto \xi Y) : \xi \in \mu_n\} \ .$$

Therefore C and D depend solely on $\mathcal{K}_{(L,K)} \subseteq \bar{L}^*$ and $\mathcal{K}_{(K,L)} \subseteq \bar{K}^*$ respectively

Proof: This is just a corollary of (3.12) and (3.16): The $\bar{k}$-automorphisms are defined by the image of X and Y respectively. (3.16) shows that for these images there are only the n possibilities of multiples by elements of μ_n. □

§ 8. Chains of Kummer Elements

If we want to consider $\bar{k}$-chains in a central simple algebra A, we can make use of the interpretation of twisted cyclic decompositions we got in (6.15).
We fix a field k and positive integers $n \geq 2$ and ℓ such that n is prime to the characteristic of k. Let A be a central simple k-algebra of degree n.

1. Definition of Chains of Kummer Elements

First we define the chains of Kummer elements:

(8.1) Definition. *A* **chain of Kummer elements** *in A of length ℓ is a $\ell+1$-tuple $([X_0], \ldots, [X_\ell]) \in \mathrm{W}(A)^{\ell+1}$ of Kummer elements such that consecutive elements are in Kummer relation, i.e.,*

$$X_{i-1}X_i \;=\; \zeta_i X_i X_{i-1}$$

for $i = 1, \ldots, \ell$ and primitive n-th roots of unity $\zeta_i \in \mu_n = \mu_n(\bar{k})$.

Note that the condition $X_{i-1} \xrightarrow{\zeta_i} X_i$ is independent of the choice of representatives $X_i \in [X_i]$.

(8.2) Notation. *We denote the set of chains of Kummer elements in A of length ℓ by the symbol*

$$\text{K-Chain}_\ell(A)\ .$$

Let $Z := (\zeta_1, \ldots, \zeta_\ell)$ be a ℓ-tuple of primitive n-th root of unity. Then we write

$$\text{K-Chain}_\ell^Z(A) := \big\{([X_0], \ldots, [X_\ell]) \in \text{K-Chain}_\ell(A) : X_{i-1}X_i = \zeta_i X_i X_{i-1},\ i = 1, \ldots, \ell\big\}\ .$$

If $Z = (\zeta, \ldots, \zeta)$, then we write just ζ instead of Z:

$$\text{K-Chain}_\ell^\zeta(A) \;:=\; \text{K-Chain}_\ell^Z(A)\ .$$

The notations $\text{K-Chain}_\ell([X],[Y];A)$, $\text{K-Chain}_\ell^Z([X],[Y];A), \ldots$ *are to be read in the same obvious way like the corresponding ones in §7.*

(8.3) Remark. Clearly, for Kummer elements $[X], [Y] \in \mathrm{W}(A)$,

$$\text{K-Chain}_\ell(A) \;=\; \coprod_Z \text{K-Chain}_\ell^Z(A)\ ,$$

and herein

$$\text{K-Chain}_\ell([X],[Y];A) \;=\; \coprod_Z \text{K-Chain}_\ell^Z([X],[Y];A)\ ,$$

where Z runs through the ℓ-tuples of primitive n-th roots of unity.

How are the different sets on the right hand side connected mutually?

(8.4) Proposition. *Let $Z = (\zeta_1, \ldots, \zeta_\ell)$ and $Z' = (\zeta'_1, \ldots, \zeta'_\ell)$ be two ℓ-tuples of primitive n-th roots of unity. Let $\nu_i \in (\mathbb{Z}/n\mathbb{Z})^*$ for $i = 1, \ldots, \ell$, be the unique elements such that $\zeta'_i = \zeta_i^{\nu_i}$. Define $\epsilon_0 := 1$ and for $i = 1, \ldots, \ell$*

$$\epsilon_i \;:=\; \frac{\nu_i}{\nu_{i-1}} \frac{\nu_{i-2}}{\nu_{i-3}} \cdots \;=\; \prod_{j=1}^{i} \nu_j^{(-1)^{i-j}} \;,$$

then the map

$$\begin{aligned} \psi_Z^{Z'} \colon \text{K-Chain}_\ell^Z(A) &\;\xrightarrow{\sim}\; \text{K-Chain}_\ell^{Z'}(A) \\ ([X_0], \ldots, [X_\ell]) &\;\longmapsto\; ([X_0^{\epsilon_0}], [X_1^{\epsilon_1}], \ldots, [X_\ell^{\epsilon_\ell}]) \end{aligned}$$

is a bijection. Furthermore we have the functoriality

$$\psi_Z^Z \;=\; \mathrm{id} \quad \text{and} \quad \psi_Z^{Z''} \;=\; \psi_{Z'}^{Z''} \circ \psi_Z^{Z'} \;,$$

where Z'' is a third ℓ-tuple of primitive n-th roots of unity. In the special case of $Z = (\zeta, \ldots, \zeta)$ and $Z' = (\zeta', \ldots, \zeta')$, where $\zeta' = \zeta^\nu$, we get

$$\epsilon_i \;=\; \begin{cases} \nu, & \text{if } i \text{ is odd} \\ 1, & \text{if } i \text{ is even.} \end{cases}$$

Proof: The map $\psi_Z^{Z'}$ is well defined: First note that $[X_i^n] = [1]$; moreover $X_{i-1} \xrightarrow{\zeta_i} X_i$ implies $X_{i-1}^{\epsilon_{i-1}} \xrightarrow{\zeta'_i} X_i^{\epsilon_i}$, since $\epsilon_{i-1}\epsilon_i = \nu_i$ and

$$X_{i-1}^{\epsilon_{i-1}} X_i^{\epsilon_i} X_{i-1}^{-\epsilon_{i-1}} X_i^{-\epsilon_i} \;=\; \zeta_i^{\epsilon_{i-1}\epsilon_i} \;=\; \zeta_i^{\nu_i} \;=\; \zeta'_i \;.$$

The functoriality is obvious and it implies the bijectivity by the standard argument. □

(8.5) Corollary. *Let $[X], [Y] \in \mathrm{W}(A)$ be two Kummer elements. In the situation of (8.4) the map $\psi_Z^{Z'}$ induces the bijections*

$$\psi_Z^{Z'} \colon \text{K-Chain}_\ell^Z([X], -; A) \;\xrightarrow{\sim}\; \text{K-Chain}_\ell^{Z'}([X], -; A)$$

and

$$\psi_Z^{Z'} \colon \text{K-Chain}_\ell^Z([X], [Y]; A) \;\xrightarrow{\sim}\; \text{K-Chain}_\ell^{Z'}([X], [Y^{\epsilon_\ell}]; A) \;.$$

In particular, we have the bijective map

$$\psi_Z^{Z'} \colon \coprod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} \text{K-Chain}_\ell^Z([X], [Y^i]; A) \;\xrightarrow{\sim}\; \coprod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} \text{K-Chain}_\ell^{Z'}([X], [Y^i]; A) \;.$$

Now we see that for many questions, it is enough to consider the case $Z = (\zeta, \ldots, \zeta)$. For these cases, we have the addendum:

(8.6) Corollary. *Let ζ and $\zeta' = \zeta^\nu$ be two primitive n-th roots of unity, such that $\nu \in (\mathbb{Z}/n\mathbb{Z})^*$.*
If ℓ is even, we have the bijective map

$$\begin{aligned} \psi_\zeta^{\zeta'} \colon \text{K-Chain}_\ell^\zeta([X],[Y];A) &\xrightarrow{\sim} \text{K-Chain}_\ell^{\zeta'}([X],[Y];A) \\ ([X_0],\ldots,[X_\ell]) &\longmapsto ([X_0],[X_1^\nu],[X_2],\ldots,[X_{\ell-1}^\nu],[X_\ell]) \ . \end{aligned}$$

If ℓ is odd, we have the bijective map

$$\begin{aligned} \psi_\zeta^{\zeta'} \colon \text{K-Chain}_\ell^\zeta([X],[Y];A) &\xrightarrow{\sim} \text{K-Chain}_\ell^{\zeta'}([X],[Y^\nu];A) \\ ([X_0],\ldots,[X_\ell]) &\longmapsto ([X_0],[X_1^\nu],[X_2],\ldots,[X_{\ell-1}],[X_\ell^\nu]) \ . \end{aligned}$$

(8.7) Notation. *For any ℓ-tuple Z of primitive n-th roots of unity and Kummer elements $[X],[Y] \in \mathrm{W}(A)$, we define*

$$\widetilde{\text{K-Chain}}_\ell^Z([X],[Y];A) := \coprod_{i\in(\mathbb{Z}/n\mathbb{Z})^*} \text{K-Chain}_\ell^Z([X],[Y^i];A) \ .$$

(8.8) Remark. By virtue of the bijections $\psi_Z^{Z'}$, we can *canonically* identify these sets for different ℓ-tuples Z and Z'.

2. The Notion of Chain Equivalence of Kummer Elements

Analogously to §7, 2. we make the following notations and definitions:

(8.9) Notation. *Let $k'|k$ be a field extensions, and let $[X],[Y] \in \mathrm{W}(A)$ be two Kummer elements, then we denote with*

$$\text{K-Chain}_\ell([X],[Y];A)_{k'} := \text{K-Chain}_\ell([X],[Y];A_{k'})$$

the set of all k'-chains from $[X]$ to $[Y]$ in A of length ℓ.

(8.10) Definition. *Two Kummer elements $[X],[Y] \in \mathrm{W}(A)$ are called (ℓ,Z,ν)-**chain equivalent** (or **-related**) **over** k', if*

$$\text{K-Chain}_\ell^Z([X],[Y^\nu];A)_{k'} \neq \emptyset \ ,$$

where $\nu \in (\mathbb{Z}/n\mathbb{Z})^*$ and Z an ℓ-tuple of primitive n-th roots of unity. If $Z = (\zeta,\ldots,\zeta)$ we write (ℓ,ζ,ν) instead of (ℓ,Z,ν).

(8.11) Remark. In the situation of (8.5) we can see:

$$[X],[Y] \text{ are } (\ell,Z,\nu)\text{-related} \iff [X],[Y] \text{ are } (\ell,Z',\epsilon_\ell\cdot\nu)\text{-related} \ .$$

Hence we always can reduce the question of being (ℓ,Z,ν)-related to the question of being (ℓ,ζ,ν')-related, for suitable ν'.

(8.12) Lemma. *Let $[X],[Y] \in \mathrm{W}(A)$ be Kummer elements, ζ,ζ' primitive n-th roots of unity and $\nu,\nu' \in (\mathbb{Z}/n\mathbb{Z})^*$. Then we have the following equivalences:*

If ℓ is even, then

$$[X],[Y] \text{ are } (\ell,\zeta,\nu)\text{-related} \iff [X],[Y] \text{ are } (\ell,\zeta',\nu)\text{-related}\ .$$

If ℓ is odd and $\zeta^{\nu'} = \zeta'^{\nu}$, then

$$[X],[Y] \text{ are } (\ell,\zeta,\nu)\text{-related} \iff [X],[Y] \text{ are } (\ell,\zeta',\nu')\text{-related}\ .$$

Proof: The first part follows directly with (8.6). The second part has to be shown just in one direction: For $Z = (\zeta,\dots,\zeta)$ and $Z' = (\zeta',\dots,\zeta')$ with the notations of (8.5) we have $\zeta' = \zeta^{\epsilon_\ell}$, therefore $\zeta^{\nu'} = \zeta'^{\nu} = \zeta^{\epsilon_\ell\cdot\nu}$, i.e., $\nu' = \epsilon_\ell\cdot\nu \in (\mathbb{Z}/n\mathbb{Z})^*$. But (8.11) tells us that: $[X],[Y]$ are (ℓ,ζ,ν)-related $\iff$ $[X],[Y]$ are $(\ell,\zeta',\epsilon_\ell\cdot\nu)$-related . □

(8.13) Remark. If $[X]$ and $[Y]$ are (ℓ,ζ,ν)-related, then they are $(\ell+1,\zeta,\nu)$-related: This follows from the fact that a chain of Kummer elements can be expanded at any link: If (X_{i-1},X_i) is a ζ-pair, then $(X_{i-1},X_{i-1}X_i)$ and $(X_{i-1}X_i,X_i)$ are also ζ-pairs. Cf. §6, 1.

3. Connection between K-Chains and c-Chains

To every chain of Kummer elements we can assign a chain of twisted cyclic extensions:

(8.14) Theorem. *Let Z be a ℓ-tuple of primitive n-th roots of unity and $[X],[Y] \in \mathrm{W}(A)$ any Kummer elements. Then we have a canonical bijection*

$$\begin{aligned}\psi_Z\colon \widetilde{\text{K-Chain}}_\ell^Z([X],[Y];A)_{\bar k} &\xrightarrow{\sim} \text{c-Chain}_\ell(k[X],k[Y];A)_{\bar k}\\ ([X_0],\dots,[X_\ell]) &\longmapsto (\bar k[X_0],\dots,\bar k[X_\ell])\end{aligned}$$

and for another Z', we have the compatibility relation

$$\psi_{Z'}\circ\psi_Z^{Z'} = \psi_Z\ .$$

Proof: The map is well defined, since the algebras $\bar k[X_i]$ are separable commutative $\bar k$-subalgebras of $\bar A = A_{\bar k}$. Because of (6.15) the pairs $(\bar k[X_{i-1}],\bar k[X_i])$ are twisted cyclic decompositions of $\bar A$. Furthermore one observes

$$\mathcal{K}_{(\bar k[X_i],\bar k[X_{i-1}])} = \{[X_i^0],\dots,[X_i^{n-1}]\}$$

and

$$\mathcal{K}_{(\bar k[X_i],\bar k[X_{i+1}])} = \{[X_i^0],\dots,[X_i^{n-1}]\}\ ,$$

therefore by (7.18) the chain $(\bar k[X_0],\dots,\bar k[X_\ell])$ is coherent. The last formula is clear.
Injectivity of ψ_Z: Let be given two chains $([X_0],\dots,[X_\ell])$ and $([X_0'],\dots,[X_\ell'])$ out of $\widetilde{\text{K-Chain}}_\ell^Z([X],[Y];A)_{\bar k}$ which are mapped to the same coherent chain via ψ_Z. Let i be the least integer such that $[X_i] \neq [X_i']$. Since $[X_0] = [X] = [X_0']$ we know $i \geq 1$.

Furthermore we know that (X_{i-1}, X_i) and $(X_{i-1}, X'_i) = (X'_{i-1}, X'_i)$ are ζ_i-pairs, where $Z = (\zeta_1, \ldots, \zeta_\ell)$. Since

$$\bar{k}[X_{i-1}] \;=\; \bar{k}[X'_{i-1}] \quad \text{and} \quad \bar{k}[X_i] \;=\; \bar{k}[X'_i]$$

the sets

$$\mathcal{K}_{(\bar{k}[X_i], \bar{k}[X_{i-1}])} \;=\; \mathcal{K}_{(\bar{k}[X'_i], \bar{k}[X'_{i-1}])}$$

are equal and $[X_i]$ as well as $[X'_i]$ are the unique element of this set which is in ζ_i-relation with $[X_{i-1}] = [X'_{i-1}]$. Hence $[X_i] = [X'_i]$, and we have shown injectivity.
Surjectivity of ψ_Z: Let $(\bar{L}_0, \ldots, \bar{L}_\ell) \in \text{c-Chain}_\ell(k[X], k[Y]; A)_{\bar{k}}$ be a coherent chain. For $i = 1, \ldots, \ell$ choose a generator $[X_i]$ of the cyclic group $\mathcal{K}_{(\bar{L}_i, \bar{L}_{i-1})}$ $(= \mathcal{K}_{(\bar{L}_i, \bar{L}_{i+1})}$ for $i < \ell)$. Then $\bar{L}_i = \bar{k}[X_i]$ and $([X_0], \ldots, [X_\ell]) \in \text{K-}\widetilde{\text{Chain}}_\ell^{Z'}([X], [Y]; A)_{\bar{k}}$ for $[X_0] := [X]$ and some ℓ-tuple Z' of primitive n-th root of unity. This chain maps to $(\bar{L}_0, \ldots, \bar{L}_\ell)$ via $\psi_{Z'}$. Because of $\psi_{Z'} = \psi_Z \circ \psi^Z_{Z'}$, our surjectivity follows. □

Chapter IV
Geometry of Kummer Elements and Chains

The objects we considered in the last chapter have, in a natural way, a geometric structure: We will see that $\mathrm{W}(A)$, $\text{K-Chain}_\ell(A)$, $\text{K-Chain}_\ell([X], -; A), \ldots$ can be identified with the k-rational points of smooth varieties.

§ 9. The Variety of Kummer Elements

In this section we fix a field k and a positive integer $n \geq 2$ which is not divisible by the characteristic of k. Let A be a central simple k-algebra of degree n and $\zeta \in \mu_n = \mu_n(\bar{k})$ a primitive n-th root of unity.

1. A as a k-Scheme

Since A is an n^2-dimensional k-vector space, it gives rise, in the well known way, to an n^2-dimensional affine space over k, which is isomorphic to $\mathbb{A}_k^{n^2}$ as k-scheme.

(9.1) Definition. *Let $\check{A} := \mathrm{Hom}_{k\text{-lin}}(A, k)$ be the (k-vector space) dual of A and $S(\check{A})$ its associated symmetric algebra, then we define the k-schemes*

$$\mathbf{A}(A) := \mathrm{Spec}\big(S(\check{A})\big) \quad \text{and} \quad \mathbf{P}(A) := \mathrm{Proj}\big(S(\check{A})\big) .$$

(9.2) Remark. For every field extension $k'|k$ we have the canonical identification of the k'-rational points of $\mathbf{A}(A)$ with the elements of $A_{k'} = A \otimes_k k'$:

$$\begin{aligned} \mathbf{A}(A)(\mathrm{Spec}\, k') &= \mathrm{Hom}_{k\text{-alg}}\big(S(\check{A}), k'\big) \\ &= \mathrm{Hom}_{k\text{-lin}}(\check{A}, k') \\ &= \mathrm{Hom}_{k\text{-lin}}(\check{A}, k) \otimes k' \\ &= A_{k'} . \end{aligned}$$

Analogously

$$\mathbf{P}(A)(\mathrm{Spec}\, k') = \big(A_{k'} - \{0\}\big)/k'^* .$$

If we choose a k-basis $a_1, \ldots, a_{n^2}$ of A, then the isomorphism of the (graded) k-algebras

$$\begin{aligned} k[X_1, \ldots, X_{n^2}] &\xrightarrow{\sim} S(\check{A}) \\ X_i &\longmapsto \check{a}_i \end{aligned}$$

for $i = 1, \ldots, n^2$ and the dual basis $\check{a}_1, \ldots, \check{a}_{n^2}$ of $a_1, \ldots, a_{n^2}$, induces isomorphisms $\mathbf{A}(A) \xrightarrow{\sim} \mathbb{A}_k^{n^2}$ and $\mathbf{P}(A) \xrightarrow{\sim} \mathbb{P}_k^{n^2-1}$. Additionally we have a multiplication morphism

on the affine scheme: The multiplication induces a morphism $A \otimes_k A \to A$, $x \otimes y \mapsto xy$ of k-modules, and after dualizing we get

$$\check{A} \longrightarrow \check{A} \otimes_k \check{A} .$$

If we compose this morphism with the double tensor product of the canonical injections $\check{A} \otimes_k \check{A} \to S(\check{A}) \otimes_k S(\check{A})$, we get the k-linear morphism

$$\check{A} \longrightarrow S(\check{A}) \otimes_k S(\check{A}) ;$$

by the universal property of the symmetric algebras. This factorizes in the form

$$\begin{array}{ccc} \check{A} & \longrightarrow & \check{A} \otimes_k \check{A} \\ \downarrow & & \downarrow \\ S(\check{A}) & \xrightarrow{\psi} & S(\check{A}) \otimes_k S(\check{A}) , \end{array}$$

where ψ is unique. Then it induces the morphism of k-schemes

$$\mathrm{Spec}(\psi)\colon \mathbf{A}(A) \times_k \mathbf{A}(A) \longrightarrow \mathbf{A}(A) ,$$

which is on the k'-rational points just the multiplication on $A_{k'}$.

In §6, 1., we defined the maps

$$\mathrm{Srd}_\nu\colon A \longrightarrow k ,$$

$\nu = 1, \ldots, n$, in particular the reduced norm $\mathrm{Nrd} = \mathrm{Srd}_n$ and trace $\mathrm{Trd} = \mathrm{Srd}_1$. Furthermore we define the maps

$$\begin{aligned} T^\nu\colon A &\longrightarrow k \\ X &\longmapsto \mathrm{Trd}(X^\nu) . \end{aligned}$$

(9.3) Lemma. *Assume k is algebraically closed. Then the maps Srd_ν and T^ν are regular functions on the scheme $\mathbf{A}(A)$, i.e., there are uniquely defined (homogeneous) elements in $S(\check{A}) = \mathcal{O}\big(\mathbf{A}(A)\big)$—which we also denote by Srd_ν and T^ν—such that they represent these maps. Srd_ν and T^ν are homogeneous of degree ν.*

Proof: Choose an isomorphism $\alpha\colon A \xrightarrow{\sim} A_0 = \mathrm{M}_n(k)$ of k-algebras. This also induces an isomorphism $\mathbf{A}(A) \xrightarrow{\sim} \mathbf{A}(A_0)$ of k-schemes as well as the graded isomorphism of the global section rings $S(\check{A}_0) \xrightarrow{\sim} S(\check{A})$. Therefore we may assume that $A = A_0$. We choose the canonical basis E_{ij}, $i, j = 1, \ldots, n$, of the k-vector space A_0, and we denote with X_{ij}, $i, j = 1, \ldots, n$, its dual basis. Then

$$S(\check{A}_0) = k[X_{11}, X_{12}, \ldots, X_{nn}] ,$$

and it is clear that Srd_ν is a homogeneous polynomial in the X_{ij} of degree ν, e.g.,

$$\mathrm{Srd}_1 = \mathrm{Trd} = X_{11} + X_{22} + \cdots + X_{nn} .$$

The ν-th power of the matrix (X_{ij}) is given by n^2 homogeneous polynomials of degree ν. Therefore $\mathrm{Trd}\big((X_{ij})^\nu\big)$ is also a homogeneous polynomial of degree ν. □

(9.4) Remark. In the proof we have of course $\mathrm{Srd}_\nu, T^\nu \in \mathbb{Z}[X_{11}, X_{12}, \ldots, X_{nn}]$.

Now let k again be an arbitrary field of characteristic prime to n.

(9.5) Lemma. *The regular functions of (9.3) are already defined over the base field:*

$$\mathrm{Srd}_\nu, T^\nu \in S(\check{A}) \ .$$

Proof: First of all

$$\mathrm{Srd}_\nu, T^\nu \in S(\check{A}) \otimes_k \bar{k} \ = \ \mathcal{O}(\mathbf{A}(A) \times_k \bar{k}) \ ,$$

where $\bar{k}$ is a separable closure. In fact this is true for $A = A_0$, as we have seen above, and there are already $\bar{k}$-isomorphisms $\alpha\colon \bar{A} \xrightarrow{\sim} \bar{A}_0$, hence $\alpha_*\colon \mathbf{A}(\bar{A}) \xrightarrow{\sim} \mathbf{A}(\bar{A}_0)$, because A is a central simple k-algebra.
Now all we have to show is that for $f := \mathrm{Srd}_\nu, T^\nu$ and $\gamma \in \Gamma = \mathrm{Gal}(\bar{k}|k)$, the diagram

$$\begin{array}{ccc} \bar{A} & \xrightarrow{f} & \bar{k} \\ {\scriptstyle \mathrm{id}\otimes\gamma}\downarrow & & \downarrow{\scriptstyle \gamma} \\ \bar{A} & \xrightarrow{f} & \bar{k} \end{array}$$

is commutative. This follows from the commutative diagram

$$\begin{array}{ccccc} \bar{A} & \xrightarrow[\alpha]{\sim} & \mathrm{M}_n(\bar{k}) & \xrightarrow{f} & \bar{k} \\ {\scriptstyle \mathrm{id}\otimes\gamma}\downarrow & & {\scriptstyle \kappa_{X_\gamma}\circ(\mathrm{id}\otimes\gamma)}\downarrow & & \downarrow{\scriptstyle \gamma} \\ \bar{A} & \xrightarrow[\alpha]{\sim} & \mathrm{M}_n(\bar{k}) & \xrightarrow{f} & \bar{k} \ . \end{array}$$

For the left part cf. §4,2. The commutativity of the right part is clear, since Srd_ν and T^ν are invariant under any conjugation κ_{X_γ}, and commute with the Galois action. □

(9.6) Remark. $T^\nu \in S(\check{A})$ already follows from $\mathrm{Trd} \in S(\check{A})$ since the morphism "taking the ν-th power" $\mathbf{A}(A) \to \mathbf{A}(A)$ is a morphism, which is defined over k. The k-rationality of Trd is clear, since Trd is linear, so the k-rationality only has to be checked on a k-basis of A and this is clear.

