On Euler's Proof of the Fundamental Theorem of Algebra*

Simone Böttger[1] AND Uwe Storch[2]

Abstract | In this article, Euler's (incomplete) proof of the Fundamental Theorem of Algebra from 1749 is used as a motivation to develop simple criteria for the surjectivity of finite polynomial mappings $K^N \to K^N$, particularly for real closed fields K. The core of this article consists of criteria for the existence of K-rational points of finite (commutative) K-algebras. The main tools are quadratic forms and their signatures (if K is an ordered field) which are derived from K-linear forms on such algebras, in particular from the trace and its generalizations. For finite polynomial mappings an algebraic mapping degree is defined as such a signature. This mapping degree will serve as a very effective tool to prove the surjectivity of finite polynomial mappings over real closed fields K (as in differential topology for $K = \mathbb{R}$). In addition, it solves all the problems arising in Euler's proof which will be discussed in detail in the last section.

Introduction

This article is inspired by Euler's work on the Fundamental Theorem of Algebra (FTA). In response to d'Alembert's proof of the FTA, published in 1748 in [1], Euler wrote an article which appeared in 1751 and contains (besides many other things) another proof of this theorem, cf. [5]. Euler accepted d'Alembert's proof completely, but he wanted to provide a more algebraic proof.

Gauss criticized both proofs in his doctoral thesis, cf. [7]. He mentions four major points of criticism on Euler's proof. In Section 6, we describe the point which is in our opinion the most serious one. On the other hand, in 1907, Frobenius delivered a talk on occasion of Euler's 200th birthday in which he approved Euler's arguments without expressing any doubts, but also without giving any details. Moreover, in 1956, Speiser praised Euler's proof as a starting point of a new epoch of algebra (and simultaneously condemned d'Alembert's proof), cf. [15]. However, in [10], Remmert doubts that Euler's considerations can be extended to a complete proof of the FTA (within the scope given by Euler).

We agree that there are gaps in Euler's sketchy proof. But we are convinced of his ideas and methods and present in this article a proof of the FTA without any deficiency, which follows the lines of Euler rather closely, cf. Section 6. The main purpose of this article is to develop Euler's approach to the FTA in modern language and with a more general viewpoint.

[1]Department of Mathematics, Universität Osnabrück, Germany

[2]Department of Mathematics, Ruhr-Universität Bochum, Germany

E-mail: [1]siboettg@uos.de and [2]uwe.storch@rub.de

*Parts of this article have been discussed by the second author in talks at IIT Bombay and IISc Bangalore in November 2009 and December 2010, respectively. He thanks both institutes for their kind hospitality and DAAD for financial support.

First of all, Euler proves the FTA in its real form: Every real polynomial of degree ≥ 2 has a real factor of degree 2. It is very easy to see that this is an immediate consequence of the following: Any real polynomial of degree $2k = 2^{\gamma+1}$, $\gamma \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$, is the product of two real polynomials of degree k. Hence, Euler considers the multiplication mapping $\mathrm{V}_{(k,k)} : \mathbb{R}^k \times \mathbb{R}^k \to \mathbb{R}^{2k}$, $(F,G) \mapsto FG$, for monic real polynomials F,G of degree k, and shows that this mapping is surjective. Here and in the following, we identify quite generally any m-tuple $(x_1,\ldots,x_m) \in A^m$ of elements of a commutative ring A with the monic polynomial

$$Z^m - x_1 Z^{m-1} + \cdots + (-1)^m x_m \in A[Z]$$

of degree $m \in \mathbb{N}$. Euler's proof is algebraic in the following sense. He only assumes that the Intermediate Value Theorem holds for real polynomials. In modern terminology, this is equivalent to saying that the field $\mathbb{R}$ of real numbers is a real closed field (cf. [8, Chapter 11]).

This is the motivation for the general setting throughout this article: For an arbitrary r-tuple $\mathbf{m} = (m_1,\ldots,m_r) \in (\mathbb{N}^*)^r$ with $|\mathbf{m}| = m_1 + \cdots + m_r$ and an arbitrary field K, we consider the multiplication mapping

$$\mathrm{V}_{\mathbf{m}} : K^{\mathbf{m}} = K^{m_1} \times \cdots \times K^{m_r} \longrightarrow K^{|\mathbf{m}|} = K^{m_1+\cdots+m_r}$$