(9.7) Notation. *We denote the distinguished open subschemes of* $\mathbf{A}(A)$ *and* $\mathbf{P}(A)$, *associated to* Nrd, *by*

$$\mathrm{GL}_1(A) \ := \ \mathrm{Spec}\, S(\check{A})_{\mathrm{Nrd}} \ = \ D(\mathrm{Nrd}) \ \subseteq \ \mathbf{A}(A)$$

and

$$\mathrm{PGL}_1(A) \ := \ \mathrm{Spec}\big(S(\check{A})\big)_{(\mathrm{Nrd})} \ = \ D_+(\mathrm{Nrd}) \ \subseteq \ \mathbf{P}(A) \ .$$

(9.8) Remark. For every field extension $k'|k$ we have the identifications of the k'-rational points $\mathrm{GL}_1(A)(\mathrm{Spec}\, k') = (A \otimes_k k')^*$ and $\mathrm{PGL}_1(A)(\mathrm{Spec}\, k') = A^*_{k'}/k'^*$. Moreover there are morphisms of k-schemes

$$\mathrm{GL}_1(A) \times_k \mathbf{A}(A) \ \longrightarrow \ \mathbf{A}(A)$$

and

$$\mathrm{GL}_1(A) \times_k \mathbf{P}(A) \longrightarrow \mathbf{P}(A) ,$$

which are on the k'-rational points just the conjugation:

$$\begin{aligned} A_{k'}^* \times A_{k'} &\longrightarrow A_{k'} \\ (g, a) &\longmapsto gag^{-1} . \end{aligned}$$

2. $\mathcal{W}(A)$ and $\mathrm{W}(A)$ as Varieties over an Algebraically Closed Field

We want to see $\mathcal{W}(A)$ and $\mathrm{W}(A)$ as subvarieties of $\mathbf{A}(A)$ and $\mathbf{P}(A)$ respectively.
First we want to consider this in the algebraically closed setting. So in this subsection let k be algebraically closed.
In the last subsection we have seen that the maps $\mathrm{Srd}_\nu, T^\nu \colon A \to k$ are homogeneous elements of the global section ring $\mathcal{O}\big(\mathbf{A}(A)\big)$. So we can make the following definition

(9.9) Definition. *We define the subvarieties*

$$\begin{aligned} \bar{\mathcal{W}}(A) &:= V(\mathrm{Srd}_1, \cdots, \mathrm{Srd}_{n-1}) \subseteq \mathbf{A}(A) \\ \bar{\mathrm{W}}(A) &:= V_+(\mathrm{Srd}_1, \cdots, \mathrm{Srd}_{n-1}) \subseteq \mathbf{P}(A) \\ \mathcal{W}(A) &:= \bar{\mathcal{W}}(A) \cap D(\mathrm{Nrd}) \subseteq \mathbf{A}(A) \\ \mathrm{W}(A) &:= \bar{\mathrm{W}}(A) \cap D_+(\mathrm{Nrd}) \subseteq \mathbf{A}(A) , \end{aligned}$$

where $D(\mathrm{Nrd})$ *and* $D_+(\mathrm{Nrd})$ *are the distinguished open subsets associated to* Nrd.

(9.10) Remark. The closed, i.e., k-rational points of $\mathcal{W}(A)$ and $\mathrm{W}(A)$ are exactly the Kummer elements and Kummer lines of A. Hence we used the same symbols as in the sections above.

In the language of schemes we can define the varieties in the following way:

(9.11) Lemma. *Let* $I := (\mathrm{Srd}_1, \ldots, \mathrm{Srd}_{n-1}) \subseteq S(\check{A})$ *be the graded Ideal generated by the elements* $\mathrm{Srd}_1, \ldots, \mathrm{Srd}_{n-1}$ *and let* $\sqrt{I}$ *denote the radical of* I. *Then*

$$\begin{aligned} \bar{\mathcal{W}}(A) &:= \mathrm{Spec}\big(S(\check{A})/\sqrt{I}\big) \\ \bar{\mathrm{W}}(A) &:= \mathrm{Proj}\big(S(\check{A})/\sqrt{I}\big) \\ \mathcal{W}(A) &:= \mathrm{Spec}\big(S(\check{A})/\sqrt{I}\big)_{\mathrm{Nrd}} \\ \mathrm{W}(A) &:= \mathrm{Spec}\big(S(\check{A})/\sqrt{I}\big)_{(\mathrm{Nrd})} . \end{aligned}$$

We will see that I is actually radical in $S(\check{A})_{\mathrm{Nrd}}$.

(9.12) Claim. *If $(n!)$ is prime to the characteristic of k, then $T^1, \dots, T^{n-1}$ is another set of generators of the Ideal I:*

$$(T^1, \dots, T^{n-1}) \;=\; (\mathrm{Srd}_1, \dots, \mathrm{Srd}_{n-1}) \;\subseteq\; S(\check{A}) \;.$$

Proof: Like in (6.5) this follows from the formula

$$T^\nu - T^{\nu-1}\,\mathrm{Srd}_1 + T^{\nu-2}\,\mathrm{Srd}_2 - \cdots + (-1)^{\nu-1} T^1\,\mathrm{Srd}_{\nu-1} + (-1)^\nu \nu\,\mathrm{Srd}_\nu \;=\; 0 \;,$$

$\nu = 1, \dots, n-1$, which follows from Newton's formula: In the case $A = A_0 = \mathrm{M}_n(k)$ one diagonalizes the generic matrix, and then the formula directly follows. □

(9.13) Remark. The morphisms $\mathrm{GL}_1(A) \times \mathbf{A}(A) \to \mathbf{A}(A)$ and $\mathrm{GL}_1(A) \times \mathbf{P}(A) \to \mathbf{P}(A)$, mentioned in (9.8) induce morphisms

$$\mathrm{GL}_1(A) \times \mathcal{W}(A) \;\longrightarrow\; \mathcal{W}(A) \quad \text{and} \quad \mathrm{GL}_1(A) \times \mathrm{W}(A) \;\longrightarrow\; \mathrm{W}(A) \;,$$

i.e., $\mathrm{GL}_1(A)$ acts on $\mathcal{W}(A)$ and $\mathrm{W}(A)$ by conjugation. The last action is transitive, cf. (6.3), i.e., for any closed point $[X] \in \mathrm{W}(A)$ the morphism

$$\begin{aligned} \mathrm{GL}_1(A) &\longrightarrow \mathrm{W}(A) \\ G &\longmapsto [GXG^{-1}] \end{aligned}$$

is surjective. The first action is not transitive—one misses the scaling; however the morphism

$$\begin{aligned} \mathrm{GL}_1(A) \times (\mathbb{G}_\mathrm{m})_k \times \mathcal{W}(A) &\longrightarrow \mathcal{W}(A) \\ (G, g, X) &\longmapsto gGXG^{-1} \end{aligned}$$

gives a transitive action.

(9.14) Proposition. *$\mathcal{W}(A)$ and $\mathrm{W}(A)$ are irreducible topological spaces.*

Proof: This is a corollary of (9.13) since $\mathrm{GL}_1(A)$ (which is open, dense in $\mathbf{A}(A) \cong \mathbb{A}^{n^2}$) and $\mathrm{GL}_1(A) \times (\mathbb{G}_\mathrm{m})_k$ are irreducible and they map surjectively to $\mathrm{W}(A)$ and $\mathcal{W}(A)$ respectively, by the action on some fixed element $[X] \in \mathrm{W}(A)$ or $X \in \mathcal{W}(A)$. □

(9.15) Corollary. *The open subsets $\mathcal{W}(A) \subseteq \bar{\mathcal{W}}(A)$ and $\mathrm{W}(A) \subseteq \bar{\mathrm{W}}(A)$ are dense, hence $\bar{\mathcal{W}}(A)$ and $\bar{\mathrm{W}}(A)$ are irreducible topological spaces.*

Proof: We may assume $A = A_0 = \mathrm{M}_n(k)$. Let $X \in \bar{\mathcal{W}}(A) - \mathcal{W}(A)$ or equivalently $[X] \in \bar{\mathrm{W}}(A) - \mathrm{W}(A)$, i.e., $\mathrm{Prd}(X, t) = t^n$. Therefore X is nilpotent and (after conjugation with a suitable element in $\mathrm{GL}_1(A)$) we may assume that X is a strictly (upper) triangular matrix: The diagonal entries are zero.
For every $\lambda \in k^*$ and any primitive n-th root $\zeta \in \mu_n$ of unity we have

$$X + \lambda X_0(\zeta) \in \mathcal{W}(A) \quad \text{and} \quad [X + \lambda X_0(\zeta)] \in \mathrm{W}(A) \;,$$

since $\mathrm{Prd}(X + \lambda X_0(\zeta), t) = t^n - \lambda^n$. Hence X lies in the closure of $\mathcal{W}(A)$. The claim follows. □

As a further consequence of the transitive action we immediately get

(9.16) Proposition. *The varieties $\mathcal{W}(A)$ and $\mathrm{W}(A)$ are non-singular.*

Now we are going to give another proof of the non-singularity of $\mathcal{W}(A)$ and $\mathrm{W}(A)$. This will be done by direct computation, using the Jacobi criterion.

(9.17) Lemma. *Let $A = A_0 = \mathrm{M}_n(k)$ and let $\mathrm{Srd}_\nu \in k[X_{11}, X_{12}, \ldots, X_{nn}]$ be the homogeneous polynomials of degree ν from above. Then the partial derivatives of Srd_ν in the point $X = X_0(\zeta)$ in the coordinate X_{ij} is given by*

$$\frac{\partial \mathrm{Srd}_\nu}{\partial X_{ij}}\big(X_0(\zeta)\big) \;=\; \begin{cases} 0, & \text{if } i \neq j, \\ (-1)^{\nu-1}\zeta^{i(\nu-1)}, & \text{if } i = j\ . \end{cases}$$

Proof: Let $\mathbf{X} := (X_{ij})_{i,j=1,\ldots,n}$. We have

$$\det(t - \mathbf{X}) \;=\; t^n - t^{n-1}\,\mathrm{Srd}_1(\mathbf{X}) + \cdots + (-1)^n\,\mathrm{Srd}_n(\mathbf{X})\ ;$$

therefore we know

$$\frac{\partial \det(t-\mathbf{X})}{\partial X_{ij}} \;=\; -t^{n-1}\frac{\partial \mathrm{Srd}_1(\mathbf{X})}{\partial X_{ij}} + t^{n-2}\frac{\partial \mathrm{Srd}_2(\mathbf{X})}{\partial X_{ij}} - \cdots + (-1)^n t^0 \frac{\partial \mathrm{Srd}_n(\mathbf{X})}{\partial X_{ij}}\ .$$

On the other hand we have

$$\begin{aligned} \frac{\partial \det(t-\mathbf{X})}{\partial X_{ij}}\bigg|_X \;&=\; \frac{\partial \det\big(t-(X+\lambda E_{ij})\big)}{\partial \lambda}\bigg|_{\lambda=0} \\ &= \begin{cases} \dfrac{\partial}{\partial\lambda}\left[\prod_{\nu=1}^{n}(t-\zeta^\nu)\right]\bigg|_{\lambda=0} = 0, & \text{if } i \neq j \\ \dfrac{\partial}{\partial\lambda}\left[(t-\zeta^i-\lambda)\prod_{\substack{\nu=1\\ \nu\neq i}}^{n}(t-\zeta^\nu)\right]\bigg|_{\lambda=0} = -\dfrac{t^n-1}{t-\zeta^i}, & \text{if } i = j\ , \end{cases} \end{aligned}$$

but

$$\frac{t^n-1}{t-\zeta^i} \;=\; \frac{t^n-(\zeta^i)^n}{t-\zeta^i} \;=\; t^{n-1} + t^{n-2}\zeta^i + t^{n-3}\zeta^{2i} + \cdots + \zeta^{(n-1)i}\ .$$

Comparing the last with the first formula completes the proof. □

(9.18) Theorem. *The varieties $\mathcal{W}(A)$ and $\mathrm{W}(A)$ are non-singular k-varieties of dimension $n^2-(n-1)$ and n^2-n respectively.*

Proof: We may assume $A = A_0$. Because of the transitive actions on $\mathcal{W}(A)$ and $\mathrm{W}(A)$ mentioned in (9.13), all we have to prove (by virtue of the Jacobi criterion) is that the $(n-1)\times n^2$-matrix

$$\left(\frac{\partial \mathrm{Srd}_\nu}{\partial X_{ij}}\right)_{\substack{\nu=1,\ldots,n-1\\ i,j=1,\ldots,n}}\bigg|_{X_0(\zeta)} \;=\; \left(\frac{\partial \mathrm{Srd}_\nu}{\partial X_{ij}}\big(X_0(\zeta)\big)\right)_{\substack{\nu=1,\ldots,n-1\\ i,j=1,\ldots,n}}$$

has rank $n-1$. Again, $\zeta \in \mu_n$ is a primitive n-th root of unity. But by lemma (9.17) this matrix has a $(n-1) \times n$ minor of the form

$$\Big((-1)^{\nu-1}\zeta^{i(\nu-1)}\Big)_{\substack{\nu=1,\dots,n-1\\ i=1,\dots,n}} \quad .$$

We even know that besides this minor there are only trivial (zero) entries in the matrix. But this minor is a (modified) minor of the Vandermonde matrix $(\zeta^{ij})_{i,j=1,\dots,n}$ which has full rank n. Therefore our minor has rank $(n-1)$ and we are done. □

We immediately get from the proof:

(9.19) Corollary. *The ideal $I = (\mathrm{Srd}_1, \dots, \mathrm{Srd}_{n-1}) \subseteq \mathcal{O}(\mathcal{W}(A)) = S(\check{A})_{\mathrm{Nrd}}$ is already the ideal of vanishing functions. Since $\mathcal{W}(A)$ is irreducible, I is a prime ideal, especially $\sqrt{I} = I$ in $S(\check{A})_{\mathrm{Nrd}}$.*

3. $\mathcal{W}(A)$ and $\mathrm{W}(A)$ as k-Schemes

Now let k again be an arbitrary field of characteristic prime to n. Then we define the following k-schemes:

(9.20) Definition. *For a central simple k-algebra A of degree n we define the k-subschemes of $\mathbf{A}(A)$ and $\mathbf{P}(A)$*

$$\mathcal{W}^0(A) \;:=\; \mathrm{Spec}\big(S(\check{A})/(\mathrm{Srd}_1, \dots, \mathrm{Srd}_{n-1})\big)_{\mathrm{Nrd}} \;\subseteq\; \mathbf{A}(A)$$

and

$$\mathrm{W}^0(A) \;:=\; \mathrm{Spec}\big(S(\check{A})/(\mathrm{Srd}_1, \dots, \mathrm{Srd}_{n-1})\big)_{(\mathrm{Nrd})} \;\subseteq\; \mathbf{P}(A)$$

(9.21) Remark. For any field extension $k'|k$ we have

$$\mathcal{W}^0(A_{k'}) = \mathcal{W}^0(A) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k') \quad \text{and} \quad \mathrm{W}^0(A_{k'}) = \mathrm{W}^0(A) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k') \; .$$

(9.22) Proposition. *$\mathcal{W}^0(A)$ and $\mathrm{W}^0(A)$ are smooth integral k-schemes of dimension $n^2-(n-1)$ and n^2-n respectively. For any field extension $k'|k$ we have the identification of k'-rational points and Kummer elements*

$$\mathcal{W}^0(A)(\mathrm{Spec}\, k') \;=\; \mathcal{W}(A_{k'}) \quad \text{and} \quad \mathrm{W}^0(A)(\mathrm{Spec}\, k') \;=\; \mathrm{W}(A_{k'}) \; ,$$

which is induced by the identification of (9.2).

Proof: The first part only has to be proven over an algebraic closure of k—what we have done in the last subsection, since there $\mathrm{W}^0(A) = \mathrm{W}(A)$ and $\mathcal{W}^0(A) = \mathcal{W}(A)$. The second part is clear. □

§ 10. The Variety of Chains

We fix a field k and a positive integer $n \geq 2$ which is not divisible by the characteristic of k. Let A be a central simple k-algebra of degree n and $\zeta \in \mu_n = \mu_n(\bar{k})$ a primitive n-th root of unity lying in k. Furthermore we choose a k-basis $a_1, a_2, \ldots, a_{n^2}$ of the vector space A, and we denote its dual basis by $\check{a}_1, \ldots, \check{a}_{n^2}$.

1. The "Vectorbundle of Kummer Pairs"

We want to assign to the set

$$\{(X, Y) \in \mathcal{W}(A) \times A : XY - \zeta YX = 0\}$$

of Kummer pairs (in a slight broader sense, i.e., we don't demand Y to be invertible) the structure of a scheme—and more: of a vector bundle over the k-scheme $\mathcal{W}^0(A)$. Because of (6.10) for any Kummer element $X \in \mathcal{W}(A)$, the set $\{Y \in A : XY - \zeta YX = 0\}$ is a vector space of dimension n: Using the basis $a_1, a_2, \ldots, a_{n^2}$ one can interpret the equation $XY - \zeta YX = 0$ (in Y) as n^2 linear equations in the entries $y_1, y_2, \ldots, y_{n^2}$ of $Y = y_1 \cdot a_1 + y_2 \cdot a_2 + \cdots + y_{n^2} \cdot a_{n^2}$ for $y_i \in k$. If k is algebraically closed it is clear by (6.10) that our set is an n-dimensional vector subspace of A. Therefore the gradients of the n^2 linear equations span an $(n^2 - n)$-dimensional vector space. That means, one can leave out n of the n^2 equations. Since the gradients do not change under base field extension, everything holds for a general field k.

We will write

$$R \;:=\; \mathcal{O}\big(\mathcal{W}^0(A)\big) \;=\; \big(S(\check{A})/(\mathrm{Srd}_1, \ldots, \mathrm{Srd}_{n-1})\big)_{\mathrm{Nrd}}$$

for the global section ring of the affine scheme $\mathcal{W}^0(A)$—cf. §9.

The bilinear map $A \times A \to A$, $(x, y) \mapsto xy - \zeta yx$ induces, after dualizing, a morphism

$$\varphi\colon\ \check{A} \;\longrightarrow\; \check{A} \otimes_k \check{A}$$

of k-modules.
If we compose φ with the morphism $\check{A} \otimes_k \check{A} \to R \otimes_k S(\check{A})$, $a \otimes b \mapsto a \otimes b$, of k-modules, we get a morphism $\check{A} \to R \otimes_k S(\check{A})$ which induces—by the universal property of the symmetric algebra—a morphism

$$\phi\colon\ S(\check{A}) \;\longrightarrow\; R \otimes_k S(\check{A})$$

of graded k-algebras. We set $f_i := \phi(\check{a}_i) = \varphi(\check{a}_i)$.
Applying the functor Spec to it, we get the morphism

$$\mathrm{Spec}(\phi)\colon\ \mathcal{W}^0(A) \times_k \mathbf{A}(A) \;\longrightarrow\; \mathbf{A}(A)\ ,$$

which on the rational points is just the map

$$(x, y) \;\longmapsto\; xy - \zeta yx\ .$$

So the fibre over the k-rational point zero is our choice for the scheme of Kummer pairs (in the broader sense).

§ 10. The variety of chains

(10.1) Lemma. *The fibre of* $\mathrm{Spec}(\phi)$ *over zero is given by*

$$\mathrm{Spec}\big(R \otimes_k S(\check{A})\big)/(\mathrm{im}\,\varphi) \;=\; \mathrm{Spec}\big(R \otimes_k S(\check{A})\big)/\big(\phi(S(\check{A})_+)\big)\ ,$$

where $(\mathrm{im}\,\varphi)$ *is the ideal in* $R \otimes_k S(\check{A})$ *generated by the elements of* $\mathrm{im}(\varphi)$*—or equivalently by the elements of* $\phi\big(S(\check{A})_+\big)$*, which are of degree* > 0*.*

(10.2) Remark. The ideal $\big(\phi(S(\check{A})_+)\big) = (\mathrm{im}\,\varphi)$ is a graded ideal, already generated by the n^2 elements $f_1, f_2, \ldots, f_{n^2}$, which are of degree 1. The grading of $R \otimes_k S(\check{A})$ is given by the grading of the symmetric algebra $S(R \otimes_k \check{A}) = R \otimes_k S(\check{A})$.

Proof: (of Lemma (10.1)). The fibre is given by the spectrum of

$$\big(R \otimes_k S(\check{A})\big) \otimes_{S(\check{A})} k\ ,$$

where the structure morphisms of the two $S(\check{A})$-algebras involved in the tensor product are ϕ and the projection $S(\check{A}) \to k$ with kernel $S(\check{A})_+$. The last ring morphism is the one which corresponds to the k-rational point 0 in $\mathbf{A}(A)$. Therefore

$$\begin{aligned}\big(R \otimes_k S(\check{A})\big) \otimes_{S(\check{A})} k \;&=\; \big(R \otimes_k S(\check{A})\big) \otimes_{S(\check{A})} \big(S(A)/S(A)_+\big)\\ &=\; R \otimes_k S(\check{A})/\big(\phi(S(\check{A})_+)\big)\ ,\end{aligned}$$

where $\big(\phi(S(\check{A})_+)\big) = (\mathrm{im}\,\varphi)$ since the ideal $S(\check{A})_+$ is generated by the elements of $\check{A}$, which are just the elements of $S(\check{A})$ of degree 1. □

(10.3) Definition. *We define the* k*-scheme*

$$\mathcal{E}\big(\mathcal{W}^0(A)\big) \;:=\; \mathrm{Spec}\big(R \otimes_k S(\check{A})\big)/(\mathrm{im}\,\varphi) \;=\; \mathrm{Spec}\big(R \otimes_k S(\check{A})\big)/\big(\phi(S(\check{A})_+)\big)\ .$$

(10.4) Remark. Let $k'|k$ be any field extension. Then we have the identity for the k'-rational points

$$\mathcal{E}\big(\mathcal{W}^0(A)\big)(\mathrm{Spec}\,k') \;=\; \big\{(X,Y) \in \mathcal{W}(A_{k'}) \times A_{k'} : XY - \zeta YX = 0\big\}\ .$$

(10.5) Remark. The scheme $\mathcal{E}\big(\mathcal{W}^0(A)\big)$ is equipped with the two morphisms

$$\pi_0\colon \mathcal{E}\big(\mathcal{W}^0(A)\big) \;\longrightarrow\; \mathcal{W}^0(A)\ ,$$

induced by $R \to \big(R \otimes_k S(\check{A})\big)/(\mathrm{im}\,\varphi)$, $r \mapsto r \otimes 1$ and

$$\pi_1\colon \mathcal{E}\big(\mathcal{W}^0(A)\big) \;\longrightarrow\; \mathbf{A}(A)\ ,$$

induced by $S(\check{A}) \to \big(R \otimes_k S(\check{A})\big)/(\mathrm{im}\,\varphi)$, $s \mapsto 1 \otimes s$, which are on the rational points just the projections on the first and second factor.

Now we want to show that

$$\pi_0\colon \mathcal{E}\big(\mathcal{W}^0(A)\big) \;\longrightarrow\; \mathcal{W}^0(A)\ ,$$

is a vector bundle. For this aim, we will define a locally free sheaf $\mathscr{F}$ of $\mathcal{O}_{\mathcal{W}^0(A)}$-modules for which it is the vector bundle, associated to $\mathscr{F}$:

$$\mathcal{E}\big(\mathcal{W}^0(A)\big) \,= \mathbb{V}(\mathscr{F}) \,\big(:=\, \operatorname{Spec} S(\mathscr{F})\big) \,.$$

Let $\sigma\colon \mathcal{W}^0(A) \to \operatorname{Spec}(k)$ be the structure morphism and

$$\mathscr{M} \;:=\; \mathcal{O}_{\mathcal{W}^0(A)} \otimes_k \check{A} \;=\; \sigma^*(\check{A}) \,.$$

This is an $\mathcal{O}_{\mathcal{W}^0(A)}$-algebra, which is a free $\mathcal{O}_{\mathcal{W}^0(A)}$-module of rank n^2.
$\mathscr{M}$ is the sheaf of $\mathcal{O}_{\mathcal{W}^0(A)}$-modules associated to the R-module $M := R \otimes_k \check{A}$. Let $N := R \cdot \operatorname{im}(\varphi) \subseteq M$ be the R-submodule of M, generated by $\operatorname{im}(\varphi)$; or say

$$N \;:=\; R\cdot f_1 + R\cdot f_2 + \cdots + R\cdot f_{n^2} \,.$$

Let $\mathscr{N}$ be the sheaf of $\mathcal{O}_{\mathcal{W}^0(A)}$-modules associated to the R-module N.
$\mathscr{N}$ is a sheaf of $\mathcal{O}_{\mathcal{W}^0(A)}$-submodules of $\mathscr{M}$. We define the sheaf of $\mathcal{O}_{\mathcal{W}^0(A)}$-modules $\mathscr{F}$ to be

$$\mathscr{F} \;:=\; \mathscr{M}\,/\mathscr{N} \;;$$

or in other words: $\mathscr{F}$ is the sheaf of $\mathcal{O}_{\mathcal{W}^0(A)}$-modules associated to the R-module M/N. We are going to show first that M/N is a projective R-module of constant rank n.