defined by $(F_1,\ldots,F_r) \mapsto F_1 \cdots F_r$ for monic polynomials $F_1,\ldots,F_r$ over K of degrees $m_1,\ldots,m_r$, respectively. For $\mathbf{m} = (1,\ldots,1)$ this is the classical Vieta mapping. Therefore we call all these mappings (g e n e r a l i z e d) V i e t a m a p p i n g s. A monic polynomial H over K of degree $|\mathbf{m}|$ belongs to the image of $\mathrm{V}_{\mathbf{m}} : K^{\mathbf{m}} \to K^{|\mathbf{m}|}$ if H is a product of monic polynomials of degrees $m_1,\ldots,m_r$. Hence, we are interested in the set of points $y \in K^{|\mathbf{m}|}$ for which the fiber $\mathrm{V}_{\mathbf{m}}^{-1}(y)$ is non-empty. (Here y represents the polynomial H.) Note that $\mathrm{V}_{\mathbf{m}}$ is a polynomial mapping. It is described by polynomials

$$\begin{aligned} T_1(X_1^{(1)},\ldots,X_{m_1}^{(1)};\ldots;X_1^{(r)},\ldots,X_{m_r}^{(r)}) &= T_1(X^{(1)};\ldots;X^{(r)}) \,, \\ &\vdots \\ T_{|\mathbf{m}|}(X_1^{(1)},\ldots,X_{m_1}^{(1)};\ldots;X_1^{(r)},\ldots,X_{m_r}^{(r)}) &= T_{|\mathbf{m}|}(X^{(1)};\ldots;X^{(r)}) \,, \end{aligned}$$

where $X^{(\rho)} = (X_1^{(\rho)},\ldots,X_{m_\rho}^{(\rho)})$ are the indeterminates for the coordinate functions of K^{m_ρ}. This means that the mapping $\mathrm{V}_{\mathbf{m}}$ belongs to the K-algebra homomorphism

$$\upsilon_{\mathbf{m}} : K[Y] = K[Y_1,\ldots,Y_{|\mathbf{m}|}] \longrightarrow K[X] = K[X^{(1)};\ldots;X^{(r)}]$$

with $Y_i \mapsto T_i$, $i = 1,\ldots,|\mathbf{m}|$, in the following sense: $\mathrm{V}_{\mathbf{m}}$ is the restriction of $\upsilon_{\mathbf{m}}^* : \operatorname{Spec} K[X] \to \operatorname{Spec} K[Y]$ to the set of K-rational points $K\text{-}\operatorname{Spec} K[X] = K^{\mathbf{m}}$ and $K\text{-}\operatorname{Spec} K[Y] = K^{|\mathbf{m}|}$. The fiber of $\upsilon_{\mathbf{m}}^*$ over $y \in K^{|\mathbf{m}|} \subseteq \operatorname{Spec} K[Y]$ is $\operatorname{Spec} P(y)$, where $P(y)$ is the f i b e r a l g e b r a

$$P(y) := K[X]/\mathfrak{m}_y K[X] = K[X]/\langle T_1 - y_1,\ldots,T_{|\mathbf{m}|} - y_{|\mathbf{m}|}\rangle$$

of $\upsilon_{\mathbf{m}}$ over y, where $\mathfrak{m}_y = \langle Y_1 - y_1,\ldots,Y_{|\mathbf{m}|} - y_{|\mathbf{m}|}\rangle$ is the maximal ideal in $K[Y]$ belonging to the point y. Hence, the fiber of $\mathrm{V}_{\mathbf{m}}$ over y is $K\text{-}\operatorname{Spec} P(y)$ and $\mathrm{V}_{\mathbf{m}}^{-1}(y) \neq \emptyset$ is equivalent to $K\text{-}\operatorname{Spec} P(y) \neq \emptyset$. For these elementary and basic notions, which describe the interrelation between algebraic and geometric objects, we refer to the introductory course [9]. It is easy to see that $\upsilon_{\mathbf{m}}$ is a finite K-algebra homomorphism of degree $\binom{|\mathbf{m}|}{\mathbf{m}}$, cf. Section

5, i.e. $K[X]$ is a finite (and even free) $K[Y]$-module of rank $\binom{|\mathbf{m}|}{\mathbf{m}}$ via $\upsilon_{\mathbf{m}}$. Therefore, all the fiber algebras $P(y)$, $y \in K^{|\mathbf{m}|}$, are finite K-algebras.