(10.6) Lemma. *Let $\mathfrak{p} \in \operatorname{Spec}(R) = \mathcal{W}^0(A)$ be a prime ideal and $\kappa(\mathfrak{p})$ its residue field. Then the vectors $f_1, f_2, \ldots, f_{n^2} \in M \otimes_R \kappa(\mathfrak{p}) = \check{A}_{\kappa(\mathfrak{p})} \cong \kappa(\mathfrak{p})^{n^2}$ span an (n^2-n)-dimensional vector subspace.*

Proof: The elements $f_1, f_2, \ldots, f_{n^2} \in \check{A}_{\kappa(\mathfrak{p})}$ describe the equation $XY - \zeta YX = 0$ for the Kummer element $X = \mathfrak{p}$ in $\mathcal{W}(A_{\kappa(\mathfrak{p})}) \subseteq A_{\kappa(\mathfrak{p})}$. We have seen that the space of solutions of this set of linear equations in $A_{\kappa(\mathfrak{p})}$ is n-dimensional. Hence the linear equations $f_1, f_2, \ldots, f_{n^2}$ span a vector subspace of codimension n. □

(10.7) Lemma. *Let a, b and m be positive integers with $a \leq m$, T a topological space, $P \in T$ a point and Ω a field with some topology such that $\{0\}$ is closed in Ω.*
If for $j = 1, 2, \ldots, a+b$, the maps $F_j = (F_{ij})_{i=1,\ldots,m}\colon T \longrightarrow \Omega^m$ are continuous functions (Ω^m is equipped with the product topology) such that the rank of the $m\times(a+b)$ matrices

$$\big(F_1(Q), F_2(Q), \ldots, F_{a+b}(Q)\big) \;=\; \big(F_{ij}(Q)\big)_{\substack{i=1,\ldots,m\\ j=1,\ldots,a+b}}$$

for all $Q \in T$ and the $(m \times a)$ matrix

$$\big(F_1(P), F_2(P), \ldots, F_a(P)\big) \;=\; \big(F_{ij}(P)\big)_{\substack{i=1,\ldots,m\\ j=1,\ldots,a}}$$

is a, then there exists an open neighbourhood $U \subseteq T$ of P and continuous functions $\alpha_\mu^{(\nu)}\colon U \longrightarrow \Omega$ for $\mu = 1, \ldots, a$ and $\nu = a+1, \ldots, a+b$ such that

(i) *$\alpha_\mu^{(\nu)} \in \omega\big(F_{ij}|_U : i = 1, \ldots, m;\ j = 1, \ldots, a+b\big)$, where ω is the prime field of Ω, i.e., $\mathbb{Q}$ or $\mathbb{F}_p$; in other words, the $\alpha_\mu^{(\nu)}$ are quotients of polynomials in the $F_{ij}|_U$ with coefficients in $\mathbb{Z}$.*

(ii) *In U we have: $F_\nu = \alpha_1^{(\nu)} F_1 + \alpha_2^{(\nu)} F_2 + \cdots + \alpha_a^{(\nu)} F_a$ for $\nu = a+1, \ldots, a+b$.*

Proof: After re-indexing in i, we may assume that

$$\det\big(F_{ij}(P)\big)_{i,j=1,\dots,a} \neq 0$$

and hence there is an open neighbourhood $U \subseteq T$ of P with

$$\det\big(F_{ij}(Q)\big)_{i,j=1,\dots,a} \neq 0$$

for all $Q \in U$. Since for $\nu = a+1, \dots, a+b$, we have

$$\operatorname{rank}\big(F_1(Q), F_2(Q), \dots, F_a(Q)\big) = \operatorname{rank}\big(F_1(Q), F_2(Q), \dots, F_a(Q), F_\nu(Q)\big) = a \ ,$$

there are uniquely defined elements $\alpha_\mu^{(\nu)}(Q) \in \Omega$ for $\mu = 1, \dots, a$ such that

$$F_\nu(Q) = \alpha_1^{(\nu)}(Q)F_1(Q) + \alpha_2^{(\nu)}(Q)F_2(Q) + \dots + \alpha_a^{(\nu)}(Q)F_a(Q) \ .$$

In this way we get maps $\alpha_\mu^{(\nu)}\colon U \to \Omega$ with property (ii).
It remains to prove property (i). (Continuity is then for free!): By Cramer's Rule we have

$$\begin{aligned}\alpha_\mu^{(\nu)}(Q)\det\big(F_{ij}(Q)\big)_{i,j=1,\dots,a} &= \\ &= \det\big(F_{i1}(Q), \dots, F_{i,\mu-1}(Q), F_{i\nu}(Q), F_{i,\mu+1}(Q), \dots, F_{ia}(Q)\big)_{i=1,\dots,a} \ .\end{aligned}$$

On U the left determinant is invertible, hence we get property (i). □

Putting together the last two lemmas yields the

(10.8) Proposition. *Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be a maximal prime ideal. Then—if necessary, after re-indexing of the $f_1, f_2, \dots, f_{n^2}$—we have*

$$N_\mathfrak{p} = R_\mathfrak{p} \cdot f_1 + \dots + R_\mathfrak{p} \cdot f_{n^2} = R_\mathfrak{p} \cdot f_1 + \dots + R_\mathfrak{p} \cdot f_{n^2-n} \subseteq M_\mathfrak{p} \ .$$

Proof: We use lemma (10.7): Let $T = \mathcal{W}^0(A)(\operatorname{Spec}\Omega) = \operatorname{Hom}(R, \Omega)$ be the topological space (with the Zariski topology) of the geometric points of $\mathcal{W}^0(A)$, where Ω is an algebraic closure of k, and set $m := n^2$, $a := n^2 - n$, $b := n$. Using the identification (via the $\check{a}_i$'s) $\check{A} = k^{n^2} \subseteq \check{A}_\Omega = \Omega^{n^2}$ we define for $j = 1, \dots, n^2$

$$\begin{aligned} F_j = f_j\colon T &\longrightarrow M \otimes_R \Omega = \Omega^{n^2} \\ x &\longmapsto f_j(x) \ , \end{aligned}$$

where $f_j(x)$ is the image of f_j under the morphism $\mathrm{id}_M \otimes x\colon M = M \otimes_R R \to M \otimes_R \Omega$. Then (10.6) shows that the prerequisites of (10.7) hold true for every point $x \in T$ with $\mathfrak{p} = \ker(x)$. Note that, since R is an integral Jacobson ring, we can identify the elements of R and M with their induced functions on T.
Now, (i) tells us that the functions $\alpha_\mu^{(\nu)}$ are elements of $R_\mathfrak{p}$ and (ii) gives the claim, i.e., the equation (ii) first holds true for functions on T, but that implies that it holds for the elements of M. □

(10.9) Proposition. *The R-module M/N is projective of rank n, in other words: For all $\mathfrak{p} \in \operatorname{Spec}(R)$ the $R_\mathfrak{p}$-module $(M/N)_\mathfrak{p}$ is free of rank n.*

Proof: We only have to prove the second part for a maximal prime ideal $\mathfrak{p}$. We will show: $N_\mathfrak{p}$ is a free direct summand of $M_\mathfrak{p}$ of rank (n^2-n) with a free complementary summand. Then we are done. But this is now easy to show. By (10.8) the $R_\mathfrak{p}$-module $N_\mathfrak{p}$ is generated by some (n^2-n) elements $f_1, f_2, \ldots, f_{n^2-n}$ such that

$$f_1(\mathfrak{p}), f_2(\mathfrak{p}), \ldots, f_{n^2-n}(\mathfrak{p}) \in M(\mathfrak{p}) = M_\mathfrak{p} \otimes_{R_\mathfrak{p}} \kappa(\mathfrak{p})$$

are linearly independent. We complete this set of vectors by n vectors to a basis of $M(\mathfrak{p})$. We choose liftings $g_1, g_2, \ldots, g_n \in M_\mathfrak{p}$ of them. We know from Commutative Algebra that $f_1, f_2, \ldots, f_{n^2-n}, g_1, g_2, \ldots, g_n$ is a basis of the $R_\mathfrak{p}$-module $M_\mathfrak{p}$. Hence

$$M_\mathfrak{p} = N_\mathfrak{p} \oplus \langle g_1, g_2, \ldots, g_n \rangle = N_\mathfrak{p} \oplus R_\mathfrak{p} g_1 \oplus R_\mathfrak{p} g_2 \oplus \cdots \oplus R_\mathfrak{p} g_n \ .$$

Now we are done. □

(10.10) Corollary. *The sheaves $\mathscr{F}$, $\mathscr{M}$ and $\mathscr{N}$ of $\mathcal{O}_{\mathcal{W}^0(A)}$-modules are locally free of rank n, n^2 and (n^2-n) respectively.*

(10.11) Theorem. *The morphism*

$$\pi_0 \colon \mathcal{E}\big(\mathcal{W}^0(A)\big) \longrightarrow \mathcal{W}^0(A)$$

is a vector bundle of rank n; to be precise

$$\mathcal{E}\big(\mathcal{W}^0(A)\big) = \mathbb{V}(\mathscr{F}) \ \big(= \operatorname{Spec} S(\mathscr{F})\big) \ .$$

Proof: Observe

$$\begin{aligned}
\mathcal{E}\big(\mathcal{W}^0(A)\big) &= \operatorname{Spec}\big(R \otimes_k S(\check{A})\big)/(\operatorname{im}\varphi) \\
&= \operatorname{Spec}\big(R \otimes_k S(\check{A})\big)/(f_1, \ldots, f_n) \\
&= \operatorname{Spec}\big(S\big(R \otimes_k \check{A}/\langle f_1, \ldots, f_n\rangle\big)\big) \\
&= \operatorname{Spec}\big(S(M/N)\big) \\
&= \operatorname{Spec}\big(S(\mathscr{M}/\mathscr{N})\big) \\
&= \operatorname{Spec}\big(S(\mathscr{F})\big) \\
&= \mathbb{V}(\mathscr{F}) \ .
\end{aligned}$$

□

With (9.22) this theorem yields:

(10.12) Corollary. *The morphism*

$$\pi_0 \colon \mathcal{E}\big(\mathcal{W}^0(A)\big) \longrightarrow \mathcal{W}^0(A)$$

is smooth of relative dimension n, hence $\mathcal{E}\big(\mathcal{W}^0(A)\big)$ is a smooth integral k-scheme of the dimension $n^2+1 = \dim\big(\mathcal{W}^0(A)\big) + n$.

Now we take degree zero components of R, M and N:

$$\begin{aligned} R_0 &= \big(S(\check{A})/(\mathrm{Srd}_1, \ldots, \mathrm{Srd}_{n-1})\big)_{(\mathrm{Nrd})} \\ M_0 &= R_0 \otimes_k \check{A} \\ N_0 &= R_0 \cdot \mathrm{im}(\varphi) = R_0 \cdot f_1 + \cdots + R_0 \cdot f_{n^2} \ . \end{aligned}$$

Since $\mathrm{W}^0(A) = \mathrm{Spec}(R_0)$, the R_0-modules M_0 and N_0 induce their associated sheaves of $\mathcal{O}_{\mathrm{W}^0(A)}$-modules $\mathscr{M}_0$, $\mathscr{N}_0$ and $\mathscr{F}_0 := \mathscr{M}_0/\mathscr{N}_0$. Obviously, we have the same property:

(10.13) Remark. The sheaves $\mathscr{F}_0$, $\mathscr{M}_0$ and $\mathscr{N}_0$ of $\mathcal{O}_{\mathrm{W}^0(A)}$-modules are locally free of rank n, n^2 and $n^2 - n$ respectively.

(10.14) Definition. *We define the following affine and projective bundles of rank n over $\mathrm{W}^0(A)$*

$$\mathcal{E}\big(\mathrm{W}^0(A)\big) := \mathbb{V}(\mathscr{F}_0) \subseteq \mathrm{W}^0(A) \times_k \mathbf{A}(A)$$

and

$$\mathrm{E}\big(\mathrm{W}^0(A)\big) := \mathbb{P}(\mathscr{F}_0) \subseteq \mathrm{W}^0(A) \times_k \mathbf{P}(A) \ .$$

These bundles are just the once and twice projectivised versions of $\mathcal{E}\big(\mathcal{W}^0(A)\big)$, and like in the former case each of the k-schemes comes with two morphisms

$$\pi_0\colon \mathcal{E}\big(\mathrm{W}^0(A)\big) \longrightarrow \mathrm{W}^0(A) \quad \text{and} \quad \pi_0\colon \mathrm{E}\big(\mathrm{W}^0(A)\big) \longrightarrow \mathrm{W}^0(A)$$

which are the bundle morphisms, and

$$\pi_1\colon \mathcal{E}\big(\mathrm{W}^0(A)\big) \hookrightarrow \mathrm{W}^0(A) \times_k \mathbf{A}(A) \xrightarrow{\mathrm{pr}_2} \mathbf{A}(A)$$

as well as

$$\pi_1\colon \mathrm{E}\big(\mathrm{W}^0(A)\big) \hookrightarrow \mathrm{W}^0(A) \times_k \mathbf{P}(A) \xrightarrow{\mathrm{pr}_2} \mathbf{P}(A) \ .$$

The inclusions are induced by (applying the functor $\mathbb{V}$ to) the canonical epimorphism $\mathscr{M}_0 \twoheadrightarrow \mathscr{F}_0$ of sheaves of $\mathcal{O}_{\mathrm{W}^0(A)}$-modules.
Again from (10.13) follows:

(10.15) Proposition. *The morphisms*

$$\pi_0\colon \mathcal{E}\big(\mathrm{W}^0(A)\big) \longrightarrow \mathrm{W}^0(A) \quad \text{and} \quad \pi_0\colon \mathrm{E}\big(\mathrm{W}^0(A)\big) \longrightarrow \mathrm{W}^0(A)$$

are smooth of relative dimension n and $(n-1)$ respectively.
Also $\mathcal{E}\big(\mathrm{W}^0(A)\big)$ and $\mathrm{E}\big(\mathrm{W}^0(A)\big)$ are smooth integral k-schemes of dimension

$$\dim \mathrm{W}^0(A) + n = n^2 \quad \text{and} \quad \dim \mathrm{W}^0(A) + (n-1) = n^2 - 1 \ .$$

For any field extension $k'|k$ we have the canonical identifications

$$\mathcal{E}\big(\mathrm{W}^0(A)\big)(\mathrm{Spec}\, k') = \big\{\big([X], Y\big) \in \mathrm{W}(A_{k'}) \times A_{k'} : XY - \zeta YX = 0\big\}$$

and (here with $\mathbb{P}A_{k'} = (A_{k'} - 0)/k'^*$)

$$\mathrm{E}\big(\mathrm{W}^0(A)\big)(\mathrm{Spec}\, k') = \big\{\big([X], [Y]\big) \in \mathrm{W}(A_{k'}) \times \mathbb{P}A_{k'} : XY - \zeta YX = 0\big\} \ .$$

We take the open subschemes of $\mathcal{E}\big(\mathcal{W}^0(A)\big)$ and $\mathrm{E}\big(\mathrm{W}^0(A)\big)$ of pairs of invertible elements (X, Y) and $\big([X], [Y]\big)$:

(10.16) Definition. *We define the open subschemes*

$$\mathcal{W}^1(A) \;:=\; \mathcal{E}\big(\mathcal{W}^0(A)\big) \cap \big(\mathcal{W}^0(A) \times_k D(\mathrm{Nrd})\big)$$

and

$$\mathrm{W}^1(A) \;:=\; \mathrm{E}\big(\mathrm{W}^0(A)\big) \cap \big(\mathrm{W}^0(A) \times_k D_+(\mathrm{Nrd})\big)\ .$$

(10.17) Remark. By virtue of (6.8) we also can write

$$\mathcal{W}^1(A) \;:=\; \mathcal{E}\big(\mathcal{W}^0(A)\big) \cap \big(\mathcal{W}^0(A) \times_k \mathcal{W}^0(A)\big)$$

and

$$\mathrm{W}^1(A) \;:=\; \mathrm{E}\big(\mathrm{W}^0(A)\big) \cap \big(\mathrm{W}^0(A) \times_k \mathrm{W}^0(A)\big)\ .$$

We still have the projection morphisms, induced by π_0:

$$\pi_0^1\colon \mathcal{W}^1(A) \longrightarrow \mathcal{W}^0(A) \quad \text{and} \quad \pi_0^1\colon \mathrm{W}^1(A) \longrightarrow \mathrm{W}^0(A)\ .$$

(10.18) Proposition. *The fibres of the morphisms*

$$\pi_0^1\colon \mathcal{W}^1(A) \longrightarrow \mathcal{W}^0(A) \quad \text{and} \quad \pi_0^1\colon \mathrm{W}^1(A) \longrightarrow \mathrm{W}^0(A)\ .$$

are non-empty, hence they have (full) dimension n and $n-1$ respectively, and they are dense in the corresponding fibres of $\pi_0\colon \mathcal{E}\big(\mathcal{W}^0(A)\big) \to \mathcal{W}^0(A)$ and $\pi_0\colon \mathrm{E}\big(\mathrm{W}^0(A)\big) \to \mathrm{W}^0(A)$.

Proof: One may assume that k is algebraically closed. Then the density and non-emptiness follows from the fact that for any Kummer element $X \in \mathcal{W}(A)$, one can find an invertible element $Y \in A$ which is in ζ-relation with X. All fibres are irreducible, since they are open subsets of vector spaces. □

(10.19) Theorem. *The morphisms*

$$\pi_0^1\colon \mathcal{W}^1(A) \longrightarrow \mathcal{W}^0(A) \quad \text{and} \quad \pi_0^1\colon \mathrm{W}^1(A) \longrightarrow \mathrm{W}^0(A)\ .$$

are smooth of relative dimension n and $n-1$ respectively. $\mathcal{W}^1(A)$ and $\mathrm{W}^1(A)$ are smooth integral schemes of dimension (n^2+1) and (n^2-1) respectively. For any field extension $k'|k$ we have the canonical identifications

$$\mathcal{W}^1(A)(\mathrm{Spec}\, k') \;=\; \{(X,Y) \in \mathcal{W}(A_{k'}) \times \mathcal{W}(A_{k'}) : XY - \zeta YX = 0\}$$

and

$$\mathrm{W}^1(A)(\mathrm{Spec}\, k') \;=\; \text{K-Chain}_1^{\zeta}(A_{k'})\ .$$

(10.20) Remark. Regarding (10.17) there are also morphisms

$$\pi_1^1\colon \mathcal{W}^1(A) \longrightarrow \mathcal{W}^0(A) \quad \text{and} \quad \pi_1^1\colon \mathrm{W}^1(A) \longrightarrow \mathrm{W}^0(A)$$

induced by the restriction of the morphisms

$$\pi_1\colon \mathcal{E}\big(\mathcal{W}^0(A)\big) \longrightarrow \mathbf{A}(A) \quad \text{and} \quad \pi_1\colon \mathrm{E}\big(\mathrm{W}^0(A)\big) \longrightarrow \mathbf{P}(A)$$

which then factorize through $\mathcal{W}^0(A)$ and $\mathrm{W}^0(A)$.

2. Construction of the Varieties of Chains

In the last subsection we constructed the k-schemes

$$\begin{aligned}\mathcal{E}^1(A) &:= \mathcal{E}\big(\mathcal{W}^0(A)\big) \subseteq \mathcal{W}^0(A) \times_k \mathbf{A}(A)\\ \mathrm{E}^1(A) &:= \mathrm{E}\big(\mathrm{W}^0(A)\big) \subseteq \mathrm{W}^0(A) \times_k \mathbf{P}(A)\\ \mathcal{W}^1(A) &\subseteq \mathcal{W}^0(A) \times_k \mathcal{W}^0(A)\\ \mathrm{W}^1(A) &\subseteq \mathrm{W}^0(A) \times_k \mathrm{W}^0(A)\ ,\end{aligned}$$

and all come with their projections π_0^1 and π_1^1 to their first and second factor. They represent chains in A of the length one (or better: pairs of elements in the relation $XY - \zeta YX = 0$).
Now we want to make the analogous construction for chains of higher length.
Again, ℓ denotes a positive integer. We are going to construct k-schemes

$$\begin{aligned}\mathcal{E}^\ell(A) &\subseteq \big(\mathcal{W}^0(A)\big)^\ell \times_k \mathbf{A}(A)\\ \mathrm{E}^\ell(A) &\subseteq \big(\mathrm{W}^0(A)\big)^\ell \times_k \mathbf{P}(A)\\ \mathcal{W}^\ell(A) &\subseteq \big(\mathcal{W}^0(A)\big)^{\ell+1}\\ \mathrm{W}^\ell(A) &\subseteq \big(\mathrm{W}^0(A)\big)^{\ell+1}\ ,\end{aligned}$$

together with the projections $\pi_0^\ell, \ldots, \pi_\ell^\ell$ to their $\ell+1$ factors, with the obvious properties. This will be done inductively.

(10.21) Definition. *Given the objects $\mathcal{E}^\ell(A)$, $\mathrm{E}^\ell(A)$, $\mathcal{W}^\ell(A)$ and $\mathrm{W}^\ell(A)$ with their projection morphisms $\pi_0^\ell, \ldots \pi_\ell^\ell$, the analogous objects for the index $(\ell+1)$ are defined in the following way:*

$$\begin{aligned}\mathcal{E}^{\ell+1}(A) &:= \mathcal{W}^\ell(A) \times_{\mathcal{W}^0(A)} \mathcal{E}^1(A)\\ \mathrm{E}^{\ell+1}(A) &:= \mathrm{W}^\ell(A) \times_{\mathrm{W}^0(A)} \mathrm{E}^1(A)\ ,\end{aligned}$$

i.e., the diagrams

$$\begin{array}{ccc}\mathcal{E}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathcal{E}^1(A)\\ \Big\downarrow{\scriptstyle (\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})} & & \Big\downarrow{\scriptstyle \pi_0^1}\\ \mathcal{W}^\ell(A) & \xrightarrow{\pi_\ell^\ell} & \mathcal{W}^0(A)\end{array}$$

and

$$\begin{array}{ccc}\mathrm{E}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathrm{E}^1(A)\\ \Big\downarrow{\scriptstyle (\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})} & & \Big\downarrow{\scriptstyle \pi_0^1}\\ \mathrm{W}^\ell(A) & \xrightarrow{\pi_\ell^\ell} & \mathrm{W}^0(A)\end{array}$$

are cartesian. They also explain the projection morphisms $\pi_0^{\ell+1}, \ldots, \pi_{\ell+1}^{\ell+1}$.
The k-schemes $\mathcal{W}^{\ell+1}(A)$ and $\mathrm{W}^{\ell+1}(A)$ are the open subschemes defined by

$$\begin{aligned}\mathcal{W}^{\ell+1}(A) &:= \mathcal{E}^{\ell+1}(A) \cap \big(\mathcal{W}^0(A)^{\ell+1} \times_k D(\mathrm{Nrd})\big)\\ \mathrm{W}^{\ell+1}(A) &:= \mathrm{E}^{\ell+1}(A) \cap \big(\mathrm{W}^0(A)^{\ell+1} \times_k D_+(\mathrm{Nrd})\big)\end{aligned}$$

together with the restrictions of the projection morphisms.

(10.22) Remark. The upper two diagrams are embedded in the cartesian diagrams

$$\begin{array}{ccc} \mathcal{W}^0(A)^{\ell+1} \times_k \mathbf{A}(A) & \xrightarrow{\mathrm{pr}_{\ell+1,\ell+2}} & \mathcal{W}^0(A) \times_k \mathbf{A}(A) \\ \downarrow & & \downarrow \\ \mathcal{W}^0(A)^{\ell+1} & \xrightarrow{\mathrm{pr}_\ell} & \mathcal{W}^0(A) \end{array}$$

and

$$\begin{array}{ccc} \mathrm{W}^0(A)^{\ell+1} \times_k \mathbf{P}(A) & \xrightarrow{\mathrm{pr}_{\ell+1,\ell+2}} & \mathrm{W}^0(A) \times_k \mathbf{P}(A) \\ \downarrow & & \downarrow \\ \mathrm{W}^0(A)^{\ell+1} & \xrightarrow{\mathrm{pr}_\ell} & \mathrm{W}^0(A)\,, \end{array}$$

where the vertical arrows are the obvious projections. We count the factors starting with zero!

(10.23) Remark. One can define the objects $\mathcal{W}^{\ell+1}(A)$ and $\mathrm{W}^{\ell+1}(A)$ by the following cartesian diagrams

$$\begin{array}{ccc} \mathcal{W}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathcal{W}^1(A) \\ {\scriptstyle (\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})}\downarrow & & \downarrow{\scriptstyle \pi_0^1} \\ \mathcal{W}^\ell(A) & \xrightarrow{\pi_\ell^\ell} & \mathcal{W}^0(A) \end{array}$$

and

$$\begin{array}{ccc} \mathrm{W}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathrm{W}^1(A) \\ {\scriptstyle (\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})}\downarrow & & \downarrow{\scriptstyle \pi_0^1} \\ \mathrm{W}^\ell(A) & \xrightarrow{\pi_\ell^\ell} & \mathrm{W}^0(A) \end{array}$$

This follows from the fact that the definition of the objects $\mathcal{W}^{\ell+1}(A)$ and $\mathrm{W}^{\ell+1}(A)$ is equivalent to saying that the diagrams

$$\begin{array}{ccc} \mathcal{W}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathcal{W}^1(A) \\ {\scriptstyle \mathrm{incl}}\downarrow & & \downarrow{\scriptstyle \mathrm{incl}} \\ \mathcal{E}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathcal{E}^1(A) \end{array}$$

and

$$\begin{array}{ccc} \mathrm{W}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathrm{W}^1(A) \\ {\scriptstyle \mathrm{incl}}\downarrow & & \downarrow{\scriptstyle \mathrm{incl}} \\ \mathrm{E}^{\ell+1}(A) & \xrightarrow{(\pi_\ell^{\ell+1}, \pi_{\ell+1}^{\ell+1})} & \mathrm{E}^1(A) \end{array}$$

are cartesian. Now we only have to compose these diagrams with the ones from (10.21).

(10.24) Remark. Like in (10.17), we can write

$$\begin{aligned} \mathcal{W}^{\ell+1}(A) &= \mathcal{E}^{\ell+1}(A) \cap \big(\mathcal{W}^0(A)\big)^{\ell+2} \\ \mathrm{W}^{\ell+1}(A) &= \mathrm{E}^{\ell+1}(A) \cap \big(\mathrm{W}^0(A)\big)^{\ell+2} \ , \end{aligned}$$

i.e., the last projections $\pi_{\ell+1}^{\ell+1}$ factorize through $\mathcal{W}^0(A) \hookrightarrow \mathbf{A}(A)$ and $\mathrm{W}^0(A) \hookrightarrow \mathbf{P}(A)$ respectively.
To see this, one just looks at the diagrams in (10.23) and uses (10.20).

(10.25) Remark. If we define

$$\mathscr{F}_{\mathcal{W}^\ell(A)} := (\pi_\ell^\ell)^*(\mathscr{F}) \quad \text{and} \quad \mathscr{F}_{\mathrm{W}^\ell(A)} := (\pi_\ell^\ell)^*(\mathscr{F}_0)$$

to be the pre-images of the $\mathcal{O}_{\mathcal{W}^0(A)}$-module $\mathscr{F}$ and the $\mathcal{O}_{\mathrm{W}^0(A)}$-module $\mathscr{F}_0$ under the morphisms $\pi_\ell^\ell\colon \mathcal{W}^\ell(A) \to \mathcal{W}^0(A)$ and $\pi_\ell^\ell\colon \mathrm{W}^\ell(A) \to \mathrm{W}^0(A)$, then one has directly

$$\mathcal{E}^{\ell+1}(A) = \mathbb{V}(\mathscr{F}_{\mathcal{W}^\ell(A)}) \quad \text{and} \quad \mathrm{E}^{\ell+1}(A) = \mathbb{P}(\mathscr{F}_{\mathcal{W}^\ell(A)}) \ .$$

The morphisms $\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1}$ are the old morphisms $\pi_0^\ell, \ldots, \pi_\ell^\ell$ composed with the bundle morphism.
And the new projection morphism $\pi_{\ell+1}^{\ell+1}$ is then given in the same way as in the remark after (10.14).

(10.26) Theorem. *The morphisms*

$$(\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})\colon \mathcal{E}^{\ell+1}(A) \longrightarrow \mathcal{W}^\ell(A) \quad \text{and} \quad (\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})\colon \mathrm{E}^{\ell+1}(A) \longrightarrow \mathrm{W}^\ell(A)$$

as well as

$$(\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})\colon \mathcal{W}^{\ell+1}(A) \longrightarrow \mathcal{W}^\ell(A) \quad \text{and} \quad (\pi_0^{\ell+1}, \ldots, \pi_\ell^{\ell+1})\colon \mathrm{W}^{\ell+1}(A) \longrightarrow \mathrm{W}^\ell(A)$$

are smooth of relative dimension n and $(n-1)$ respectively. Therefore $\mathcal{E}^\ell(A)$ and $\mathrm{E}^\ell(A)$ as well as the objects $\mathcal{W}^\ell(A)$ and $\mathrm{W}^\ell(A)$ are smooth integral k-schemes of dimension

$$n^2 + 1 + (\ell-1)\cdot n = (\ell+n-1)n+1 \quad \text{and} \quad n^2 - 1 + (\ell-1)(n-1) = (\ell+n)(n-1)$$

respectively.
For any field extension $k'|k$ we have the canonical identifications, induced by the morphisms $(\pi_0^\ell, \ldots, \pi_\ell^\ell)$:

$$\begin{aligned} \mathcal{W}^\ell(A)(\operatorname{Spec} k') &= \{(X_0, \ldots, X_\ell) \in \mathcal{W}(A_{k'})^{\ell+1} : X_{i-1}X_i - \zeta X_i X_{i-1} = 0;\ i = 1, \ldots, \ell\} \\ \mathrm{W}^\ell(A)(\operatorname{Spec} k') &= \text{K-Chain}_\ell^\zeta(A_{k'}) \ . \end{aligned}$$

Proof: The smoothness follows from the cartesian diagrams in (10.21) and (10.23), since it is stable under base extension. The dimension formulas follow by induction. □

3. Chains with Starting Point

Let $X \in \mathcal{W}(A)$ be a Kummer element, or equivalently a k-rational point

$$X\colon \operatorname{Spec}(k) \longrightarrow \mathcal{W}^0(A) \quad \text{and} \quad [X]\colon \operatorname{Spec}(k) \longrightarrow \mathrm{W}^0(A)\ .$$

(10.27) Definition. *We define the fibres*

$$\begin{aligned}
\mathcal{E}^\ell(X;A) &:= X \times_{\mathcal{W}^0(A)} \mathcal{E}^\ell(A) \\
\mathrm{E}^\ell([X];A) &:= [X] \times_{\mathrm{W}^0(A)} \mathrm{E}^\ell(A) \\
\mathcal{W}^\ell(X;A) &:= X \times_{\mathcal{W}^0(A)} \mathcal{W}^\ell(A) \\
\mathrm{W}^\ell([X];A) &:= [X] \times_{\mathrm{W}^0(A)} \mathrm{W}^\ell(A)\ ,
\end{aligned}$$

where the morphisms in the second factor of the product are the projections π_0^ℓ.

(10.28) Proposition. *The k-schemes $\mathcal{E}^\ell(X;A)$ and $\mathrm{E}^\ell([X];A)$ as well as $\mathcal{W}^\ell(X;A)$ and $\mathrm{W}^\ell([X];A)$ are smooth of dimension $(\ell\, n)$ and $\ell(n-1)$. For a field extension $k'|k$ we have the identification*

$$\mathrm{W}^\ell([X];A)(\operatorname{Spec} k') \;=\; \text{K-Chain}_\ell^\zeta([X],-;A)_{k'}\ .$$

Proof: Just note that the composition

$$\pi_0^\ell\colon \mathcal{E}^\ell(A) \longrightarrow \mathcal{W}^{\ell-1}(A) \longrightarrow \mathcal{W}^{\ell-2}(A) \longrightarrow \cdots \longrightarrow \mathcal{W}^0(A)$$

is smooth of relative dimension $(\ell\, n)$. Analogously for the other cases. □

(10.29) Remark. Like in (10.25) we can see that $\mathcal{E}^{\ell+1}(X;A)$ and $\mathrm{E}^{\ell+1}([X];A)$ are vector bundles over $\mathcal{W}^\ell(X;A)$ and $\mathrm{W}^\ell([X];A)$. Therefore, by induction one observes that all the schemes are irreducible, hence integral.

§ 11. The Topological Closure of $\mathrm{W}^1(A)$

We fix a field k and a positive integer $n \geq 2$ which is not divisible by the characteristic of k. Let A be a central simple k-algebra of degree n and $\zeta \in \mu_n = \mu_n(\bar{k})$ a primitive n-th root of unity. For simplicity we assume that k is algebraically closed.

The variety $\mathrm{W}^1(A)$ is given in $D_+(\mathrm{Nrd}) \times D_+(\mathrm{Nrd})$ ($\subseteq \mathbf{P}(A)^2$) by the homogeneous equation $XY - \zeta YX = 0$. We will show that its topological closure in $\mathbf{P}(A)^2$ is the subvariety of $\bar{\mathrm{W}}(A) \times \bar{\mathrm{W}}(A)$ which is given by the same equation.
This is by no means obvious: We have to show that, given elements $[X], [Y] \in \bar{\mathrm{W}}(A)$ with $XY - \zeta YX = 0$, there are elements $[Y'] \in \mathrm{W}(A)$ in any neighbourhood of $[Y]$ such that $XY' - \zeta Y'X = 0$. In order to achieve this, we need some linear algebra.

1. Some Linear Algebra

In this subsection n is allowed to be any positive integer, and k may be an arbitrary field, if we assume that all eigenvalues that appear already lie in k.

(11.1) Lemma. *Let $W = W_n \supseteq W_{n-1} \supseteq \cdots \supseteq W_0 = W_{-1} = 0$ be a finite dimensional filtered k-vector space. We set $\bar{W}_i := W_i/W_{i-1}$, $m_i := \dim_k W_i$ and $\bar{m}_i := \dim_k \bar{W}_i$ for $i = 0, \ldots, n$. Let $f \in \mathrm{End}_{\mathrm{filt}}(W)$ be an endomorphism of the filtered k-vector space W, i.e., $f(W_i) \subseteq W_i$ for all i, then we can make the following statement about the set of eigenvalues: If*

$$\dim_k W \;=\; \#\left(\bigcup_{i=1}^{n} \mathrm{EigVal}(f|_{\bar{W}_i})\right) \;,$$

—that means, if $\#\,\mathrm{EigVal}(f|_{\bar{W}_i}) = \bar{m}_i$ and the sets $\mathrm{EigVal}(f|_{\bar{W}_i})$ are disjoint—then

$$\mathrm{EigVal}(f) \;=\; \coprod_{i=1}^{n} \mathrm{EigVal}(f|_{\bar{W}_i}) \;.$$

is the disjoint sum. To be precise: For every eigenvector $\bar{v} \in \mathrm{EigVec}(f|_{\bar{W}_i}, \theta)$ for the eigenvalue θ (i.e., if $(f|_{\bar{W}_i} - \theta)v = 0$), there exists a lifting $v \in W_i$ of $\bar{v}$ such that $(f - \theta)v = 0$.

Proof: This is certainly true for $n = 1$.
By induction on n, we may assume that $\bar{v} \in \mathrm{EigVec}(f|_{\bar{W}_n}, \theta)$ and $\theta \in \mathrm{EigVal}(f|_{\bar{W}_n})$, i.e., $(f|_{\bar{W}_n} - \theta)\bar{v} = 0$. Let $v_1 \in W$ be any lifting of $\bar{v}$. Then

$$v_2 \;:=\; (f - \theta)v_1 \in W_{n-1} \;.$$

By induction $\theta \notin \mathrm{EigVal}(f|_{W_{n-1}})$, therefore $(f - \theta)|_{W_{n-1}}$ is an automorphism of W_{n-1}, and hence there is a $v_3 \in W_{n-1}$ such that

$$(f - \theta)v_3 \;=\; -v_2 \;.$$

For $v := v_1 + v_3$ we have

$$(f - \theta)v \;=\; 0 \;,$$

and v is a lifting of $\bar{v}$. □

§ 11. The topological closure of $\mathrm{W}^1(A)$

Now let V be an n-dimensional k-vector space. Fix an element $\lambda \in k^*$ and a non trivial nilpotent endomorphism $g \in \mathrm{End}_k(V)$, i.e., $g^n = 0$ and $g \neq 0$.
We set

$$U_\lambda \ := \ \{f \in \mathrm{End}_k(V) : f \circ g = \lambda \cdot g \circ f\} \ .$$

We will consider V as an R-module, where $R := k[t]/(t^n)$ and t acts on V as g.
Then g induces a filtration

$$V = V_n \supseteq V_{n-1} \supseteq \cdots \supseteq V_0 = V_{-1} = 0 \ ,$$

with $V_i := \ker(g^i)$ for $i = 0, 1, \ldots, n$. Moreover we take the R-module

$$W \ := \ V/tV \ = \ V/\operatorname{im}(g)$$

with its induced filtration

$$W = W_n \supseteq W_{n-1} \supseteq \cdots \supseteq W_0 = W_{-1} = 0 \ ,$$

where

$$W_i \ = \ (V_i + tV)/tV \ = \ V_i/(V_i \cap tV) \ = \ V_i/tV_{i+1} \ ;$$

note that $V_i \cap tV = tV_{i+1}$! Furthermore we set

$$n_i := \dim_k V_i \ , \ n := \dim_k V \ , \ m_i := \dim_k W_i \ , \ m := \dim_k W$$

and

$$\bar{W}_i := W_i/W_{i-1} \ , \ \bar{m}_i := \dim_k \bar{W}_i \ .$$

(11.2) Lemma. *We have the formula:* $n = \sum_{i=1}^{n} \bar{m}_i \cdot i$.

Proof: Writing the nilpotent g in its Jordan canonical form, one observes that, as R-module,

$$V \ \cong \ \bigoplus_{\nu=1}^{r} k[t]/(t^{l_\nu}) \ ,$$

$l_\nu \geq 1$ for all $\nu = 1, \ldots, r$. Therefore

$$V_i \ \cong \ \bigoplus_{\{\nu : l_\nu \leq i\}} k[t]/(t^{l_\nu}) \ \oplus \ \bigoplus_{\{\nu : l_\nu > i\}} t^{(l_\nu - i)} k[t]/(t^{l_\nu})$$

and thus

$$W_i \ = \ V_i/tV_{i+1} \ \cong \ \bigoplus_{\{\nu : l_\nu \leq i\}} k[t]/(t) \ = \ \bigoplus_{\{\nu : l_\nu \leq i\}} k \ .$$

Now it follows

$$\bar{m}_i \ = \ \#\{\nu : l_\nu = i\}$$

and

$$\sum_{i=1}^{n} \bar{m}_i \cdot i \ = \ \sum_{i=1}^{n} \#\{\nu : l_\nu = i\} \cdot i \ = \ \sum_{\nu=1}^{r} l_\nu \ = \ n \ .$$

Note that $\bar{m}_i$ is the number of the Jordan blocks of g of the size $i \times i$. □

In this situation let us fix an $f \in U_\lambda$. Then $f \in \mathrm{End}_{\mathrm{filt}}(V)$ and the induced endomorphism $f \in \mathrm{End}_{\mathrm{filt}}(W)$ respect the filtrations.
We further set

$$\mathrm{EigVal}(f|_{\bar{W}_i}) := \{\theta_{ij} : j = 1, \ldots, \epsilon(i)\}$$

with $\epsilon(i) := \#\,\mathrm{EigVal}(f|_{\bar{W}_i})$ and then

$$\widetilde{\mathrm{EigVal}}(f|_{\bar{W}_i}) := \{\theta_{ij}\lambda^\nu : j = 1, \ldots, \epsilon(i);\ \nu = 0, \ldots, i-1\} .$$

We know

$$\#\,\mathrm{EigVal}(f|_{\bar{W}_i}) \le \dim_k \bar{W}_i = \bar{m}_i$$

and therefore

$$\#\widetilde{\mathrm{EigVal}}(f|_{\bar{W}_i}) \le \dim_k \bar{W}_i = \bar{m}_i \cdot i .$$

(11.3) Proposition. *If $n = \#\big(\bigcup_{i=1}^n \widetilde{\mathrm{EigVal}}(f|_{\bar{W}_i})\big)$, then*

(i) $\mathrm{EigVal}(f) = \coprod_{i=1}^n \widetilde{\mathrm{EigVal}}(f|_{\bar{W}_i})$,

(ii) *For every eigenvalue $\theta \in \mathrm{EigVal}(f|_{\bar{W}_i})$ and eigenvector $\bar{v} \in \mathrm{EigVec}(f|_{\bar{W}_i}, \theta)$ for θ, there exists a lifting $v \in V_i$ of $\bar{v}$ such that $(f-\theta)v = 0$.*

Proof: (ii) implies (i), in the following way:
Let θ and v be as in (ii). Then $v \in V_i - V_{i-1}$, since $\bar{v} \neq 0$. Therefore the vectors $v, gv, g^2v, \ldots, g^{i-1}v$ are all non-zero, and for $\nu = 0, \ldots, i-1$,

$$(f - \lambda^\nu\theta)g^\nu v = g^\nu(\lambda^\nu f - \lambda^\nu\theta)v = g^\nu\lambda^\nu(f-\theta)v = 0 ,$$

hence

$$\bigcup_{i=1}^n \widetilde{\mathrm{EigVal}}(f|_{\bar{W}_i}) \subseteq \mathrm{EigVal}(f) .$$

Since the left hand side is already a set of order n, we have equality.
Because of (11.2) we know that this union is disjoint and more: All the sets

$$\mathrm{EigVal}(f|_{\bar{W}_i}) \cdot \lambda^\nu$$

for $i = 1, \ldots, n$ and $\nu = 0, \ldots, i-1$, are pairwise disjoint sets of order $\epsilon(i) = \bar{m}_i$.
Now we prove (ii):
Let $0 \le j < i$. From (11.1), applied to the space W_i/W_j, follows immediately

$$\mathrm{EigVal}(f|_{W_i/W_j}) = \coprod_{j+1 \le \nu \le i} \mathrm{EigVal}(f|_{\bar{W}_\nu}) . \tag{1}$$

Let $\bar{v} \in \mathrm{EigVec}(f|_{\bar{W}_i}, \theta)$ be an eigenvector to the eigenvalue $\theta := \theta_{ij} \in \mathrm{EigVal}(f|_{\bar{W}_i})$. By (11.1) this vector has a lifting

$$(v' \bmod tV_{i+1}) \in W_i = V_i/tV_{i+1} ,$$

with $v' \in V_i$, which is an eigenvector of $f|_{W_i}$ to the eigenvalue θ, i.e.,

$$(f-\theta)v' = tv'_{i+1} \tag{2}$$

for some $v'_{i+1} \in V_{i+1}$. Now, for every $q = 0, 1, 2, \ldots$, we are going to recursively construct a triple of vectors

$$v_{i+q} \in V_{i+q} \ , \ v'_{i+q+1} \in V_{i+q+1} \ , \ v''_q \in V_q$$

(one may read $V_p = V$ for $q > n$) in the following way: For $q = 0$ we set

$$v_i \ = \ v' \ , \ v'_{i+1} \text{ from above } , \ v'' \ = \ 0 \ .$$

For $q > 0$ we get them from the vectors for $q - 1$.
First we claim:

$$\frac{\theta}{\lambda^q} \ \notin \ \mathrm{EigVal}(f|_{W_{i+q}/W_q}) \ \overset{(1)}{=} \ \bigcup_{l=q+1}^{i+q} \mathrm{EigVal}(f|_{\bar{W}_l}) \ .$$

Otherwise for some l with $q \leq l - 1$,

$$\theta_{ij} \ = \ \theta \ = \ \theta_{l,j'}\lambda^q \ \in \ \mathrm{EigVal}(f|_{\bar{W}_l}) \cdot \lambda^q \subseteq \widetilde{\mathrm{EigVal}}(f|_{\bar{W}_l}) \ ,$$

which is a contradiction to the disjointness of the sets $\mathrm{EigVal}(f|_{\bar{W}_i})$ and $\mathrm{EigVal}(f|_{\bar{W}_l}) \cdot \lambda^q$: For $i \neq l$ this is clear, for $i = l$ observe that $0 < q \leq l - 1 = i - 1$.
Therefore $(f - \frac{\theta}{\lambda^q})|_{W_{i+q}/W_q}$ is an automorphism, and there is a $v_{i+q} \in V_{i+q}$ with

$$\lambda^q(f - \frac{\theta}{\lambda^q})v_{i+q} \ \equiv \ -v'_{i+q} \pmod{V_q + tV_{i+q+1}}$$

—note that $W_{i+q}/W_q = V_{i+q}/(V_q + tV_{i+q+1})$. So there are vectors $v'_{i+q+1} \in V_{i+q+1}$ and $v''_q \in V_q$ such that

$$(\lambda^q f - \theta)v_{i+q} + v'_{i+q} \ = \ v''_q + tv_{i+q+1} \ . \tag{3}$$

Now we set

$$v \ := \ v_i + tv_{i+1} + t^2 v_{i+2} + \cdots \in \ V_i \ ; \tag{4}$$

this sum is finite, it stops after at most n steps. We have

$$\begin{aligned}
(f - \theta)v \ &\overset{(4)}{=} \ (f - \theta)v_i + (f - \theta)tv_{i+1} + (f - \theta)t^2 v_{i+2} + \cdots \\
&= \ (f - \theta)v_i + t(\lambda f - \theta)v_{i+1} + t^2(\lambda^2 f - \theta)v_{i+2} + \ldots \\
&\overset{(3)}{=} \ (f - \theta)v_i + t(-v'_{i+1} + tv'_{i+2} + v''_1) + t^2(-v'_{i+2} + tv'_{i+3} + v''_2) + \cdots \\
&\overset{(2)}{=} \ tv'_{i+1} + t(-v'_{i+1} + tv'_{i+2} + v''_1) + t^2(-v'_{i+2} + tv'_{i+3} + v''_2) + \cdots \\
&= \ tv'_{i+1} - tv'_{i+1} + t^2 v'_{i+2} - t^2 v'_{i+2} + t^3 v'_{i+3} - \cdots \\
&= \ 0
\end{aligned}$$

and we are done. □

(11.4) Lemma. *The canonical map*

$$\varphi\colon U_\lambda \ \longrightarrow \ \mathrm{End}_{\mathrm{filt}}(W) \ \longrightarrow \ \bigoplus_{i=1}^{n} \mathrm{End}(\bar{W}_i)$$

is surjective.

Proof: We choose a basis $\{v_{ij\nu} : i = 1, \ldots, n;\ j = 1, \ldots, \bar{m}_i;\ \nu = 0, \ldots, i-1\}$ of V such that the associated matrix of g has Jordan canonical form.
The set $\{v_{ij0}, \ldots, v_{ij(i-1)}\}$ corresponds to a Jordan block (i.e., elementary Jordan matrix) of size $i \times i$. Setting $v_{iji} := 0$, we can write

$$g(v_{ij\nu}) \ = \ v_{ij(\nu+1)}$$

for $\nu = 0, \ldots, i-1$. We have

$$V_i \ = \ \bigoplus_{\substack{1 \le l \le n \\ j=1,\ldots,\bar{m}_l \\ \max\{l-i,0\} \le \nu \le l-1}} k \cdot v_{lj\nu} \ ,$$

and

$$W_i \ = \ \bigoplus_{\substack{1 \le l \le i \\ j=1,\ldots,\bar{m}_l}} k \cdot v_{lj0} \qquad \text{and} \qquad \bar{W}_i \ = \ \bigoplus_{j=1,\ldots,\bar{m}_i} k \cdot v_{ij0} \ .$$

Let now

$$\bar{f}_i \ = \ (y_{ij\beta})_{j,\beta=1,\ldots,\bar{m}_i} \in \mathrm{M}_{\bar{m}_i}(k) \ = \ \mathrm{End}(\bar{W}_i)$$

be any endomorphism of $\bar{W}_i$ for $i = 1, \ldots, n$, with respect to $\{v_{ij0} : j = 1, \ldots, \bar{m}_i\}$, the basis of $\bar{W}_i$ from above.
We define $f \in U_\lambda \subseteq \mathrm{M}_n(k)$ in the following way:

$$f(v_{ij\nu}) \ := \ \lambda^\nu \sum_{\beta=1}^{\bar{m}_i} y_{ij\beta} \cdot v_{i\beta\nu}$$

for $i = 1, \ldots, n,\ j = 1, \ldots, \bar{m}_i,\ \nu = 0, \ldots, i-1$. Then

$$f\big(g(v_{ij\nu})\big) \ = \ f(v_{ij(\nu+1)}) \ = \ \lambda^{\nu+1} \sum_{\beta=1}^{\bar{m}_i} y_{ij\beta} \cdot v_{i\beta(\nu+1)}$$

and

$$g\big(f(v_{ij\nu})\big) \ = \ g\left(\lambda^\nu \sum_{\beta=1}^{\bar{m}_i} y_{ij\beta} \cdot v_{i\beta\nu}\right) \ = \ \lambda^\nu \sum_{\beta=1}^{\bar{m}_i} y_{ij\beta} \cdot v_{i\beta(\nu+1)} \ ,$$

therefore $f \circ g = \lambda \cdot g \circ f$, i.e., $f \in U_\lambda$. Restricted to

$$\bar{W}_i \ = \ \bigoplus_{j=1}^{\bar{m}_i} k \cdot v_{ij0} \ .$$

we see

$$f(v_{ij0}) \ = \ \sum_{\beta=1}^{\bar{m}_i} y_{ij\beta} \cdot v_{i\beta0} \ = \ \bar{f}_i(v_{ij0}) \ .$$

Since the $\bar{f}_i$ were chosen arbitrarily we are done. □

(11.5) Lemma. *Let W be a k-vector space of dimension m, and let $f \in \mathrm{End}_k(W)$ be nilpotent. For any set of elements $\theta_1, \ldots, \theta_m \in k$, there exists an endomorphism $\tilde{f} \in \mathrm{End}_k(W)$ such that for any $\alpha \in k$*

$$\mathrm{EigVal}(f + \alpha\tilde{f}) \;=\; \{\alpha\theta_1, \ldots, \alpha\theta_m\} \;.$$

Proof: Let $v_1, \ldots, v_m \in W$ be a basis of W such that the matrix Y associated to f with respect to this basis is strictly (upper or lower) triangular, e.g., take the Jordan canonical form. Then we set for $\tilde{Y}$—the matrix representing $\tilde{f}$—the diagonal matrix with the entries $\theta_1, \ldots, \theta_m$. Then $Y + \alpha\tilde{Y}$ is a triangular matrix with the diagonal elements $\alpha\theta_1, \ldots, \alpha\theta_m$. □

Let again V be an n-dimensional k-vector space and g, V_i, $W_i, \ldots$ as above. We choose numbers $\theta_{ij} \in k^*$, $i = 1, \ldots, n$; $j = 1, \ldots, \bar{m}_i$ such that all the numbers $\theta_{ij}\lambda^\nu$ for $i = 1, \ldots, n$; $j = 1, \ldots, \bar{m}_i$; $\nu = 0, \ldots, i-1$, are pairwise distinct.

(11.6) Proposition. *Let $f \in \mathrm{End}_k(V)$ be nilpotent and $f \in U_\lambda$. Then there exists an $\tilde{f} \in U_\lambda$ such that*

$$f + \alpha\tilde{f} \in U_\lambda$$

for all $\alpha \in k$ and

$$\mathrm{EigVal}(f + \alpha\tilde{f}) \;=\; \{\alpha\theta_{ij}\lambda^\nu : i = 1, \ldots, n;\; j = 1, \ldots, \bar{m}_i;\; \nu = 0, \ldots, i-1\} \;.$$

Proof: Because of (11.3), it is enough to show that there is an $\tilde{f} \in U_\lambda$ such that

$$\mathrm{EigVal}\big((f + \alpha\tilde{f})|_{\bar{W}_i}\big) \;=\; \{\alpha\theta_{ij} : j = 1, \ldots, \bar{m}_i\} \;.$$

for $i = 1, \ldots, n$. By (11.5) we choose $\tilde{f}_i \in \mathrm{End}(\bar{W}_i)$ such that

$$\mathrm{EigVal}(f|_{\bar{W}_i} + \alpha\tilde{f}_i) \;=\; \{\alpha\theta_{ij} : j = 1, \ldots, \bar{m}_i\} \;.$$

Since the map φ in (11.4) is surjective we can find an element $\tilde{f} \in U_\lambda$ which maps to the tuple $(\tilde{f}_i)$. We know

$$\begin{aligned} \mathrm{EigVal}\big((f + \alpha\tilde{f})|_{\bar{W}_i}\big) \;&=\; \mathrm{EigVal}(f|_{\bar{W}_i} + \alpha\tilde{f}_i) \\ &=\; \{\alpha\theta_{ij} : j = 1, \ldots, \bar{m}_i\} \;. \end{aligned}$$

Therefore we are done. □

2. The Closure of $\mathrm{W}^1(A)$

In $\bar{\mathrm{W}}(A) \times \bar{\mathrm{W}}(A) \subseteq \mathbf{P}(A) \times \mathbf{P}(A)$ we have the closed set

$$\bar{\mathrm{W}}^1 \;:=\; \big\{\big([X],[Y]\big) \in \bar{\mathrm{W}}(A) \times \bar{\mathrm{W}}(A) : XY - \zeta YX = 0\big\} \;.$$

This set contains the open subset

$$\mathrm{W}^1 \;:=\; \big\{\big([X],[Y]\big) \in \mathrm{W}(A) \times \mathrm{W}(A) : XY - \zeta YX = 0\big\} \;.$$

(11.7) Theorem. *$\bar{\mathrm{W}}^1$ is the (Zariski) topological closure of W^1 in $\mathbf{P}(A)^2$.*

Proof: All we have to show is that W^1 is dense in $\bar{\mathrm{W}}^1$.
We first show that W^1 is dense in

$$Q := \left\{ \big([X],[Y]\big) \in \bar{\mathrm{W}}(A) \times \mathrm{W}(A) : XY - \zeta YX = 0 \right\} .$$

So let $\big([X],[Y]\big)$ be an element in Q. We may assume that $[X] \notin \mathrm{W}(A)$. Then take any $[\tilde{X}] \in \mathrm{W}(A)$ with $\tilde{X}Y - \zeta Y\tilde{X} = 0$; which always exists. Now

$$\big([X + \alpha\tilde{X}],[Y]\big) \in \mathrm{W}^1$$

for almost all $\alpha \in k^*$, since $\mathrm{Nrd}(X + \alpha\tilde{X}) \neq 0$ for almost all α. Therefore in any neighbourhood of $\big([X],[Y]\big)$ are elements of W^1.
Now we prove that Q is dense in $\bar{\mathrm{W}}^1$. Let $\big([X],[Y]\big) \in \bar{\mathrm{W}}^1$. We may assume that $[Y] \notin \mathrm{W}(A)$. For reasons of symmetry we may assume that also $[X] \notin \mathrm{W}(A)$, i.e., X and Y are nilpotent. Otherwise we had the former case with switched components.
We further assume $A = \mathrm{M}_n(k)$. In the situation of subsection 1., we set $V = k^n$, $\lambda = \zeta^{-1}$, $g = X$ and $f = Y$. Then $Y \in U_\lambda$. Because of (11.6) there exists for the case

$$\{\theta_{ij}\lambda^\nu\} = \{\zeta^0, \ldots, \zeta^{n-1}\}$$

—which is easily realized—a $\tilde{Y} \in U_\lambda$ such that

$$\mathrm{EigVal}(Y + \alpha\tilde{Y}) = \{\alpha\zeta^0, \ldots, \alpha\zeta^{n-1}\}$$

for all $\alpha \in k^*$, i.e., $Y + \alpha\tilde{Y} \in \mathrm{W}(A)$. So we may find a pair

$$\big([X],[Y + \alpha\tilde{Y}]\big) \in Q$$

in any neighbourhood of $\big([X],[Y]\big)$. □

Chapter V

Chain Equivalence for Algebras of Degree 2 and 3

Let k be a field and $n \geq 2$ a positive integer which is not divisible by the characteristic of k. Let A be a central simple k-algebra of degree n, and $\zeta \in \mu_n = \mu_n(\bar{k})$ denotes a primitive n-th root of unity. We assume that $\zeta \in k$.

If X and Y are Kummer elements of A, we are interested in the question if they are (ℓ, ζ, ν)-related for a $\nu \in (\mathbb{Z}/n\mathbb{Z})^*$ and a positive integer ℓ, i.e., if the set

$$\text{K-Chain}_\ell^\zeta\big([X], [Y^\nu]; A\big) \neq \emptyset$$

is non-empty for some ℓ and ν.
If we are interested in this question for generic $[X]$ and $[Y] \in \mathrm{W}^0(A)$, then we only have to consider the case $\nu = 1$. That means the following:
If we have shown—for some fixed ℓ and ζ—that $\text{K-Chain}_\ell^\zeta\big([X], [Y]; A\big) \neq \emptyset$ (or has a certain constant order c) for generic $[X]$ and $[Y] \in \mathrm{W}^0(A)$, then it is clear that $\text{K-Chain}_\ell^\zeta\big([X], [Y^\nu]; A\big) \neq \emptyset$ (or has the order c) for generic $[X]$ and $[Y] \in \mathrm{W}^0(A)$, since $[Y] \mapsto [Y^\nu]$ is an automorphism of $\mathrm{W}^0(A)$. Moreover we then can say, that for another primitive n-th root ζ' the set $\text{K-Chain}_\ell^{\zeta'}\big([X], [Y^\nu]; A\big) \neq \emptyset$ (or has the order c) for generic $[X]$ and $[Y] \in \mathrm{W}^0(A)$. This follows from (8.6).
We may formulate the question in the language of schemes:
Let ℓ be a positive integer. Is the morphism of projection to the first and last factor

$$(\pi_0^\ell, \pi_\ell^\ell)\colon \mathrm{W}^\ell(A) \longrightarrow \mathrm{W}^0(A) \times_k \mathrm{W}^0(A)$$

surjective on the k-rational points, or is it dominant? If yes, then how big are the fibres?
In (10.26) we saw

$$\dim \mathrm{W}^\ell(A) = (\ell + n)(n-1)$$

and from (9.22) we know

$$\dim \mathrm{W}^0(A) \times_k \mathrm{W}^0(A) = 2n(n-1)\ .$$

Hence for dominance we need at least $\ell \geq n$.

It is announced by M. Rost that for prime numbers n, the morphism (π_0^n, π_n^n) is dominant of degree prime to n.
We are going to show this for the cases $n = 2$ and 3; we even will show that the degree is actually 1 and 2 respectively.
It is clear that dominance and degree are independent under base change $k'|k$. So one may treat and prove the questions of degree and dominance in the case (n, ℓ) for just one special central simple k-algebra A and then automatically get the results for every central simple k'-algebra, where k' is any other field of the same characteristic as k. Especially one may consider the extreme cases of A being a division algebra or a matrix algebra.—Of course surjectivity depends on the base field and may change with it.

The group scheme $\mathrm{GL}_1(A)$ acts on the schemes $\mathrm{W}^\ell(A)$ and $\mathrm{W}^0(A) \times_k \mathrm{W}^0(A)$ by conjugation in every factor and the projection morphisms $\pi_0^\ell\colon \mathrm{W}^\ell(A) \to \mathrm{W}^0(A)$ as well as $\mathrm{pr}_1\colon \mathrm{W}^0(A) \times_k \mathrm{W}^0(A) \to \mathrm{W}^0(A)$ are $\mathrm{GL}_1(A)$-morphisms. Since $\mathrm{GL}_1(A)$ acts transitively on $\mathrm{W}^0(A)$ we may ask our questions in the following formulation: Is the morphism

$$\pi_\ell^\ell\colon \mathrm{W}^\ell([X]; A) \longrightarrow \mathrm{W}^0(A)$$

dominant and what is the degree (which is the same as the degree above)?

§ 12. The Case of Algebras of Degree 2

We fix a field k of characteristic $\neq 2$. Let A be a central simple k-algebra of degree 2 and $\zeta = -1$.

1. Chain Equivalence for $n = \ell = 2$

We are going to prove that (almost) any two Kummer elements $[X], [Y] \in \mathrm{W}(A)$ are connected by one chain of length two.
We will split up this problem into the two cases that A is a division algebra or a matrix algebra.

(12.1) Lemma. *For $[X]$ and $[X'] \in \mathrm{W}(A)$ the condition $XX' - X'X = 0$ implies $[X] = [X']$.*

Proof: X' commutes with X, therefore $X' \in k[X]$, i.e., $X' = \alpha X + \beta$, where $\alpha, \beta \in k$. But

$$0 \;=\; \mathrm{Trd}(X') \;=\; \mathrm{Trd}(\alpha X + \beta) \;=\; \mathrm{Trd}(\beta) \;=\; 2\beta\ ,$$

hence $X' = \alpha X$. □

(12.2) Notation. *For any central simple k-algebra A of (arbitrary) degree n, with characteristic of k not dividing n and any primitive n-th root ζ of unity we denote*

$$u(\zeta, [X]) \;:=\; u(\zeta, [X]; A) \;:=\; \{[Y] \in \mathrm{W}(A) : XY - \zeta YX = 0\}$$

for any $[X] \in \mathrm{W}(A)$. In other words

$$\{[X]\} \times u(\zeta, [X]) \;=\; \mathrm{W}^1([X]; A)(\mathrm{Spec}\, k)\ .$$

Now we first assume that A is a division algebra of degree 2.

(12.3) Proposition. *If A is a division algebra and $[X], [Y] \in \mathrm{W}(A)$ are Kummer elements, then $\text{K-Chain}_2^\zeta([X], [Y]; A) \neq \emptyset$. To be precise:*

$$\text{K-Chain}_2^\zeta([X], [Y]; A) \;=\; \begin{cases} \big\{\big([X], [XY - YX], [Y]\big)\big\}, & \text{if } [X] \neq [Y] \\ \{[X]\} \times u(\zeta, [X]) \times \{[Y]\}, & \text{if } [X] = [Y] \end{cases}$$

Proof: The second case is clear, since $\zeta = \zeta^{-1} = -1$; and $u(\zeta, [X]) \neq \emptyset$ because of (6.16). If $[X] \neq [Y]$, then by (12.1) the commutator $XY - YX \neq 0$ is invertible, and

we obviously have $X \xrightarrow{\zeta} (XY - YX) \xrightarrow{\zeta} Y$, e.g., $X(XY - YX) + (XY - YX)X = X^2Y - XYX + XYX - YX^2 = X^2Y - YX^2 = 0$.
In particular $[XY - YX] \in \mathrm{W}(A)$—cf. (6.8). All we have to show now is that there is only one $[Z] \in \mathrm{W}(A)$ with $X \xrightarrow{\zeta} Z \xrightarrow{\zeta} Y$. In this case, since $\zeta = \zeta^{-1}$, we have

$$[Z] \in u(\zeta, [X]) \cap u(\zeta, [Y])$$

and since $u(\zeta, [X])$ and $u(\zeta, [Y])$ are one-dimensional linear subspaces of $\mathbf{P}(A)$ they intersect in exactly one point or they are equal. But only the first case is true: Otherwise we got $k[X]Z = k[Y]Z$, hence $k[X] = k[Y]$. By (12.1) we had $[X] = [Y]$. □

Now we assume that A is a matrix algebra. First let $A = A_0 = \mathrm{M}_2(k)$

(12.4) Remark. From the definition of Kummer elements follows:

$$\mathcal{W}(A_0) = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a^2 + bc \neq 0 \right\} .$$

(12.5) Lemma. *For* $X_0 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *we have*

$$u(\zeta, [X_0]) = \left\{ \left[\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \right] : \beta\gamma \neq 0 \right\} .$$

Proof: Consider the equivalences

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in u(\zeta, [X_0]) \iff \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = - \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(k)$$
$$\iff \alpha = \delta = 0,\ \beta\gamma \neq 0 .$$

□

(12.6) Proposition. *Let* $X_0 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $Y = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \in \mathcal{W}(A_0)$ *be two Kummer elements. Then*

$$\text{K-Chain}_2^{\zeta}([X_0], [Y]; A_0) =$$
$$= \begin{cases} \{([X_0], [X_0Y - YX_0], [Y])\}, & \text{if } bc \neq 0 \\ \{[X_0]\} \times u(\zeta, [X_0]) \times \{[Y]\}, & \text{if } b = c = 0, \text{ i.e., } [X_0] = [Y] \\ \emptyset, & \text{if } (b \neq 0, c = 0) \text{ or } (b = 0, c \neq 0) . \end{cases}$$

Proof: Because of (12.5) we just have to solve the equation

$$\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} = - \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}$$

for $\gamma\beta \neq 0$. But this equation is equivalent to $\beta c + \gamma b = 0$.
If $b = c = 0$ all $\beta, \gamma \in k^*$ do the job.
If $cb \neq 0$, then $\frac{\beta}{\gamma} = \frac{b}{-c}$, which gives us the one solution.
If $(b \neq 0, c = 0)$ or $(b = 0, c \neq 0)$ the equation is not solvable for $\beta\gamma \neq 0$. □

Now let A be any algebra isomorphic to $A_0 = \mathrm{M}_2(k)$.

(12.7) Corollary. *Let $X, Y \in \mathrm{W}(A)$ be any Kummer elements. Then*

$$\text{K-Chain}_2^{\zeta}([X],[Y];A) = \\ = \begin{cases} \{([X],[XY-YX],[Y])\}, & \text{if } \det(XY-YX) \neq 0 \\ \{[X]\} \times u(\zeta,[X]) \times \{[Y]\}, & \text{if } XY-YX=0, \text{ i.e., } [X]=[Y] \\ \emptyset, & \text{otherwise} \end{cases}$$

Proof: The first two cases are clear. Note that the uniqueness in the first case can be proved after base field extension such that $[X]$ is conjugate to $[X_0]$. The last case may also be shown after base extension: Then we again may assume that $[X] = [X_0]$ and $Y = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \in \mathcal{W}(A)$. But the condition $\det(X_0Y - YX_0) = 0$ and $X_0Y - YX_0 \neq 0$ just means $(b \neq 0, c = 0)$ or $(b = 0, c \neq 0)$: Observe $X_0Y - YX_0 = \left(\begin{smallmatrix} 0 & -2b \\ 2c & 0 \end{smallmatrix}\right)$. □

2. The Geometric Point of View

In §9 and §10 we gave a description of $\mathrm{W}(A)$ and $\text{K-Chain}_2^{\zeta}(A)$ as the k-schemes $\mathrm{W}^0(A)$ and $\mathrm{W}^2(A)$.
The projection onto the first and last component

$$(\pi_0^2, \pi_2^2)\colon \mathrm{W}^2(A) \longrightarrow \mathrm{W}^0(A) \times_k \mathrm{W}^0(A)$$

is a morphism of k-schemes. In fact, we will show that it is—cum grano salis—a blowing up in the diagonal.

We assume that k is algebraically closed and $A = A_0 = \mathrm{M}_2(k)$ is a matrix algebra.

(12.8) Remark. Since $\bar{\mathrm{W}}(A)$ is the subvariety of $\mathbf{P}(A)$ given by the polynomial Trd, we can write

$$\bar{\mathrm{W}}(A) = \left\{ \left[\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \right] : (a,b,c) \neq (0,0,0) \right\} .$$

One can identify $\bar{\mathrm{W}}(A)$ with $\mathbb{P}_k^2$ via

$$\begin{aligned} \psi\colon \bar{\mathrm{W}}(A) &\xrightarrow{\sim} \mathbb{P}_k^2 \\ \left[\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \right] &\longmapsto (2a : b-c : b+c) \end{aligned}$$

or

$$\begin{aligned} \psi'\colon \bar{\mathrm{W}}(A) &\xrightarrow{\sim} \mathbb{P}_k^2 \\ \left[\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \right] &\longmapsto (2a : c-b : b+c) . \end{aligned}$$

The inverse of, e.g., ψ is given by:

$$\psi^{-1}(\alpha : \beta : \gamma) = \left[\begin{pmatrix} \frac{\alpha}{2} & \frac{\beta+\gamma}{2} \\ \frac{\gamma-\beta}{2} & -\frac{\alpha}{2} \end{pmatrix} \right] .$$

(12.9) Lemma. *The diagram*

$$\begin{array}{ccc} \big\{\big([X],[Y],[Z]\big) \in \bar{\mathrm{W}}(A)^3 : XY+YX=0, XZ+ZX=0\big\} & \xrightarrow{(\mathrm{pr}_1,\mathrm{pr}_3)} & \bar{\mathrm{W}}(A)\times\bar{\mathrm{W}}(A) \\ \varphi:=\psi\times\psi'\times\psi \big\downarrow \wr & & \wr \big\downarrow \psi\times\psi \\ B := \big\{\big([u],[v],[w]\big) \in (\mathbb{P}^2_k)^3 : v(u)=0, v(w)=0\big\} & \xrightarrow{p_{13}:=(\mathrm{pr}_1,\mathrm{pr}_3)} & \mathbb{P}^2_k\times\mathbb{P}^2_k \end{array}$$

is commutative with vertical isomorphisms. For $[v]=(v_0:v_1:v_2)$, $[u]=(u_0:u_1:u_2)$ *the expression* $v(u)=0$ *stands for* $v_0u_0+v_1u_1+v_2u_2=0$.

Proof: The relations $XY+YX=0$ and $YZ+ZY=0$ are transformed by φ into $v(u)=0$ and $v(w)=0$, where $[u]=\psi([X])$, $[v]=\psi'([Y])$ and $[w]=\psi([Z])$: Set $X=\left(\begin{smallmatrix} a & b \\ c & -a\end{smallmatrix}\right)$ and $Y=\left(\begin{smallmatrix} a' & b' \\ c' & -a'\end{smallmatrix}\right)$, then

$$\begin{aligned} XY+YX = \begin{pmatrix} 2aa'+bc'+cb' & 0 \\ 0 & 2aa'+bc'+cb' \end{pmatrix} &= 0 \\ \iff 4aa'+2bc'+2cb' &= 0 \\ \iff (2a)(2a')+(b-c)(c'-b')+(b+c)(b'+c') &= 0 \\ \iff v(u) &= 0\ . \end{aligned}$$

Analogous for the other relation. The rest is clear. □

The projection morphism $p_{13}\colon B \longrightarrow \mathbb{P}^2_k\times\mathbb{P}^2_k$ is the blowing up of $\mathbb{P}^2_k\times\mathbb{P}^2_k$ in its diagonal. In order to show that, we need some lemmas.

(12.10) Lemma. *The projection morphism onto the first and third factor*

$$p_{13} := (\mathrm{pr}_1,\mathrm{pr}_3)\colon \big\{(x,[y],z) \in \mathbb{A}^2_k\times\mathbb{P}^1_k\times\mathbb{A}^2_k : x\in[y]\big\} \longrightarrow \mathbb{A}^2_k\times\mathbb{A}^2_k$$

is the blowing up of $\mathbb{A}^2_k\times\mathbb{A}^2_k$ *in* $\{0\}\times\mathbb{A}^2_k$. *Here the relation* $x\in[y]$ *means* $y_1x_2=y_2x_1$ *for* $x=(x_1,x_2)$ *and* $[y]=(y_1:y_2)$.

Proof: By definition, the projection morphism on the first factor

$$\mathrm{pr}_1\colon \big\{(x,[y]) \in \mathbb{A}^2_k\times\mathbb{P}^1_k : x\in[y]\big\} \longrightarrow \mathbb{A}^2_k$$

is the blowing up of $\mathbb{A}^2_k$ in $\{0\}$, and the morphism of the claim is the base extension with $\mathbb{A}^2_k \longrightarrow \operatorname{Spec} k$. □

(12.11) Lemma. *The projection morphism onto the first and third factor*

$$p_{13}\colon \big\{(x,[y],z) \in \mathbb{A}^2_k\times\mathbb{P}^1_k\times\mathbb{A}^2_k : x-z\in[y]\big\} \longrightarrow \mathbb{A}^2_k\times\mathbb{A}^2_k$$

is the blowing up of $\mathbb{A}^2_k\times\mathbb{A}^2_k$ *in its diagonal.*

Proof: This follows from (12.10) by the following coordinate transformation

$$\begin{array}{ccc} \big\{(x,[y],z) \in \mathbb{A}^2_k\times\mathbb{P}^1_k\times\mathbb{A}^2_k : x-z\in[y]\big\} & \xrightarrow{p_{13}} & \mathbb{A}^2_k\times\mathbb{A}^2_k \\ \wr \big\downarrow & & \big\downarrow \wr \\ \big\{(u,[v],w) \in \mathbb{A}^2_k\times\mathbb{P}^1_k\times\mathbb{A}^2_k : u\in[v]\big\} & \xrightarrow{p_{13}} & \mathbb{A}^2_k\times\mathbb{A}^2_k\ , \end{array}$$

where the left vertical arrow is given by $(x,[y],z)\mapsto(u,[v],w)$, with $u=x-z$, $w=z$, $[v]=[y]$; and the right vertical arrow is given by $(x,z)\mapsto(u,w)$. with $u=x-z$, $w=z$. It induces an isomorphism between the diagonal of $\mathbb{A}^2_k\times\mathbb{A}^2_k$ and $\{0\}\times\mathbb{A}^2_k$. □

(12.12) Proposition. *The following morphism is an isomorphism*

$$\big\{(x,[y],z)\in\mathbb{A}^2_k\times\mathbb{P}^1_k\times\mathbb{A}^2_k : x-z\in[y]\big\}\ \xrightarrow{\sim}\ \big\{\big(u,[v],w\big)\in\mathbb{A}^2_k\times\mathbb{P}^2_k\times\mathbb{A}^2_k : v(u)=0, v(w)=0\big\}$$

defined by

$$\begin{aligned}\big((x_1,x_2),(y_1:y_2),(z_1,z_2)\big)&\longmapsto\big((x_1,x_2),(y_1z_2-y_2z_1:y_2:-y_1),(z_1,z_2)\big)\\ \big((u_1,u_2),(v_2:-v_1),(w_1,w_2)\big)&\longmapsto\big((u_1,u_2),(v_0:v_1:v_2),(w_1,w_2)\big)\end{aligned}$$

Here the expression $v(u)=0$ means $v_0+v_1u_1+v_2u_2=0$, where $[v]=(v_0:v_1:v_2)$ and $u=(u_1,u_2)$.

Proof: We only have to prove that the two mappings are well-defined, since they are (almost) obviously inverse to each other.
Let $x=(x_1,x_2)$, $z=(z_1,z_2)\in\mathbb{A}^2_k$ and $y=(y_1:y_2)\in\mathbb{P}^1_k$. Then

$$\begin{aligned}x-z\in[y]&\implies(x_1-z_1)y_2=y_1(x_2-z_2)\\&\implies(x_1-z_1)y_2+(x_2-z_2)(-y_1)=0\\&\implies v(u)=v_0+v_1u_1+v_2u_2=(y_1z_2-y_2z_1)+x_1y_2+x_2(-y_1)=0\end{aligned}$$

and

$$x-z\in[y]\implies v(w)=v_0+v_1w_1+v_2w_2=(y_1z_2-y_2z_1)+z_1y_2+z_2(-y_1)=0$$

for $u=x$, $[v]=(y_1z_2-y_2z_1:y_2:-y_1)$ and $w=z$.
On the other hand, let $u=(u_1,u_2)$, $w=(w_1,w_2)\in\mathbb{A}^2_k$ and $[v]=(v_0:v_1:v_2)\in\mathbb{P}^2_k$, then $v(u)=0$ and $v(w)=0$ implies

$$0=v(u)-v(w)=(u_1-w_1)v_1+(u_2-w_2)v_2$$

hence $(u_1-w_1)(-v_1)=(u_2-w_2)(v_2)$, i.e., $x-z\in[y]$ for $x=u$, $[y]=(v_2:-v_1)$ and $z=w$.
But it also implies $v_0=-v_1w_1-v_2w_2$ hence

$$\begin{aligned}v&=(v_0:v_1:v_2)\\&=(-v_1w_1-v_2w_2:v_1:v_2)\\&=(v_2w_2+v_1w_1:-v_1:v_2)\\&=(y_1z_2-y_2z_1:y_2:-y_1)\end{aligned}$$

what we need for proving that one composition of the two mappings is the identity. □

(12.13) Corollary. *The morphism p_{13}: $B\longrightarrow\mathbb{P}^2_k\times\mathbb{P}^2_k$ is the blowing up of $\mathbb{P}^2_k\times\mathbb{P}^2_k$ in its diagonal.*

Proof: All we have to show is that the map, restricted to the open sets of an open covering of $\mathbb{P}^2_k\times\mathbb{P}^2_k$ is a blowing up. Therefore we take a neighbourhood of a point

$([u],[w]) \in \mathbb{P}^2_k \times \mathbb{P}^2_k$, $[u] = (u_0 : u_1 : u_2)$, $[w] = (w_0 : w_1 : w_2)$. Applying a suitable unitary transformation on all factors $\mathbb{P}^2_k$ of the map p_{13}—it leaves the conditions $v(u) = v(w) = 0$ invariant—we may assume $u_0 = w_0 = 1$, and we consider the open neighbourhood

$$\begin{aligned} \mathbb{A}^2_k \times \mathbb{A}^2_k &\hookrightarrow \mathbb{P}^2_k \times \mathbb{P}^2_k \\ \big((u_1,u_2),(w_1,w_2)\big) &\longmapsto \big((1:u_1:u_2),(1:w_1:w_2)\big) \end{aligned}$$

the rest is just (12.12) with (12.11). □

Now we know with (12.9) that the map

$$p_{13}\colon \big\{\big([X],[Y],[Z]\big) \in \bar{\mathrm{W}}(A)^3 : XY + YX = 0, XZ + ZX = 0\big\} \longrightarrow \bar{\mathrm{W}}(A)^2$$

is a blowing up in the diagonal. Restricting (or taking base extension) to the open subscheme $\mathrm{W}(A) \times \mathrm{W}(A)$ we get the blowing up of $\mathrm{W}(A) \times \mathrm{W}(A)$ in its diagonal. Additionally, for any $[X_0] \in \mathrm{W}(A)$ we may take base extension with $\{[X_0]\} \times \mathrm{W}(A) \hookrightarrow \mathrm{W}(A) \times \mathrm{W}(A)$. In all we get

(12.14) Theorem. *The morphisms*

$$\Big\{\big([X],[Y],[Z]\big) \in \mathrm{W}(A) \times \bar{\mathrm{W}}(A) \times \mathrm{W}(A) : XY + YX = 0, XZ + ZX = 0\Big\} \xrightarrow{p_{13}} \mathrm{W}(A)^2$$

and

$$\Big\{\big([X],[Y],[Z]\big) \in \{[X_0]\} \times \bar{\mathrm{W}}(A) \times \mathrm{W}(A) : XY + YX = 0, XZ + ZX = 0\Big\} \xrightarrow{\mathrm{pr}_3} \mathrm{W}(A)$$

are blowing ups in the diagonal and in $\{[X_0]\}$ *respectively. The left varieties are the (Zariski) closures of* $\mathrm{W}^2(A)$ *in* $\mathrm{W}(A) \times \bar{\mathrm{W}}(A) \times \mathrm{W}(A)$ *and* $\mathrm{W}^2([X_0]; A)$ *in* $\bar{\mathrm{W}}(A) \times \mathrm{W}(A)$.

(12.15) Remark. Comparing (12.14) with (12.7) one observes that the pre-image (under pr_3) of the point $(b \neq 0, c = 0)$ and $(b = 0, c \neq 0)$ lie in $\big(\bar{\mathrm{W}}(A) - \mathrm{W}(A)\big) \times \mathrm{W}(A)$.

§ 13. The Case of Algebras of Degree 3 and Length 3

We fix a field of characteristic prime to 6 with a primitive 3-rd root $\zeta \in \mu_3(k)$ of unity lying in k. Let A be a central simple k-algebra of degree 3. We choose a ζ-pair (X, Y), i.e., $X, Y \in \mathcal{W}(A)$ such that $XY - \zeta YX = 0$.

1. Preliminaries and Conditions for Chains of Length 2

From (6.14) we know

$$A \;=\; \bigoplus_{0 \le i,j \le 2} k \cdot X^i Y^j$$

or, if we set $L := k[X] = k \oplus kX \oplus kX^2$,

$$A \;=\; L \oplus YL \oplus LY^{-1} \;.$$

(13.1) Notation. *Every element $T \in A$ has a unique presentation in the form*

$$T \;=\; \alpha + Y\beta + \gamma Y^{-1}$$

with $\alpha, \beta, \gamma \in L$. In this section, if we write T, we will always work with this presentation.
Y acts on L via conjugation:

$$\begin{aligned} \kappa_Y \colon L &\longrightarrow L \\ X &\longmapsto YXY^{-1} = \zeta^{-1}X \;. \end{aligned}$$

We denote this action by $\alpha \mapsto \overline{\alpha}$.

(13.2) Lemma. *For $\alpha \in L$, we have the equivalences*

$$\begin{array}{lllll} \alpha = \zeta\overline{\overline{\alpha}} & \Longleftrightarrow & \overline{\alpha} = \zeta\alpha & \Longleftrightarrow & \alpha \in kX^2 \;, \\ \overline{\overline{\alpha}} = \zeta\alpha & \Longleftrightarrow & \alpha = \zeta\overline{\alpha} & \Longleftrightarrow & \alpha \in kX \;, \\ & & \alpha = \overline{\alpha} & \Longleftrightarrow & \alpha \in k \;. \end{array}$$

Furthermore, if we write $\alpha = \alpha_0 + \alpha_1 X + \alpha_2 X^2$ for α_0, α_1, $\alpha_2 \in k$, then

$$\operatorname{Trd}(\alpha) \;=\; \operatorname{Trd}(\overline{\alpha}) \;=\; 3\alpha_0 \;.$$

Proof: Observe for $\alpha = \alpha_0 + \alpha_1 X + \alpha_2 X^2$ that $\overline{\alpha} = \alpha_0 + \zeta^{-1}\alpha_1 X + \zeta\alpha_2 X^2$. □

(13.3) Lemma. *For $T = \alpha + Y\beta + \gamma Y^{-1} \in A$ we have*

$$\begin{aligned} \operatorname{Trd}(T) \;&= \operatorname{Trd}(\alpha) \\ \operatorname{Trd}(T^2) \;&=\; \operatorname{Trd}(\alpha^2) + 2\operatorname{Trd}(\beta\gamma) \;. \end{aligned}$$

Proof: Note that X, Y, X^2, Y^2, YX, YX^2, XY^2, X^2Y^2 are Kummer elements (cf. (6.9)) hence their reduced trace is zero.

$$\begin{aligned}\mathrm{Trd}(T) &= \mathrm{Trd}(\alpha) + \mathrm{Trd}(Y\beta) + \mathrm{Trd}(\gamma Y^{-1}) \\ &= \mathrm{Trd}(\alpha)\ , \\ \mathrm{Trd}(T^2) &= \mathrm{Trd}(\alpha^2 + Y\beta\gamma Y^{-1} + \gamma Y^{-1} Y\beta) \\ &= \mathrm{Trd}(\alpha^2) + \mathrm{Trd}(\overline{\beta\gamma}) + \mathrm{Trd}(\gamma\beta) \\ &= \mathrm{Trd}(\alpha^2) + \mathrm{Trd}(\beta\gamma) + \mathrm{Trd}(\beta\gamma)\ .\end{aligned}$$

□

(13.4) Lemma. *For invertible $T \in A^*$, the following conditions are equivalent:*

(i) *$T \in \mathcal{W}(A)$ is a Kummer element,*

(ii) *$\mathrm{Trd}(\alpha) = 0$ and $\mathrm{Trd}(\alpha^2) = -2\,\mathrm{Trd}(\beta\gamma)$.*

Proof: Since the characteristic of k is prime to (3!) we know from (6.5) that (i) is equivalent to $\mathrm{Trd}(T) = \mathrm{Trd}(T^2) = 0$, and this is by (13.3) equivalent to (ii). □

Any Kummer element $X_1 \in \mathcal{W}(A)$ which is in ζ-relation with $X_0 := X$, i.e., $X_0X_1 - \zeta X_1X_0 = 0$, has the form $X_1 = Y\lambda$ for a $\lambda \in L^*$.
What are the conditions for an element $T \in A$ to be the third entry in a ζ-chain $([X_0], [X_1], [T]) \in \text{K-Chain}_2^{\zeta}(A)$?

(13.5) Lemma. *Let $X_1 := Y\lambda$ with $\lambda \in L$ and $T = \alpha + Y\beta + \gamma Y^{-1} \in A$, then the following conditions are equivalent:*

(i) *$X_1T - \zeta TX_1 = 0$*

(ii) *$\alpha\lambda = \zeta\overline{\overline{\alpha}}\lambda,\ \ \overline{\gamma}\overline{\lambda} = \zeta\gamma\lambda,\ \ \beta\overline{\overline{\lambda}} = \zeta\overline{\overline{\beta}}\lambda$.*

Proof: Observe

$$\begin{aligned}X_1T - \zeta TX_1 &= (Y\lambda)(\alpha + Y\beta + \gamma Y^{-1}) - \zeta(\alpha + Y\beta + \gamma Y^{-1})(Y\lambda) \\ &= Y\lambda\alpha + Y\lambda Y\beta + Y\lambda\gamma Y^{-1} - \zeta\alpha Y\lambda - \zeta Y\beta Y\lambda - \zeta\gamma\lambda \\ &= (\overline{\lambda}\overline{\gamma} - \zeta\gamma\lambda) + Y(\lambda\alpha - \zeta\overline{\overline{\alpha}}\lambda) + Y^2(\overline{\overline{\lambda}}\beta - \zeta\overline{\overline{\beta}}\lambda)\ .\end{aligned}$$

The coefficients are zero if and only if (i) holds. □

(13.6) Proposition. *If for $T = \alpha + Y\beta + \gamma Y^{-1} \in \mathcal{W}(A)$ the conditions*

(I) $\mathrm{Trd}(\alpha X^2) = 0$

(II) $\mathrm{Trd}(\beta\gamma X) = 0$

(III') $\beta \in L^*$ *or* (III'') $\gamma \in L^*$

hold, then there exists an $X_1 \in \mathcal{W}(A)$ with

$$X_0X_1 - \zeta X_1X_0 \ =\ 0 \quad \text{and} \quad X_1T - \zeta TX_1 \ =\ 0\ .$$

Proof: With (13.2) and (13.4) we know for $\alpha = \alpha_0 + \alpha_1 X + \alpha_2 X^2$ that $\alpha_0 = \frac{1}{3}\,\mathrm{Trd}(\alpha) = \frac{1}{3}\,\mathrm{Trd}(T) = 0$.

Condition (I) implies that $\alpha_1 = \frac{1}{3}\operatorname{Trd}(\alpha X^{-1}) = \operatorname{Trd}(\alpha X^2)/(3X^3) = 0$. Therefore $\alpha = \alpha_2 X^2$, hence $\alpha^2 = \alpha_2^2 X^4$ and $\operatorname{Trd}(\alpha^2) = 0$. Because of (13.4) we get $\operatorname{Trd}(\beta\gamma) = 0$. Together with condition (II) we get $\beta\gamma \in kX$.
Now we assume that (III') holds true: In this case set

$$\lambda := \beta X \quad \text{and} \quad X_1 := Y\lambda \in \mathcal{W}(A) \ ,$$

and then we have $X_0X_1 - \zeta X_1X_0 = 0$. Moreover the equations of (13.5)(ii) are valid:
From $\alpha = \alpha_2 X^2$ follows $\alpha = \zeta\overline{\overline{\alpha}}$, hence $\alpha\lambda = \zeta\overline{\overline{\alpha}}\lambda$.
$\frac{\lambda}{\beta} = X$ implies $\overline{\overline{\left(\frac{\lambda}{\beta}\right)}} = \zeta\left(\frac{\lambda}{\beta}\right)$, i.e., $\beta\overline{\overline{\lambda}} = \zeta\overline{\overline{\beta}}\lambda$.
Finally, $\beta\gamma \in kX$ shows $\lambda\gamma \in kX^2$, hence $\overline{\gamma}\overline{\lambda} = \zeta\gamma\lambda$.
If we assume (III'') then set

$$\lambda := \gamma^{-1}X^2 \quad \text{and} \quad X_1 := Y\lambda \in \mathcal{W}(A) \ ,$$

and the rest follows analogously. □

(13.7) Proposition. *Let $T = \alpha + Y\beta + \gamma Y^{-1} \in A$ such that there is an $X_1 \in \mathcal{W}(A)$ with*

$$X_0X_1 - \zeta X_1X_0 \ = \ 0 \quad \text{and} \quad X_1T - \zeta TX_1 \ = \ 0 \ .$$

Then

(I) $\operatorname{Trd}(\alpha X^2) = 0$, *i.e.*, $\alpha_1 = 0$

(II) $\operatorname{Trd}(\beta\gamma X) = 0$.

Proof: Because of the first Kummer relation, $X_1 = Y\lambda$ for a $\lambda \in L^*$. The situation, applied to (13.5), gives us

$$\alpha\lambda = \zeta\overline{\overline{\alpha}}\lambda, \ \overline{\gamma}\overline{\lambda} = \zeta\gamma\lambda, \ \beta\overline{\overline{\lambda}} = \zeta\overline{\overline{\beta}}\lambda \ .$$

Since λ is invertible, we can divide it out of the first equation and get $\alpha = \zeta\overline{\overline{\alpha}}$, hence by (13.2) $\alpha \in kX^2$, which implies (I).
Conjugating the third equation by Y we get $\overline{\beta}\lambda = \zeta\beta\overline{\lambda}$; multiplying this one with the second equation yields $\overline{\beta}\lambda\overline{\gamma}\overline{\lambda} = \zeta^2\beta\overline{\lambda}\gamma\lambda$, i.e., $\overline{\gamma}\overline{\beta} = \zeta^{-1}\gamma\beta$, hence we get $\gamma\beta \in kX$, which shows (II). □

(13.8) Proposition. *If for a $T = \alpha + Y\beta + \gamma Y^{-1} \in A^*$, with $\beta \in L^*$ or $\gamma \in L^*$, there exists an $X_1 \in \mathcal{W}(A)$ such that $([X_0], [X_1], [T]) \in \text{K-Chain}_2^{\zeta}(A)$, then $[X_1]$ is unique with this property.*

Proof: Any X_1 with $X_0 \xrightarrow{\zeta} X_1 \xrightarrow{\zeta} T$ has the form $X_1 = Y\lambda$ for a $\lambda \in L^*$. Then if $\beta \in L^*$, we know from the proof of (13.7) that $\overline{\overline{\left(\frac{\lambda}{\beta}\right)}} = \zeta\left(\frac{\lambda}{\beta}\right)$, i.e., $\frac{\lambda}{\beta} \in kX$ or $\lambda \in k\beta X$. But that means λ is unique up to scaling with an element of k^*. Therefore $[Y\lambda]$ is unique.
Analogous if $\gamma \in L^*$. □

(13.9) Example. There are exactly two chains of length three connecting $[X]$ with $[Y]$, namely

$$([X],[XY],[XY^2],[Y]) \quad \text{and} \quad ([X],[X^2Y],[XY],[Y]) \ .$$

Indeed, one get the chains by expanding the ζ-pair $([X],[Y])$ to $([X],[XY],[Y])$ and then again expanding in the first or second link—cf. (6.9). But they are the only ones: Let $([X],[X_1],[T],[Y]) \in \text{K-Chain}_3^{\zeta}(A)$ be a ζ-chain. Then we know for $T = \alpha + Y\beta + \gamma Y^{-1}$ from (6.10) that $T \in k[Y] \cdot X$, i.e.,

$$\alpha_0 = \alpha_2 = \beta_0 = \beta_2 = \gamma_0 = \gamma_2 = 0$$

or $T = \alpha_1 X + Y\beta_1 X + \gamma_1 XY^{-1}$. Furthermore we know from (13.7) that

(I) $\alpha_1 = 0$ and

(II) $\beta_1\gamma_1 = 0$.

This has two (projective) solutions $(\beta_1 = 0, \gamma_1 \neq 0)$ and $(\beta_1 \neq 0, \gamma_1 = 0)$ which lead to the two chains from above.

Note that the two solution-chains are already k-rational!

2. Existence of Connecting Chains of Length 3

Now we formulate the main theorem of this section which roughly says that almost any two Kummer elements can be connected by exactly two chains of length three.

(13.10) Theorem. *The morphism*

$$\pi_3^3\colon \mathrm{W}^3([X];A) \longrightarrow \mathrm{W}^0(A)$$

is a dominant morphism of degree 2. *In other words, there is an open non-empty, therefore dense, subset* $U \subseteq \mathrm{W}^0(A)$ *with the following property: If* $[Z] \in U$ *then* $(\pi_3^3)^{-1}([Z])$ *is a set of two points of degree (of the residue field extension) 1 or one point of degree 2.*

(13.11) Remark. We can formulate the theorem in the following way: Let $k'|k$ be a field extension in some algebraic closure $\bar{k}$ of k and let $[Z] \in \mathrm{W}(A_{k'}) \cap U$ be a k'-rational point, i.e., Kummer element, lying in U. Then there exists a field extension $l|k'$ of degree one or two such that

$$\text{K-Chain}_3^{\zeta}([X],[Z];A_l) \ = \ \text{K-Chain}_3^{\zeta}([X],[Z];A_{\bar{k}}) \ ,$$

and this is a set of two elements.

At the beginning of this chapter we mentioned that the degree of (π_3^3)—and therefore the whole theorem—does not depend on the special choice of the central simple algebra A (of degree 3) and the field k for a fixed characteristic. So for the proof we choose and fix A and k in a way such that A is a division algebra. (In particular k is not separably closed!)

§ 13. The case of algebras of degree 3 and length 3

Let

$$\begin{aligned} f_1\colon A &\longrightarrow k \\ T &\longmapsto \operatorname{Trd}(\alpha X^2) \end{aligned}$$

and

$$\begin{aligned} f_2\colon A &\longrightarrow k \\ T &\longmapsto \operatorname{Trd}(\beta\gamma X)\ , \end{aligned}$$

where $T = \alpha + Y\beta + \gamma Y^{-1}$.
For a 3-dimensional vector subspace $E \subseteq A$ we say that the system (f_1, f_2) is non degenerate in E if the following two conditions hold:

(i) $f_1|_E \neq 0$

(ii) The quadratic form f_2 restricted to $E \cap \ker(f_1)$ is non degenerate.

Note, that by (i) the vector space $E' := E \cap \ker(f_1)$ has dimension 2. Condition (ii) means that the quadratic form $q := f_2|_{E'}$ is non degenerate.

Let $\mathscr{A} := A \otimes_k \mathcal{O}_{\mathrm{W}^0(A)}$—so, $\mathscr{A}$ is the dual to the sheaf of $\mathcal{O}_{\mathrm{W}^0(A)}$-modules $\mathscr{M}$, which we know from §10—, and let $\mathscr{E}$ be the the $\mathcal{O}_{\mathrm{W}^0(A)}$-submodule of $\mathscr{A}$ of rank 3, which is given by the equation

$$TZ - \zeta ZT = 0 \quad \text{where } T \in A \text{ and } [Z] \in \mathrm{W}^0(A)\ .$$

—Cf. §10. There we can see that $\mathscr{E}$ is the dual of $\mathscr{F}$.

(13.12) Lemma. *There exists an open and dense subscheme $U \subseteq \mathrm{W}^0(A)$ such that for each point $u \in U$, the system (f_1, f_2) is non degenerate in $\mathscr{E}(u) = \mathscr{E}_u \otimes_{\mathcal{O}_{\mathrm{W}^0(A),u}} \kappa(u) \subseteq A \otimes_k \kappa(u)$.*

Proof: The non degeneracy condition is an open condition and the variety $\mathrm{W}^0(A)$ is irreducible by (9.22). Therefore it suffices to find one point $u \in \mathrm{W}^0(A)$ such that (f_1, f_2) is non degenerate in $\mathscr{E}(u)$.
We put $u = [Y]$. Then $\mathscr{E}(u) = X \cdot k[Y]$ and we have $T = \alpha_1 X + Y\beta_1 X + \gamma_1 XY^{-1}$ for $\alpha_1,\ \beta_1,\ \gamma_1 \in \kappa(u)$.
The system (f_1, f_2) restricted to $\mathscr{E}(u)$ is given by

$$(\alpha_1, \beta_1, \gamma_1) \longmapsto (3X^3\alpha_1, 3X^3\beta_1\gamma_1)$$

which is obviously non degenerate. □

Let $V \subseteq \mathbf{P}(A) \times_k \mathrm{W}^0(A)$ be the subscheme defined by the equations

(1) $TZ - \zeta ZT = 0$

(2) $\operatorname{Trd}(\alpha X^2) = 0$

(3) $\operatorname{Trd}(\beta\gamma X) = 0$.

where $[T] = [\alpha + Y\beta + \gamma Y^{-1}] \in \mathbf{P}(A)$ and $[Z] \in \mathrm{W}^0(A)$.
As we have seen in §10, equation (1) defines the 2-dimensional projective bundle $\mathbb{P}(\mathscr{F}) = \operatorname{Proj}\big(S(\check{\mathscr{E}})\big)$ on $\mathrm{W}^0(A)$. Thus V is the subscheme of $\mathbb{P}(\mathscr{F})$ given by the system (f_1, f_2).
Let $p\colon V \to \mathrm{W}^0(A)$ be the restriction of the projection $\mathbf{P}(A) \times_k \mathrm{W}^0(A) \longrightarrow \mathrm{W}^0(A)$ and let $\eta \in \mathrm{W}^0(A)$ be the generic point of $\mathrm{W}^0(A)$, with residue field $F := \kappa(\eta)$ and $V_\eta = p^{-1}(\eta)$ the fiber over η.

§ 13. The case of algebras of degree 3 and length 3

(13.13) Proposition. *We have the following facts:*

(i) *One has $V_\eta = \mathrm{Spec}(K)$ where the F-algebra K is a separable extension of F of degree 2.*

(ii) *The F-algebra A_F is a division algebra.*

(iii) *If K is a field, the K-algebra A_K is a division algebra.*

Proof: (i) follows from (13.12).
For (ii) note that A is a division algebra and that $\mathrm{W}^0(A)$ has a smooth k-rational point, e.g., $[X]$ or $[Y]$.
(iii) follows since $[K : F] = 2$ is prime to the index of A. □

Let $S \subseteq \mathbf{P}(A) \times_k \mathrm{W}^0(A)$ be the closed subscheme given by the equations

$$\mathrm{Nrd}(\beta) \;=\; \mathrm{Nrd}(\gamma) \;=\; 0 \quad \text{where } [T] = [\alpha + Y\beta + \gamma Y^{-1}] \in \mathbf{P}(A)\ .$$

(13.14) Proposition. *$V_\eta \cap S = \emptyset$.*

Proof: Let $x \in V_\eta$ and let $H := \kappa(x)$ be the residue field. Thus $H = K$ if K is a field or $H = F$ if $K = F \oplus F$. The point $x \in V_\eta$ is of the form

$$\big([T_x], [Z_\eta]\big) \in \mathbf{P}(A)(\mathrm{Spec}\, H) \times \mathrm{W}^0(A)(\mathrm{Spec}\, F)$$

where $[Z_\eta] \in \mathrm{W}^0(A)(\mathrm{Spec}\, F)$ is the generic element, i.e., the F-rational point localized in the generic point η and $[T_x] = [\alpha + Y\beta + \gamma Y^{-1}]$ with α, β, $\gamma \in H[X]$.
If $x \in V_\eta \cap S$ then $\mathrm{Nrd}(\beta) = \mathrm{Nrd}(\gamma) = 0$. Since A_H is a division algebra by (13.13)(ii) and (iii), we must have even $\beta = \gamma = 0$. Further, since $\mathrm{Trd}(\alpha) = 0$ and $\mathrm{Trd}(\alpha X^2) = 0$ (the first equation holds, because [T] is a Kummer element and the second by the equation (2)) we have $[T_x] = [X^2]$.
But then

$$T_x Z_\eta \;=\; \zeta Z_\eta T_x$$

implies

$$X^2 Z_\eta \;=\; \zeta Z_\eta X^2\ .$$

This would mean that the generic element of $\mathrm{W}^0(A)$ stands in Kummer relation to X^2. This is a contradiction. □

Let

$$g := (\pi_2^3, \pi_3^3)\colon \mathrm{W}^3([X]; A) \;\longrightarrow\; \mathbf{P}(A) \times_k \mathbf{P}(A)\ .$$

By proposition (13.7) the image of g is contained in V. Therefore we have a commutative diagram

$$\begin{array}{ccc} \mathrm{W}^3([X]; A) & & \\ {\scriptstyle g}\downarrow & \searrow^{\pi_3^3} & \\ V & \xrightarrow{\;p\;} & \mathrm{W}^0(A)\ . \end{array}$$

By proposition (13.6) and (13.14) we have

$$V_\eta \subseteq \mathrm{im}(g)\ .$$

Hence there exists a point $y \in \mathrm{W}^3([X]; A)$ such that $g(y) \in V_\eta$, i.e., y maps under π_3^3 to the generic point of $\mathrm{W}^0(A)$.

Since $\dim \mathrm{W}^3([X]; A) = \dim \mathrm{W}^0(A)$, the point must be the generic point of $\mathrm{W}^3([X]; A)$. Hence

$$g^{-1}(V_\eta) \;=\; \{y\}$$

consists of only one point. It follows that

$$V_\eta \;=\; \{g(y)\}$$

is irreducible and $V_\eta = \mathrm{Spec}(K)$ where $K|F$ is a field extension. Moreover by proposition (13.8) the morphism, i.e., field extension, $\mathrm{Spec}(K) = \kappa\big(g(y)\big) \hookrightarrow \kappa(y)$ must be of degree one, hence an isomorphism. This proves our theorem.

§ 14. The Case of Algebras of Degree 3 and Length 4

In the last section we proved that almost any two Kummer elements can be connected by a chain of length 3, if necessary, after a base field extension of degree 2. For chains of length 4 this is true for any two Kummer elements and over the base field itself if A is a skew field.

We fix a field of characteristic prime to 3 with a primitive 3-rd root $\zeta \in \mu_3(k)$ of unity lying in k. Let A be a central simple k-algebra of degree 3.
Moreover, we assume that A is a division algebra.
We choose a ζ-pair (X, Y), i.e., $X, Y \in \mathcal{W}(A)$ such that $XY - \zeta YX = 0$. From above we know

$$A \;=\; L \oplus YL \oplus LY^{-1} \;,$$

with $L = k[X]$.

(14.1) Notation. *For any Kummer element $Z \in \mathcal{W}(A)$ we set*

$$e(\zeta, Z) := \{Z' \in A : ZZ' - \zeta Z'Z = 0\} \;.$$

For example

$$e(\zeta, X) \;=\; k[X]Y \;=\; Yk[X] \;=\; YL$$

and

$$e(\zeta^2, X) \;=\; k[X]Y^{-1} \;=\; Y^{-1}k[X] \;=\; LY^{-1} \;.$$

(14.2) Theorem. *If A is a division algebra then any two Kummer elements of A can be connected by a ζ-chain in A of length 4, i.e., the map induced by (π_0^4, π_4^4)*

$$\text{K-Chain}_4^{\zeta}(A) \;\longrightarrow\; \text{W}(A) \times \text{W}(A)$$

is surjective.

For completeness we reproduce the proof with minor changes given in M. Rost [RoCL].

Additionally to the elements X and Y, we take an arbitrary Kummer element $Z \in \mathcal{W}(A)$ and we will show that there exist invertible elements X_1, X_2, $X_3 \in A^* = A - \{0\}$ such that the following conditions hold:

(1) $X_1 \in e(\zeta, X)$
(2) $X_1X_2 - \zeta X_2X_1 = 0$
(3) $X_2X_3 - \zeta X_3X_2 = 0$
(4) $X_3 \in e(\zeta^2, Z)$
(5) $X_2 \in X^2k \oplus e(\zeta^2, X) = X^2k \oplus LY^{-1}$
(6) $X_3 \in e(\zeta, X) \oplus e(\zeta^2, X) = YL \oplus LY^{-1}$

(14.3) Remark. The conditions (1)–(4) just mean that

$$X \xrightarrow{\zeta} X_1 \xrightarrow{\zeta} X_2 \xrightarrow{\zeta} X_3 \xrightarrow{\zeta} Z$$

is a ζ-chain.

(14.4) Lemma. $\dim_k \big(e(\zeta^2, Z) \cap \big(e(\zeta, X) \oplus e(\zeta^2, X)\big)\big) \geq 1$.

Proof: This follows from

$$\dim_k e(\zeta^2, Z) = 3 \quad \text{and} \quad \dim_k \big(e(\zeta, X) \oplus e(\zeta^2, X)\big) = 6$$

and the fact that these vector spaces lie in the 8-dimensional vector subspace of the A of trace zero elements. Hence the vector spaces have non-trivial intersection. □

Now let X_3 be a non-zero element of $e(\zeta^2, Z) \cap \big(e(\zeta, X) \oplus e(\zeta^2, X)\big)$, i.e., the points (4) and (6) hold for X_3 and it remains to find X_1 and X_2 such that (1)–(3) and (5) are valid.
Now, X_3 has the form

$$X_3 \;=\; Y\mu' + \mu''Y^{-1}$$

for some μ', $\mu'' \in L$.

In two trivial cases it is easy to find the remaining elements.

Case I: If $\mu' = 0$, then $X_3 = \mu Y^{-1}$ for $\mu \in L^*$.
Then the elements

$$X_1 := X_3^{-1} = Y\mu^{-1} \quad \text{and} \quad X_2 := X^2$$

fulfill the remaining conditions. In fact we have:
$X_1 = Y\mu^{-1} \in YL = e(\zeta, X)$ hence (1),
$X_1 = Y\mu^{-1} \in YL = e(\zeta^{-1}, X^2) = e(\zeta^{-1}, X_2)$ hence (2),
$X_3 = \mu Y^{-1} \in LY^{-1} = e(\zeta, X^2)$ hence (3),
$X_2 \in kX^2$ hence (5).

Case II: If $\mu'' = 0$, then $X_3 = Y\mu$ for $\mu \in L^*$, hence $X_3 \in e(\zeta, X)$.
Then the elements

$$X_1 := X_3X = Y(\mu X) \quad \text{and} \quad X_2 := X_3^2X = X_3X_1$$

fulfill the remaining conditions. In fact:
$X_1 \in YL \in e(\zeta, X)$ hence (1),
$X_1X_2 = X_3XX_3^2X = \zeta X_3X_3XX_3X = \zeta X_2X_1$ hence (2),
$X_2X_3 = X_3^2XX_3 = \zeta X_3^2X_3X = \zeta X_3X_2$ hence (3),
$X_2 = Y\mu Y\mu X \in Y^2L = LY^{-1} = e(\zeta^2, X)$ hence (5).

For the rest we may assume that μ', $\mu'' \in L^*$. Since the only property of Y we need is $X \xrightarrow{\zeta} Y$, we may change Y to $(Y\mu'')$. Then we have

$$X_3 \;=\; Y\mu + Y^{-1}$$

for $\mu = \mu'\mu'' \in L^*$.

(14.5) Lemma. *Let $T = Y\mu + Y^{-1}$ for any $\mu = m_0 + m_1X + m_2X^2 \in L$ for $m_i \in k$. Furthermore let c_2 be the second coefficient of the reduced characteristic polynomial of T. Then $c_2 = -3m_0$.*

Proof: $\mathrm{Trd}(T) = \mathrm{Trd}(Y\mu) + \mathrm{Trd}(Y^{-1}) = 0$ and $\mathrm{Trd}(T^2) = 2\,\mathrm{Trd}(\mu) = 6m_0$—cf. (13.3). Since $2c_2 = \mathrm{Trd}(T)^2 - \mathrm{Trd}(T^2)$, it follows that $2c_2 = -6m_0$. This proves the claim for characteristic $\neq 2$. For characteristic 2, consider $c_2 = -3m_0$ as a polynomial identity in the variables m_i. It suffices to verify this identity for a standard ζ-pair in $\mathrm{M}_3(\mathbb{Z}[\zeta])$. This follows from the characteristic 0 case. □

This lemma gives us for $X_3 := T$

$$\mu = m_1X + m_2X^2 \quad \text{and} \quad X_3 = Y(m_1X + m_2X^2) + Y^{-1}$$

for some m_1, $m_2 \in k$.

Case III: If $m_1 = 0$, then $X_3 = m_2YX^2 + Y^{-1}$.
Then the elements

$$X_1 := Y \quad \text{and} \quad X_2 := (YX)^{-1} = X^{-1}Y^{-1}$$

fulfill the remaining points. In fact:
(1) is clear. $X_1X_2 = YX^{-1}Y^{-1} = \zeta X^{-1}YY^{-1} = \zeta X_2X_1$ hence (2). The point (3) follows from

$$\begin{aligned} X_2X_3 &= (X^{-1}Y^{-1})(m_2YX^2 + Y^{-1}) \\ &= m_2X + X^{-1}Y^{-2} \\ &= \zeta m_2YXY^{-1} + \zeta Y^{-1}X^{-1}Y^{-1} \\ &= \zeta X_3X_2\ . \end{aligned}$$

Point (5) is obvious since $X^{-1}Y^{-1} \in LY^{-1} \in e(\zeta^2, X)$.
Finally we have

Case IV: If $m_1 \neq 0$, let

$$b := Y^{-3} \in k^*,\ c := \zeta^{-1}m_1b/\,\mathrm{N}_{L|k}(\mu) \in k^*,\ \lambda := c\mu X \in L^*$$

and set

$$X_1 := Y\lambda \quad \text{and} \quad X_2 := X^2(1 + (Y\lambda)^{-1})\ .$$

With these settings, (1) and (5) are obvious, and (2) is easily seen:
$X \xrightarrow{\zeta} Y\lambda$, i.e., $Y\lambda \xrightarrow{\zeta} X^2$ and therefore $e(\zeta, Y\lambda) = X^2k[(Y\lambda)]$.
It remains to verify (3):

$$X^2(1 + (Y\lambda)^{-1})(Y\mu + Y^{-1}) \;=\; \zeta(Y\mu + Y^{-1})X^2(1 + (Y\lambda)^{-1})\ .$$

This is equivalent to either of the following lines:

$$X^2(1 + (Y\lambda)^{-1})(Y\mu + Y^{-1}) \;= \zeta X^2(\zeta Y\mu + \zeta^2Y^{-1})(1 + (Y\lambda)^{-1})\ ,$$

i.e.,

$$(1 + (Y\lambda)^{-1})(Y\mu + Y^{-1}) \;= (\zeta^2Y\mu + Y^{-1})(1 + (Y\lambda)^{-1})\ ,$$

i.e.,

$$Y\mu + Y^{-1} + \lambda^{-1}\mu + \lambda^{-1}Y^{-2} \;=\; \zeta^2 Y\mu + Y^{-1} + \zeta^2 Y\mu\lambda^{-1}Y^{-1} + Y^{-1}\lambda^{-1}Y^{-1} \;.$$

We use the identity $\lambda^{-1}\mu = \zeta^2 Y\mu\lambda^{-1}Y^{-1}$, which follows from $\mu\lambda^{-1} = \lambda^{-1}\mu = c^{-1}X^{-1}$, in order to get the equivalent version

$$Y\mu + \lambda^{-1}Y^{-2} \;=\; \zeta^2 Y\mu + Y^{-1}\lambda^{-1}Y^{-1} \;.$$

Now with $Y^3 = b^{-1}$ and the notation $\overline{\lambda} := Y\lambda Y^{-1}$ from (13.1) we reformulate our problem to proving the equation

$$Y\mu + Y\overline{\overline{\lambda}}^{-1}b \;=\; \zeta^2 Y\mu + Yb\overline{\lambda}^{-1}$$

or equivalently

$$\mu + \overline{\overline{\lambda}}^{-1}b \;=\; \zeta^2\mu + b\overline{\lambda}^{-1} \;.$$

This immediately follows from

(14.6) Lemma. $\mu\,\overline{\lambda}\,\overline{\overline{\lambda}} + \overline{\lambda}\,b = \zeta^2\,\mu\,\overline{\lambda}\,\overline{\overline{\lambda}} + b\,\overline{\overline{\lambda}}$.

Proof: We have to show

$$(1-\zeta^2)\,\mu\,\overline{\lambda}\,\overline{\overline{\lambda}} \;=\; b\,(\overline{\overline{\lambda}} - \overline{\lambda}) \;.$$

Since

$$\mathrm{N}_{L|k}(\mu) = \mu\,\overline{\mu}\,\overline{\overline{\mu}} \quad \text{and} \quad \lambda = c\,\mu\,X$$

we have for the left hand side

$$\begin{aligned}(1-\zeta^2)\mu\,\overline{\lambda}\,\overline{\overline{\lambda}} \;&=\; (1-\zeta^2)\mu\,c\,\overline{\mu}\,\overline{X}\,c\,\overline{\overline{\mu}}\,\overline{\overline{X}} \\ &=\; (1-\zeta^2)\big(\mu\,\overline{\mu}\,\overline{\overline{\mu}}\,c\big)\,cX^2 \\ &=\; (1-\zeta^2)\zeta^2\,m_1\,b\,c\,X^2 \;.\end{aligned}$$

For the right hand side we have

$$\begin{aligned}b\,\big(\overline{\overline{\lambda}} - \overline{\lambda}\big) \;&=\; b\,\big(c\,\overline{\overline{\mu}}\,\overline{\overline{X}} - c\,\overline{\mu}\,\overline{X}\big) \\ &=\; b\,c\,X\,\big(\zeta\,\overline{\overline{\mu}} - \zeta^2\,\overline{\mu}\big) \\ &=\; b\,c\,X\,\big(\zeta(m_1\zeta X - m_2\zeta^2X^2) - \zeta^2(m_1\zeta^2X + m_2\zeta X^2)\big) \\ &=\; b\,c\,X\,(\zeta^2 m_1 X - \zeta m_1 X) \\ &=\; b\,c\,X\,(\zeta^2-\zeta)m_1X\end{aligned}$$

and we are done. □

Chapter VI
Relation to the Product Map of Tori

Out interest lies in the degree of the morphism

$$\pi_n^n\colon \mathrm{W}^n([X];A) \longrightarrow \mathrm{W}^0(A)$$

for a central simple k-algebra of degree n and $[X] \in \mathrm{W}(A)$, or equivalently in the degree of

$$(\pi_0^n, \pi_n^n)\colon \mathrm{W}^n(A) \longrightarrow \mathrm{W}^0(A) \times_k \mathrm{W}^0(A)\ .$$

Cf. chapter V. There we mentioned that it does not depend on k and the special form of A but only on n.

Now, in the whole chapter, k is assumed to be algebraically closed (and therefore $A \cong \mathrm{M}_n(k)$).

We are going to construct an explicit map which has—up to the factor (n^{n-1})—the same degree as π_n^n.
Later we will see that this morphism can be interpreted as a multiplication map of tori.

§ 15. A Covering of $\mathrm{W}(A)$

If we projectivise the variety GL_n in another way as the usual, namely regarding the column vectors in the matrices, we will see that we can get an n-fold covering of the variety of Kummer lines.

We fix an algebraically closed field k and a positive integer $n \geq 2$ not divisible by the characteristic of k. Let $\zeta \in \mu_n(k)$ be a primitive n-th root of unity and A a central simple k-algebra of degree n.
Furthermore we fix a ζ-pair (X,Y) in A, i.e., Kummer elements X, $Y \in \mathcal{W}(A)$ such that $XY - \zeta YX = 0$, and we set $L := k[X]$, $K := k[Y]$.
Let $D := R_{L|k}(\mathbb{G}_\mathrm{m})$ be the torus of L-units.

(15.1) Example. Since k is algebraically closed we have essentially only the one case: $A = \mathrm{M}_n(k)$, $X = X_0(\zeta)$ and $Y = Y_0$. Then D is the torus of invertible diagonal matrices.

1. The Variety $\mathrm{GL}_1(A)/D$

The torus D acts on $\mathrm{GL}_1(A)$ by the right multiplication. Now we are going to divide out this action (i.e., subgroup) and fix the following

§ 15. A covering of $\mathrm{W}(A)$

(15.2) Notation. *The variety*

$$\mathrm{GL}_1(A)/D$$

is defined to be the units of A modulo the units of L. The canonical epimorphism is denoted by

$$\begin{aligned} \{\}\colon \mathrm{GL}_1(A) &\longrightarrow \mathrm{GL}_1(A)/D \\ v &\longmapsto \{v\} := vD \ . \end{aligned}$$

(15.3) Remark. In our standard case of (15.1) we easily see that $\mathrm{GL}_1(A)/D = \mathrm{GL}_{n,k}/D =: \mathrm{P}^n\mathrm{GL}_{n,k}$ is the open subvariety of $(\mathbb{P}_k^{n-1})^n = \mathbb{P}_k^{n-1} \times_k \cdots \times_k \mathbb{P}_k^{n-1}$, defined by the condition

$$([v_1], \ldots, [v_n]) \in \mathrm{P}^n\mathrm{GL}_{n,k} \quad \Longleftrightarrow \quad (v_1, \ldots, v_n) \in \mathrm{GL}_{n,k} \ .$$

The v_i's are column vectors!

Therefore we know

(15.4) Remark. $\mathrm{GL}_1(A)/D$ is a smooth k-variety of dimension $n(n-1)$.

There are several operations on $\mathrm{GL}_1(A)/D$:
The multiplication on $\mathrm{GL}_1(A)$ induces on $\mathrm{GL}_1(A)/D$ the left-action

$$\begin{aligned} \mathrm{GL}_1(A) \times \mathrm{GL}_1(A)/D &\longrightarrow \mathrm{GL}_1(A)/D \\ (g, \{v\}) &\longmapsto g\{v\} := \{gv\} \ . \end{aligned}$$

This action is transitive.
Another action is given by multiplying with Y:

(15.5) Lemma. *The right multiplication with Y induces a (right-)action of $\mathbb{Z}/n\mathbb{Z}$ on $\mathrm{GL}_1(A)/D$ given by*

$$\begin{aligned} \mathrm{GL}_1(A)/D \times (\mathbb{Z}/n\mathbb{Z}) &\longrightarrow \mathrm{GL}_1(A)/D \\ \big(\{v\}, (m \bmod n\mathbb{Z})\big) &\longmapsto \sigma^m\{v\} := \{vY^m\} \ . \end{aligned}$$

This action is fixed point free, especially it is faithful.

Proof: Since Y normalizes D, i.e., $DY = YD$, the action is well defined. If $\{v\}$ is a fixed point, i.e., $\{vY^m\} = \{v\} = \{v1_A\}$, then by the upper left-action we see that $\{Y^m\} = \{1_A\}$, i.e., $Y^m \in D$. But since $K \cap L$ we have $m \equiv 0 \,(\mathrm{mod}\, n)$. □

(15.6) Remark. These two actions respect each other, i.e., for $g \in \mathrm{GL}_1(A)$ and $m \in \mathbb{Z}$ we have

$$g\sigma^m\{v\} \ = \ \{gvY^m\} \ = \ \sigma^m g\{v\} \ ,$$

(15.7) Example. In our standard situation of (15.1) one has

$$\sigma^m([v_1], \ldots, [v_n]) \ = \ ([v_{1+m}], \ldots, [v_{n+m}]) \ = \ ([v_{\sigma^m(1)}], \ldots, [v_{\sigma^m(n)}])$$

for $m \in \mathbb{Z}$, $([v_1], \ldots, [v_n]) \in \mathrm{P}^n\mathrm{GL}_{n,k}$, and the indices are viewed modulo n. Further we view σ on the right hand side as the permutation $\sigma = (1\ 2\ \ldots\ n) \in S_n$.

This follows from

$$(v_1, \ldots, v_n) \cdot Y_0 \;=\; (v_2, \ldots, v_n, v_1)$$

in $\mathrm{GL}_n(k)$.

2. The Covering

In (6.3) we mentioned that every Kummer element (or better: Kummer line) of $\mathrm{M}_n(k)$ is conjugate to $[X_0(\zeta)]$, or

$$\begin{aligned} \kappa(X)\colon \mathrm{GL}_1(A) &\longrightarrow \mathrm{W}(A) \\ g &\longmapsto [gXg^{-1}] = [\kappa_g(X)] \end{aligned}$$

is a surjective morphism. In other words $\mathrm{GL}_1(A)$ acts transitively on $\mathrm{W}(A)$ by conjugation.
Since the elements of $\mathrm{GL}_1(A)$ which commute with X are exactly the elements of D, we immediately get the

(15.8) Claim. *The morphism $\kappa(X)\colon \mathrm{GL}_1(A) \to \mathrm{W}(A)$ of k-varieties induces the morphism*

$$\begin{aligned} M := M_X\colon \mathrm{GL}_1(A)/D &\longrightarrow \mathrm{W}(A) \\ \{v\} &\longmapsto M\{v\} := [vXv^{-1}]\ , \end{aligned}$$

such that $\kappa(X) = M \circ \{\}$. This morphism is surjective.

(15.9) Remark. For any $v \in \mathrm{GL}_1(A)$ we have $\mathrm{Nrd}(X) = \mathrm{Nrd}(vXv^{-1})$.

(15.10) Lemma. *For any v, $w \in \mathrm{GL}_1(A)$ the following conditions are equivalent*

(i) $vXv^{-1} = wXw^{-1}$

(ii) $\{v\} = \{w\}$.

In other words, the lifted morphism

$$\begin{aligned} \tilde{M}\colon \mathrm{GL}_1(A)/D &\longrightarrow \mathrm{GL}_1(A) \\ \{v\} &\longmapsto vXv^{-1} \end{aligned}$$

is a well defined morphism and it is an injective map.

Proof: $vXv^{-1} = wXw^{-1} \iff w^{-1}vX = Xw^{-1}v \iff w^{-1}v \in L.$ □

On $\mathrm{W}(A)$ we also have an action of $\mathrm{GL}_1(A)$, namely the conjugation. The morphism M respects the action of $\mathrm{GL}_1(A)$:

§ 15. A covering of $\mathrm{W}(A)$

(15.11) Lemma. *For any $g \in \mathrm{GL}_1(A)$ the diagram*

$$\begin{array}{ccc} \mathrm{GL}_1(A)/D & \xrightarrow{M} & \mathrm{W}(A) \\ {\scriptstyle g\cdot}\downarrow & & \downarrow{\scriptstyle \kappa_g} \\ \mathrm{GL}_1(A)/D & \xrightarrow{M} & \mathrm{W}(A) \end{array}$$

is commutative, i.e., M is $\mathrm{GL}_1(A)$-equivariant.

Proof: This is clear since for any $v \in \mathrm{GL}_1(A)$,

$$Mg\{v\} = M\{gv\} = [gvXv^{-1}g^{-1}] = \kappa_g[vXv^{-1}] = \kappa_g M\{v\} \ .$$

□

About the action of $\mathbb{Z}/n\mathbb{Z}$ on $\mathrm{GL}_1(A)/D$ we know the following

(15.12) Lemma. *For any $v \in \mathrm{GL}_1(A)$ and $m \in \mathbb{Z}$,*

$$\tilde{M}(\sigma^m\{v\}) \ = \ \zeta^{-m}\tilde{M}\{v\}$$

hence

$$M(\sigma^m\{v\}) \ = \ M\{v\} \ .$$

In other words M is $(\mathbb{Z}/n\mathbb{Z})$-invariant.

Proof: $\tilde{M}(\sigma^m\{v\}) = \tilde{M}\{vY^m\} = vY^mXY^{-m}v^{-1} = \zeta^{-m}vXv^{-1} = \zeta^{-m}\tilde{M}\{v\}$. □

Patching together these lemmas we get

(15.13) Proposition. *For $\{v\}$, $\{w\} \in \mathrm{GL}_n(A)/D$ the following conditions are equivalent*

(i) $M\{v\} = M\{w\}$

(ii) $\{v\} = \sigma^m\{w\}$ *for some $m \in \mathbb{Z}$.*

Then $(m \bmod n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$ is unique.

Proof: (i) is equivalent to $\tilde{M}\{v\} = \lambda\tilde{M}\{w\}$ for some $\lambda \in \mathbb{G}_{\mathrm{m},k}$. With remark (15.9) we see that this is equivalent to

$$\tilde{M}\{v\} \ = \ \zeta^{-m}\tilde{M}\{w\}$$

for some unique $(m \bmod n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$. By (15.12) this is equivalent to

$$\tilde{M}\{v\} \ = \ \tilde{M}\sigma^m\{w\}$$

and this is equivalent to (ii), by virtue of (15.10). □

(15.14) Theorem. *The action of* $(\mathbb{Z}/n\mathbb{Z})$ *on* $\mathrm{GL}_1(A)/D$ *induces free actions on the fibres of the morphism*

$$M = M_X\colon \mathrm{GL}_1(A)/D \longrightarrow \mathrm{W}(A)\ .$$

(15.15) Corollary. $\deg(M_X) = n$.

(15.16) Remark. We get

$$\dim \mathrm{W}(A) \;=\; \dim \mathrm{GL}_1(A)/D \;=\; n^2 - n\ .$$

Furthermore we get the morphism

$$\big(\mathrm{GL}_1(A)/D\big)/(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathrm{W}(A)$$

which is bijective. The two varieties are birational equivalent and since $\mathrm{GL}_1(A)$ acts transitively on both varieties—compatible with the morphism—, it is an isomorphism; which again shows smoothness.

(15.17) Example. In our case of (15.1), the morphism

$$M_{X_0(\zeta)}\colon \mathrm{P}^n\mathrm{GL}_{n,k} \longrightarrow \mathrm{W}(A)$$

can be interpreted in the following way: For $([v_1],\dots,[v_n]) \in \mathrm{P}^n\mathrm{GL}_{n,k}$ the element $\tilde{M}([v_1],\dots,[v_n]) \in \mathrm{GL}_{n,k}$ is the (unique) matrix with eigenvalues $\zeta^1,\dots,\zeta^n$ to the eigenvectors $v_1,\dots,v_n$ respectively.

§ 16. A Covering of Chain Varieties

By virtue of the covering $M = M_X\colon \mathrm{GL}_1(A)/D \to \mathrm{W}(A)$ we will also find a covering of the chain variety $\mathrm{W}^\ell([X]; A)$ for any positive integer ℓ.
In order to do that we first have to find out how the ζ-relation is reflected in $\mathrm{GL}_1(A)/D$.

We use the same assumptions as in §15. Furthermore we assume that $X^n = Y^n \in k^*$. In this case there exists by Skolem-Noether an element $\phi \in \mathrm{GL}_1(A) = A^*$ such that

$$\phi X \phi^{-1} \;=\; Y \quad \text{and} \quad \phi Y \phi^{-1} \;=\; X^{-1} \;.$$

Just take the automorphism of A which maps the ζ-pair (X, Y) to the ζ-pair (Y, X^{-1}). As a consequence we can write

$$Y = \tilde{M}\{\phi\} = \tilde{M}_X\{\phi\} \;.$$

(16.1) Example. In the situation of (15.1) take ϕ to be the matrix $(\zeta^{-ij})_{i,j=1,\ldots,n}$ as one can see in the proof of (3.7).

1. The Kummer Relation

(16.2) Lemma. *Let d_1, $d_2 \in D$, then the condition $\phi d_1 \phi^{-1} = d_2$, i.e., $\phi d_1 = d_2 \phi$ implies the condition $[d_1] = [d_2] = [1_A]$ in $\mathbf{P}(D) \subseteq \mathbf{P}(A)$.*

Proof: If $\phi d_1 \phi^{-1} = d_2$ then $d_1 \in L$ and $d_1 = \phi^{-1} d_2 \phi \in \phi^{-1} L \phi = K$. Since $L \cap K = k$, the claim follows. □

(16.3) Corollary. *For d_1, $d_2 \in D$, the following conditions are equivalent*

(i) $[d_1] = [d_2]$ *in* $\mathbf{P}(D)$
(ii) $\{d_1\phi\} = \{d_2\phi\}$
(iii) $\{v d_1 \phi\} = \{v d_2 \phi\}$ *for any* $v \in \mathrm{GL}_1(A)$.

Proof: The direction "(i)⇒(ii)" is clear; so is the equivalence of (ii) and (iii).
Now assume (ii). This means there exists a $d \in D$ with $d_1\phi = d_2\phi d$ or equivalently

$$d_2^{-1} d_1 \phi \;=\; \phi d$$

and this implies $[d_2^{-1} d_1] = [1_A]$, i.e., $[d_1] = [d_2]$. □

(16.4) Remark. The corollary (16.3) just says that for any fixed $v \in \mathrm{GL}_1(A)$ the morphism

$$\begin{aligned} \mathbf{P}(D) &\longrightarrow \mathrm{GL}_1(A)/D \\ [d] &\longmapsto \{v d \phi\} \end{aligned}$$

is injective.

(16.5) Lemma. *Let v, $w \in \mathrm{GL}_1(A)$. Then the following conditions are equivalent*

(i) $(\tilde{M}\{v\}, \tilde{M}\{w\})$ *is a ζ-pair*

(ii) $\{w\} = \{vd\phi\}$ *for some $d \in D$.*

In this case, $[d]$ is unique in $\mathbf{P}(D)$.

Proof: "(i)⇒(ii)": By (6.14) there is a $G \in \mathrm{GL}_1(A)$ such that

$$G\tilde{M}\{v\}G^{-1} = X \quad \text{and} \quad G\tilde{M}\{w\}G^{-1} = Y \ .$$

Therefore

$$\tilde{M}\{Gv\} = \tilde{M}\{1_A\} \quad \text{and} \quad \tilde{M}\{Gw\} = \tilde{M}\{\phi\} \ .$$

By (15.10) we get

$$\{Gv\} = \{1_A\} \quad \text{and} \quad \{Gw\} = \{\phi\} \ ,$$

i. e.,

$$Gv = d_1 \quad \text{and} \quad Gw = \phi d_2$$

for some d_1, $d_2 \in D$. Combining the two equations gives

$$w = G^{-1}\phi d_2 = vd_1^{-1}\phi d_2 \ ,$$

hence $\{w\} = \{vd\phi\}$ for $d := d_1^{-1}$.

"(ii)⇒(i)": Set $G := vd$. Then

$$\tilde{M}\{v\} = GXG^{-1} \quad \text{and} \quad \tilde{M}\{w\} = GYG^{-1} \ .$$

The first equation is clear, the second is

$$GYG^{-1} = G\tilde{M}\{\phi\}G^{-1} = \tilde{M}\{G\phi\} = \tilde{M}\{vd\phi\} = \tilde{M}\{w\} \ .$$

Uniqueness: $\{vd_1\phi\} = \{vd_2\phi\}$, then multiplying with v^{-1} we get $\{d_1\phi\} = \{d_2\phi\}$ and (16.3) yields the claim. □

The injective morphism

$$\begin{aligned} \hat{\omega}_v \colon \mathbf{P}(D) &\longrightarrow \mathrm{GL}_1(A)/D \\ [d] &\longmapsto \{vd\phi\} \end{aligned}$$

parametrizes all elements lying (via $\tilde{M}$) over Kummer elements which are in ζ-relation with $\tilde{M}\{v\}$.

There are two operations of $(\mathbb{Z}/n\mathbb{Z})$ on $\mathbf{P}(D)$:
The first one is given in the following way. Let $m \in \mathbb{Z}$, then

$$\begin{aligned} \mathbf{P}(D) &\longrightarrow \mathbf{P}(D) \\ [d] &\longmapsto [X^{-m}d] = [dX^{-m}] \end{aligned}$$

gives the action of $(m \bmod n\mathbb{Z})$ on $\mathbf{P}(D)$.

(16.6) Lemma. *For $m \in \mathbb{Z}$, the following diagram is commutative.*

$$\begin{array}{ccc} \mathbf{P}(D) & \xrightarrow{\hat{\omega}_v} & \mathrm{GL}_1(A)/D \\ \Big\downarrow & & \Big\downarrow{\scriptstyle \sigma^m} \\ bf\,\mathbf{P}(D) & \xrightarrow{\hat{\omega}_v} & \mathrm{GL}_1(A)/D \end{array}$$

where the left vertical arrow is the action of $(m \bmod n\mathbb{Z})$ on $\mathbf{P}(D)$.

Proof: $X^{-1}\phi = \phi Y$ implies $\{vdX^{-m}\phi\} = \{vd\phi Y^m\}$. □

The second action is given in the following way. Let $m \in \mathbb{Z}$ then

$$\begin{array}{rcl} \mathbf{P}(D) & \longrightarrow & \mathbf{P}(D) \\ [d] & \longmapsto & [Y^{-m}dY^m] \end{array}$$

gives the action of $(m \bmod n\mathbb{Z})$ on $\mathbf{P}(D)$.

(16.7) Lemma. *For $m \in \mathbb{Z}$, the following diagram is commutative.*

$$\begin{array}{ccc} \mathbf{P}(D) & \xrightarrow{\hat{\omega}_v} & \mathrm{GL}_1(A)/D \\ \Big\downarrow & & \Big\downarrow{\scriptstyle \mathrm{id}} \\ \mathbf{P}(D) & \xrightarrow{\hat{\omega}_{vY^m}} & \mathrm{GL}_1(A)/D \end{array}$$

where the left vertical arrow is the second action of $(m \bmod n\mathbb{Z})$ on $\mathbf{P}(D)$.

Proof: $\{vY^mY^{-m}dY^m\phi\} = \{vdY^m\phi\} = \{vd\phi X^m\} = \{vd\phi\}$. □

(16.8) Claim. *Both actions are compatible, i.e., they commute.*
Therefore we get an action of $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ on $\mathbf{P}(D)$ described by

$$\begin{array}{rcl} (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \times \mathbf{P}(D) & \longrightarrow & \mathbf{P}(D) \\ \big((m \bmod n\mathbb{Z}, p \bmod n\mathbb{Z}), [d]\big) & \longmapsto & {}^{(m,p)}[d] := [Y^{-m}X^{-p}dY^m] \end{array}$$

Proof:

$$\begin{aligned} {}^{(m,0)(0,p)}[d] &= [Y^{-m}X^{-p}dY^m] \\ &= [X^{-p}Y^{-m}dY^m\zeta^{-pm}] \\ &= {}^{(0,p)(m,0)}[d]\ . \end{aligned}$$

□

(16.9) Example. In the standard situation of (15.1) we get for $d = \mathrm{diag}(d_1, \ldots, d_n)$

$${}^{(m,p)}[\mathrm{diag}(d_1, \ldots, d_n)] = [\mathrm{diag}(\zeta^{-1p}d_{1+m}, \zeta^{-2p}d_{2+m}, \ldots, \zeta^{-np}d_{n+p})]\ .$$

We choose an element $v \in \mathrm{GL}_1(A)$, then the morphism

$$\begin{array}{rccc} \omega_v^{(1)}\colon \mathbf{P}(D) & \xrightarrow{\hat{\omega}_v} & \mathrm{GL}_1(A)/D & \xrightarrow{M} & \mathrm{W}(A) \\ [d] & \longmapsto & \{vd\phi\} & \longmapsto & M\{vd\phi\} \end{array}$$

has as its image the elements of $u(\zeta, M\{v\})$, the Kummer elements which are in a ζ-relation with $M\{v\}$. This follows from (16.5).

(16.10) Proposition. *The morphism*

$$\omega_v^{(1)}\colon \mathbf{P}(D) \longrightarrow u(\zeta, M\{v\})$$

is surjective and the first action of $(\mathbb{Z}/n\mathbb{Z})$ *on* $\mathbf{P}(D)$ *induces a free action an each fibre.*

Proof: The surjectivity follows from (16.5). The fact that the action induces actions on the fibres follows from (16.6) together with (15.12).
Free action: Let

$$\omega_v^{(1)}([d_1]) = \omega_v^{(1)}([d_2])$$

for $[d_1]$, $[d_2] \in \mathbf{P}(D)$, then

$$M\{vd_1\phi\} = M\{vd_2\phi\}\ .$$

With (15.13)

$$\{vd_1\phi\} = \sigma^m\{vd_2\phi\} = \{vd_2\phi Y^m\} = \{vd_2X^{-m}\phi\}$$

for unique $(m \bmod n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$.
Hence $[d_1] = [d_2X^{-m}]$ for the unique $(m \bmod n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$, by (16.3). □

2. The Covering

We consider the following morphism of k-varieties:

(16.11) Notation. *For any* $v \in \mathrm{GL}_1(A)$ *and any positive integer* ℓ *we define the morphism*

$$\begin{array}{rcl} \hat{\omega}_v^{(\ell)}\colon \mathbf{P}(D)^\ell = \mathbf{P}(D) \times \cdots \times \mathbf{P}(D) & \longrightarrow & \mathrm{GL}_1(A)/D \\ ([d_1], \ldots, [d_\ell]) & \longmapsto & \{vd_1\phi d_2\phi \cdots d_\ell\phi\}\ . \end{array}$$

There is an action of $(\mathbb{Z}/n\mathbb{Z})^\ell$ on $\mathbf{P}(D)^\ell$ given in the following way:

$$\begin{array}{rcl} (\mathbb{Z}/n\mathbb{Z})^\ell \times \mathbf{P}(D)^\ell & \longrightarrow & \mathbf{P}(D)^\ell \\ \big((\bar{a}_1, \ldots, \bar{a}_\ell), ([d_1], \ldots, [d_\ell])\big) & \longmapsto & \big({}^{(b_1,c_1)}[d_1], \ldots, {}^{(b_\ell,c_\ell)}[d_\ell]\big) \end{array}$$

where $b_i := a_{i-1}$ and $c_i := a_i + a_{i-2}$ for $i = 1, \ldots, \ell$ and $a_0 = a_{-1} = 0$.

(16.12) Remark. The action of $e_1 = (1, 0, \ldots, 0)$ on $([d_1], \ldots, [d_\ell])$ yields

$$([d_1X^{-1}], [Y^{-1}d_2Y], [X^{-1}d_3], [d_4], \ldots) \ .$$

The action of $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ on $([d_1], \ldots, [d_\ell])$ yields for $i \leq \ell - 2$

$$(\ldots, [d_{i-1}], [d_iX^{-1}], [Y^{-1}d_{i+1}Y], [X^{-1}d_{i+2}], [d_{i+3}], \ldots) \ .$$

The action of $e_{\ell-1} = (0, \ldots, 0, 1, 0)$ on $([d_1], \ldots, [d_\ell])$ yields

$$(\ldots, [d_{\ell-1}], [d_{\ell-1}X^{-1}], [Y^{-1}d_\ell Y]) \ .$$

The action of $e_\ell = (0, \ldots, 0, 1)$ on $([d_1], \ldots, [d_\ell])$ yields

$$(\ldots, [d_{\ell-1}], [d_\ell X^{-1}]) \ .$$

On $\mathrm{GL}_1(A)/D$ the group $(\mathbb{Z}/n\mathbb{Z})^\ell$ may act in the following way

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\ell \times \mathrm{GL}_1(A)/D &\longrightarrow \mathrm{GL}_1(A)/D \\ \big((\bar{a}_1, \ldots, \bar{a}_\ell), \{v\}\big) &\longmapsto \{vY^{a_\ell}\} = \sigma^{a_\ell}\{v\} \ . \end{aligned}$$

(16.13) Lemma. *With these actions, the morphism* $\hat{\omega}_v^{(\ell)}\colon \mathbf{P}(D)^\ell \longrightarrow \mathrm{GL}_1(A)/D$ *is* $(\mathbb{Z}/n\mathbb{Z})^\ell$*-equivariant.*

Proof: One observes that the action of $e_i = (0, \ldots, 1, \ldots, 0)$ commutes with $\hat{\omega}_v^{(\ell)}$: Note that for $i \leq \ell - 2$

$$d_iX^{-1}\phi Y^{-1}d_{i+1}Y\phi X^{-1}d_{i+2} \ = \ d_i\phi d_{i+1}\phi d_{i+2}$$

and

$$\{v'd_{\ell-1}X^{-1}\phi Y^{-1}d_\ell Y\phi\} \ = \ \{v'd_{\ell-1}\phi d_\ell\phi X\} \ = \ \{v'd_{\ell-1}\phi d_\ell\phi\}$$

for any $v' \in \mathrm{GL}_1(A)$. Further

$$\{v'd_\ell X^{-1}\phi\} \ = \ \{v'd_\ell\phi Y\} \ = \ \sigma\{v'd_\ell\phi\} \ .$$

We used $X^{-1}\phi Y^{-1} = \phi$ and $Y\phi X^{-1} = \phi$. □

(16.14) Notation. *Putting together* $\hat{\omega}_v^{(1)}, \ldots, \hat{\omega}_v^{(\ell)}$ *we define*

$$\begin{aligned} \hat{\Omega}_v^{(\ell)} := \big(\hat{\omega}_v^{(1)}, \ldots, \hat{\omega}_v^{(\ell)}\big)\colon \mathbf{P}(D)^\ell &\longrightarrow \big(\mathrm{GL}_1(A)/D\big)^\ell \\ \big([d_1], \ldots, [d_\ell]\big) &\longmapsto \big(\{vd_1\phi\}, \{vd_1\phi d_2\phi\}, \ldots, \{vd_1\phi \ldots d_\ell\phi\}\big) \end{aligned}$$

The group $(\mathbb{Z}/n\mathbb{Z})^\ell$ may act on $\big(\mathrm{GL}_1(A)/D\big)^\ell$ in the following way

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\ell \times \big(\mathrm{GL}_1(A)/D\big)^\ell &\longrightarrow \big(\mathrm{GL}_1(A)/D\big) \\ \big((\bar{a}_1, \ldots, \bar{a}_\ell), (\{v_1\}, \ldots, \{v_\ell\})\big) &\longmapsto \big(\sigma^{a_1}\{v_1\}, \ldots, \sigma^{a_\ell}\{v_\ell\}\big) \ . \end{aligned}$$

(16.15) Lemma. *With these actions, the morphism* $\hat{\Omega}_v^{(\ell)}\colon \mathbf{P}(D)^\ell \longrightarrow \big(\mathrm{GL}_1(A)/D\big)^\ell$ *is* $(\mathbb{Z}/n\mathbb{Z})^\ell$*-equivariant.*

Proof: This is a direct consequence of (16.13). □

(16.16) Proposition. *The morphism* $\hat{\Omega}_v^{(\ell)}\colon \mathbf{P}(D)^\ell \longrightarrow \big(\mathrm{GL}_1(A)/D\big)^\ell$ *is injective.*

Proof: We get this from (16.3) by induction:

$$\{vd_1\phi\} \;=\; \{vd_1'\phi\} \quad\Longrightarrow\quad [d_1] \;=\; [d_1']$$

then

$$\{vd_1\phi d_2\phi\} \;=\; \{vd_1'\phi d_2'\phi\} \;=\; \{vd_1\phi d_2'\phi\} \quad\Longrightarrow\quad [d_2] \;=\; [d_2']$$

and so on. □

Now we compose $\hat{\Omega}_v^{(\ell)}$ with (ℓ-times) the morphism $M = M_X\colon \mathrm{GL}_1(A)/D \to \mathrm{W}(A)$ in order to get

$$\Omega_v^{(\ell)} := M^\ell \circ \hat{\Omega}_v^{(\ell)}\colon \mathbf{P}(D)^\ell \longrightarrow \big\{M\{v\}\big\} \times \mathrm{W}(A)^\ell$$

(we just added a trivial first component) and by (16.5) we see that this morphism factorizes through

$$\mathrm{W}^\ell(M\{v\}; A) \hookrightarrow \big\{M\{v\}\big\} \times \mathrm{W}(A)^\ell \;.$$

(16.17) Theorem. *The morphism*

$$\begin{aligned} \Omega_v^{(\ell)}\colon \mathbf{P}(D)^\ell &\longrightarrow \mathrm{W}^\ell(M\{v\}; A) \\ \big([d_1], \ldots, [d_\ell]\big) &\longmapsto \big(M\{v\}, M\{vd_1\phi\}, M\{vd_1\phi d_2\phi\}, \ldots, M\{vd_1\phi\cdots d_\ell\phi\}\big) \end{aligned}$$

is surjective and the action of $(\mathbb{Z}/n\mathbb{Z})^\ell$ *on* $\mathbf{P}(D)^\ell$ *induces free actions on the every fibre of the map.*

Proof: The surjectivity is now easily shown:
Let $(M\{v\}, M\{v_1\}, \ldots, M\{v_\ell\}) \in \mathrm{W}^\ell(M\{v\}; A)$, then by (16.5) we see inductively that there exist $[d_1], \ldots, [d_\ell] \in \mathbf{P}(D)$ such that $\{v_i\} = \{v_{i-1}d_i\phi\}$ for $i = 1, \ldots, \ell$ with $v_0 := v$, and therefore

$$\Omega_v^{(\ell)}([d_1], \ldots, [d_\ell]) \;=\; \big(M\{v\}, M\{v_1\}, \ldots, M\{v_\ell\}\big) \;.$$

Now, the fibre of

$$M^\ell\colon \big(\mathrm{GL}_1(A)/D\big)^\ell \longrightarrow \mathrm{W}^\ell(M\{v\}; A)$$

over the given point is by (15.13) the orbit

$$\big\{\big(\sigma^{a_1}\{v_1\}, \ldots, \sigma^{a_\ell}\{v_\ell\}\big) : \bar{a}_1, \ldots, \bar{a}_\ell \in \mathbb{Z}/n\mathbb{Z}\big\} \;=\; (\mathbb{Z}/n\mathbb{Z})^\ell \cdot (\{v_1\}, \ldots, \{v_\ell\}) \;.$$

But this set of n^ℓ elements is exactly what we get if we let $(\mathbb{Z}/n\mathbb{Z})^\ell$ act on the tuple $([d_1], \ldots, [d_\ell]) \in \mathbf{P}(D)^\ell$ and then map it via $\hat{\Omega}_v^{(\ell)}$ to $\big(\mathrm{GL}_1(A)/D\big)^\ell$. This proves the claim. □

(16.18) Remark. As a consequence we get again statements like the irreducibility of $\mathrm{W}^\ell([X]; A)$ and the dimension formula: $\dim \mathrm{W}^\ell([X]; A) = \dim \mathbf{P}(D)^\ell = \ell(n-1)$.

Now we go back to our problem at the beginning, the case $\ell = n$.

We have the commutative diagram

$$\begin{array}{ccc} \mathbf{P}(D)^n & \xrightarrow{\Omega_v^{(n)}} & \mathrm{W}^n(M\{v\};A) \\ {\scriptstyle \hat{\omega}_v^{(n)}}\downarrow & & \downarrow{\scriptstyle \pi_n^n} \\ \mathrm{GL}_1(A)/D & \xrightarrow{M_X} & \mathrm{W}(A) \end{array}$$

therefore

$$\deg \pi_n^n \cdot \deg \Omega_v^{(n)} \;=\; \deg \hat{\omega}_v^{(n)} \cdot \deg M_X \;.$$

By (16.17) and (15.15) we get

$$\deg \pi_n^n \cdot n^n \;=\; \deg \hat{\omega}_v^{(n)} \cdot n$$

(16.19) Corollary. *For any $v \in \mathrm{GL}_1(A)$, the morphism*

$$\begin{aligned} \hat{\omega}_v^{(n)}\colon \mathbf{P}(D)^n &\longrightarrow \mathrm{GL}_1(A)/D \\ ([d_1],\ldots,[d_n]) &\longmapsto \{vd_1\phi d_2\phi\cdots d_n\phi\} \end{aligned}$$

has degree

$$\deg \hat{\omega}_v^{(n)} \;=\; n^{n-1} \cdot \deg \pi_n^n \;.$$

§ 17. Reformulation in the Product Map of Tori

First of all, we are going to "de-projectivise" the morphism $\hat{\omega}_v^{(n)}$ for $v = 1 = 1_A \in A^*$. Then we will reformulate the map a second time such that it can be interpreted as the product map of tori.

We keep the notations and assumptions of §16.

(17.1) Notation. *We denote with*

$$\bar{D} \;=\; D \times_{\mathbb{G}_{\mathrm{m}}} \cdots \times_{\mathbb{G}_{\mathrm{m}}} D$$

the quotient of D^{n+1} *by the group action*

$$\begin{aligned} \mathbb{G}_{\mathrm{m},k}^{\;n} \times D^{n+1} &\longrightarrow D^{n+1} \\ \big((t_1,\ldots,t_n),(d_1,\ldots,d_{n+1})\big) &\longmapsto (t_1,\ldots,t_n)\cdot(d_1,\ldots,d_{n+1}) := (d_1',\ldots,d_{n+1}') \end{aligned}$$

where

$$\begin{aligned} d_1' &= d_1 t_1^{-1} \\ d_i' &= t_{i-1} d_i t_i^{-1} \quad \text{for } i = 2,\ldots,n \\ d_{n+1}' &= t_n d_{n+1}\ . \end{aligned}$$

We define Ψ_n *to be the morphism*

$$\begin{aligned} \Psi_n\colon \bar{D} &\longrightarrow \mathrm{GL}_1(A) \\ (d_1,\ldots,d_{n+1}) &\longmapsto d_1\phi d_2\phi\cdots d_n\phi d_{n+1}\ . \end{aligned}$$

(17.2) Remark. The following diagram is commutative:

$$\begin{array}{ccc} \bar{D} & \xrightarrow{\Psi_n} & \mathrm{GL}_1(A) \\ {\scriptstyle p}\big\downarrow & & \big\downarrow{\scriptstyle \{\}} \\ \mathbf{P}(D)^n & \xrightarrow{\hat{\omega}_1^{(n)}} & \mathrm{GL}_1(A)/D \end{array}$$

where

$$\begin{aligned} p\colon \bar{D} &\longrightarrow \mathbf{P}(A)^n \\ (d_1,\ldots,d_{n+1}) &\longmapsto ([d_1],\ldots,[d_n])\ . \end{aligned}$$

Note that

$$p^{-1}([d_1],\ldots,[d_n]) \;=\; \big\{(d_1,\ldots,d_n,d) : d \in D\big\} \;=\; \big\{(d_1,\ldots,d_n)\big\} \times D\ .$$

D acts on $\bar{D}$ and $\mathrm{GL}_1(A)$ in the following way:

$$\begin{aligned} D \times \bar{D} &\longrightarrow \bar{D} \\ \big(d,(d_1,\ldots,d_n)\big) &\longmapsto (d_1,\ldots,d_n d) \end{aligned}$$

and

$$\begin{aligned} D \times \mathrm{GL}_1(A) &\longrightarrow \mathrm{GL}_1(A) \\ (d,g) &\longmapsto gd \end{aligned}$$

The following is clear:

§ 17. Reformulation in the product map of tori

(17.3) Lemma. *With these actions, the morphisms p and $\{\}$ are D-invariant and Ψ_n is D-equivariant. These actions induce free actions an all fibres of p and $\{\}$.*

From this lemma one instantaneously gets

(17.4) Proposition. $\deg \Psi_n \;=\; \deg \hat{\omega}_{1_A}^{(n)} \;=\; n^{n-1} \cdot \deg \pi_n^n$.

Since $\phi^2 X \phi^{-2} = X^{-1}$, conjugation with ϕ^2 is an automorphism of D.

(17.5) Lemma. *For any $i = 1, \ldots, n$, the following diagram is commutative*

$$\begin{array}{ccc} \bar{D} & \xrightarrow{\Psi_n} & \mathrm{GL}_1(A) \\ {\scriptstyle \beta_i}\big\downarrow & & \big\downarrow{\scriptstyle \phi^{-2}\cdot} \\ \bar{D} & \xrightarrow{\alpha_i} & \mathrm{GL}_1(A) \end{array}$$

where

$$\begin{aligned} \beta_i \colon \bar{D} &\longrightarrow \bar{D} \\ (d_1, \ldots, d_{n+1}) &\longmapsto (\phi^{-2} d_1 \phi^2, \ldots, \phi^{-2} d_i \phi^2, d_{i+1}, \ldots, d_{n+1}) \end{aligned}$$

and

$$\begin{aligned} \alpha_i \colon \bar{D} &\longrightarrow \mathrm{GL}_1(A) \\ (d_1, \ldots, d_n) &\longmapsto d_1 \phi d_2 \cdots \phi d_i \phi^{-1} d_{i+1} \phi \cdots \phi d_{n+1} \ . \end{aligned}$$

Therefore: $\deg \Psi_n = \deg \alpha_i$.

Proof: Clear. □

In this way we can change ϕ to ϕ^{-1} in any place without changing the degree of the map.

Let's assume that n is an odd number.

(17.6) Proposition. *The morphism*

$$\begin{aligned} \Psi_n' \colon \bar{D} &\longrightarrow \mathrm{GL}_1(A) \\ (d_1, \cdots, d_{n+1}) &\longmapsto \big(d_1(\phi d_2 \phi^{-1}) d_3 (\phi d_4 \phi^{-1}) \cdots d_n (\phi d_{n+1} \phi^{-1})\big) \end{aligned}$$

has degree: $\deg \Psi_n' = \deg \Psi_n$.

Proof: One changes the ϕ to ϕ^{-1} at the places after d_2, $d_4, \ldots, d_{n-1}$ and multiply additionally with ϕ^{-1} from the right. □

Now projectivising again the morphism and writing S and T for the projective tori associated to L and $K = \phi L \phi^{-1}$ we get

(17.7) Corollary. *The multiplication morphism*

$$\begin{aligned} \Phi_n\colon S \times T \times S \times T \times \cdots \times S \times T = (S \times T)^{\frac{n+1}{2}} &\longrightarrow \mathrm{PGL}_1(A) \\ ([d_1], [d_2], \ldots, [d_{n+1}]) &\longmapsto d_1 d_2 \cdots d_{n+1} \end{aligned}$$

has degree

$$\deg \Phi_n \;=\; \deg \Psi_n \;=\; n^{n-1} \cdot \deg \pi_n^n \;.$$

(17.8) Remark. If n is even, then one analogously gets: The multiplication morphism

$$\begin{aligned} \Phi_n\colon S \times T \times S \times T \times \cdots \times S \times T \times S = (S \times T)^{\frac{n}{2}} \times S &\longrightarrow \mathrm{PGL}_1(A) \\ ([d_1], [d_2], \ldots, [d_{n+1}]) &\longmapsto d_1 d_2 \cdots d_{n+1} \end{aligned}$$

has degree

$$\deg \Phi_n \;=\; \deg \Psi_n \;=\; n^{n-1} \cdot \deg \pi_n^n \;.$$

References

[BI] M.-A. Knus & A. S. Merkurjev & H. M. Rost & J.-P. Tignol. *The Book of Involutions,* American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998

[LaQF] T. Y. Lam. *The Algebraic Theory of Quadratic Forms,* W. A. Benjamin, Inc., Reading, Massachusetts, 1973

[PeSR] H. P. Petersson & M. L. Racine. An Elementary Approach to the Serre-Rost Invariant of Albert Algebras, *Indag. Mathem., N. S.* **7** (1996), 343-365

[RoCL] M. Rost. The Chain Lemma for Kummer Elements of degree 3, *C. R. Acad. Sci. Paris*, t. **328**, Série I, p. 185-190 (1999)

[SchQH] W. Scharlau. *Quadratic and Hermitian Forms,* Springer Verlag, Berlin Heidelberg New York, 1985

[SeCG] J.-P. Serre. *Cohomologie Galoisienne,* Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin Heidelberg New York, 1964

[SeLF] J.-P. Serre. *Local Fields,* Springer Verlag, Berlin Heidelberg New York, 1979

[ShPG] S. S. Shatz. *Profinite Groups, Arithmetic and Geometry,* Annals of Mathematics Studies **67**, Princeton University Press, Princeton, 1972

[WaAL] B. L. van der Waerden. *Algebra I,* Springer Verlag, Berlin Heidelberg New York, 1971