So, *we are looking for criteria which guarantee that a finite K-algebra has a K-rational point*, i.e. *a maximal ideal with residue class field K*. This is the content of Sections 1-3. The main tools are the trace form considered as a quadratic form and its generalizations, which are defined in a canonical way by K-linear forms on such algebras. For an ordered field K, the signatures of these forms are of particular importance. The main results are Theorem 3.2 and Theorem 3.4. The latter theorem proves to be very useful in connection with the mapping degree. We define it for finite polynomial mappings $T : K^N \to K^N$ over an ordered field K as the (constant) signature of the generalized trace form on the fibers $P(y)$, $y \in K^N$, which is derived from the K-algebra homomorphism $\tau : K[Y] \to K[X]$ belonging to T as described in [11]. This mapping degree $\delta(T) = \delta(\tau)$ is the counterpart of the topological mapping degree in case $K = \mathbb{R}$, cf. also [4]. If K is a real closed field and $\delta(T) \neq 0$ then T is surjective (Theorem 4.6). Since the mapping degrees of the Vieta mappings are easily calculated (cf. Theorem 5.5) this gives the surjectivity of these mappings for all cases for which surjectivity can be expected. In particular, Euler's case $\mathrm{V}_{(k,k)} : K^k \times K^k \to K^{2k}$, $k = 2^\gamma$, $\gamma \in \mathbb{N}^*$, is settled in this way, which yields the FTA, cf. Theorem 5.6 and Theorem 5.7. In the last Section 6, we come back to Euler's original considerations. What he really proves, in an ingenious way, is the existence of a non-zero polynomial E in $2k$ variables over K such that every monic polynomial H of degree $2k$ over K with $E(H) \neq 0$ belongs to the image of $\mathrm{V}_{(k,k)}$, k as above (cf. Theorem 6.1). From this "generic" result, the FTA can be derived already with the trace form using Theorem 3.2.

In this article "ring" always means "commutative ring with unity". For a sequence $a = (a_1, \ldots, a_r)$ of elements of a ring, $\langle a \rangle = \langle a_1, \ldots, a_r \rangle$ denotes the ideal generated by $a_1, \ldots, a_r$ in the ring under consideration (which, for example, may be a subring containing these elements).

§ 1 Symmetric bilinear forms over ordered fields

In this section, K always denotes an ordered field. Thus, K is a field with a total order $\leq$, which satisfies the usual rules of monotony for addition and multiplication. Then K is equipped with the order topology, for which the open intervals $]a,b[$, $a,b \in K$, $a < b$, form a base. The vector spaces K^n, $n \in \mathbb{N}$, are endowed with the product topology (with a base given by the open cuboids $]a_1,b_1[\times \cdots \times]a_n,b_n[$, $a_i < b_i$, $i = 1, \ldots, n$). Addition, multiplication and inverse are continuous functions on $K \times K$ and $K^\times = K \setminus \{0\}$, respectively. It follows that polynomial functions and more general rational functions F/G in n variables are continuous K-valued functions on K^n outside of the (closed) zero set of the denominator G. Furthermore, the topology of K^n transfers uniquely to every n-dimensional K-vector space by a K-linear isomorphism $f : V \to K^n$. Any other isomorphism $g : V \to K^n$ defines the same topology, since $gf^{-1} : K^n \to K^n$ and $(gf^{-1})^{-1} = fg^{-1} : K^n \to K^n$ are continuous (polynomial) mappings. Thus, polynomial and rational functions are also defined on any finite-dimensional vector space V by such an isomorphism $f : V \to K^n$. The topology on V may be characterized as the small-

est topology for which the K-linear functions $V \to K$ are continuous (with respect to the topology on K from above). If necessary, we call the topology on V just described the strong topology on V (in contrast to the Zariski topology, which is weaker if $V \neq 0$).

For two points $x, y \in V$ the (closed) line segment $[x,y] = [y,x]$ is the set $\{(1-t)x + ty \mid t \in K, 0 \leq t \leq 1\}$. For $x_0, \ldots, x_r \in V$, $r \geq 1$, we denote by $[x_1, \ldots, x_r] = \bigcup_{i=1}^{r} [x_{i-1}, x_i]$ the broken line from x_0 to x_r. A subset $A \subseteq V$ is called line connected if for any two points $x, y \in A$ there is a broken line from x to y which lies entirely in A. If $K = \mathbb{R}$ and $A \subseteq V$ is open, the notion of "line connected" is equivalent to the topological notion of "connected", whereas the only topologically connected subspaces of $K = \mathbb{Q}$ are the singletons. If V is a line, i.e. 1-dimensional, and if $x \in V$, then $V \setminus \{x\}$ is not line connected. However, if $\mathrm{Dim}_K V \geq 2$, then $V \setminus \{x\}$ is always line connected: If $u, w \in V \setminus \{x\}$ are arbitrary points, there is always a point $v \in V \setminus \{x\}$ such that $[u, v, w] \subseteq V \setminus \{x\}$. Obviously, the more general statement holds:

1.1 Lemma *If $U_1, \ldots, U_k$ are affine subspaces of codimension ≥ 2 of a finite-dimensional K-vector space V and if $A \subseteq V$ is open and line connected, then $A \setminus \bigcup_{j=1}^{k} U_j$ is (open and) line connected.*

Now, let Φ be a symmetric bilinear form on the finite-dimensional K-vector space V. We identify any symmetric bilinear form Φ over a field of characteristic $\neq 2$ with its associated quadratic form $Q = Q_\Phi$ such that $Q(x) = \Phi(x,x)$. The bilinear form Φ is determined by Q via the polarization formula $\Phi(x,y) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y))$. It is well-known that there exists a Φ-orthogonal base $v_1, \ldots, v_n$ of V (such that $\Phi(v_i, v_j) = 0$ for $i \neq j$). Let $v_1, \ldots, v_n$ be normalized in such a way that the Gramian matrix $(\Phi(v_i, v_j))_{1 \leq i,j \leq n}$ is a diagonal matrix $\mathrm{diag}(a_1, \ldots, a_p, b_1, \ldots, b_q, 0, \ldots, 0)$ with $a_1, \ldots, a_p > 0$ and $b_1, \ldots, b_q < 0$. Then p and q are uniquely determined by Φ, i.e. they are independent of the choice of the orthogonal base $v_1, \ldots, v_n$ (Sylvester's Theorem of Inertia). Indeed, p equals the maximum of the dimensions of subspaces U of V on which Φ is positive definite, i.e. $\Phi(x,x) > 0$ on $U \setminus \{0\}$, and q is the maximum of the dimensions of subspaces U on which Φ is negative definite. The sum $p+q$ is the rank of Φ, the difference $p-q$ its signature and (p,q) is the type of Φ. We denote them by $\mathrm{rank}\,\Phi$, $\mathrm{sign}\,\Phi$ and $\mathrm{type}\,\Phi$, respectively. Often the type of Φ can be determined by the well-known Criterion of Hurwitz: If $u_1, \ldots, u_n$ is an arbitrary base of V and if all principal minors $D_m := \det(\Phi(u_i, u_j))_{1 \leq i,j \leq m}$, $m = 0, \ldots, n$, are non-zero, then $\mathrm{type}\,\Phi = (n-q, q)$, where q denotes the number of sign changes in the sequence $D_0 = 1, D_1, \ldots, D_m$. If $\mathfrak{A} = (a_{ij}) \in \mathrm{M}_n(K)$ is a symmetric matrix, then $\mathrm{rank}\,\mathfrak{A} := \mathrm{rank}\,\Phi$, $\mathrm{sign}\,\mathfrak{A} := \mathrm{sign}\,\Phi$ and $\mathrm{type}\,\mathfrak{A} := \mathrm{type}\,\Phi$, where $\Phi = \Phi_\mathfrak{A}$ is the symmetric bilinear form on K^n defined by $\mathfrak{A}$ (with $\Phi(e_i, e_j) = a_{ij}$, $1 \leq i, j \leq n$, where $e_1, \ldots, e_n$ is the standard base of K^n). Of course, $\mathrm{rank}\,\mathfrak{A}$ coincides with the usual rank of the matrix $\mathfrak{A}$.

The Criterion of Hurwitz yields easily the following lemma:

1.2 Lemma *Let $F_{ij} \in K[T]$, $1 \leq i, j \leq n$, be polynomials such that $F_{ij} = F_{ji}$. If the Gramian matrix $(F_{ij}(s))_{1 \leq i,j \leq n}$ defines a non-degenerate bilinear form for some $s \in K$, then there exists an $\varepsilon > 0$ such that the type of the Gramian matrices $(F_{ij}(t))_{1 \leq i,j \leq n}$ is the same for all $t \in]s - \varepsilon, s + \varepsilon[$. (In this sense, being of type (p,q) is an open property for non-degenerate symmetric bilinear forms over K.)*

Proof: By a linear change of coordinates on K^n, we may assume that $(F_{ij}(s))_{1\le i,j\le n}$ is a diagonal matrix $\operatorname{diag}(a_1,\dots,a_p,b_1,\dots,b_q)$ such that $a_i>0$, $b_j<0$ and $p+q=n$. Then the principal minors $D_m(t)=(F_{ij}(t))_{1\le i,j\le m}$, $m=1,\dots,n$, are non-zero and there exists an $\varepsilon>0$ such that $D_m(t)$ has the same sign as $D_m(s)$ for all $t\in]s-\varepsilon,s+\varepsilon[$ and all $m=0,\dots,n$ (because the polynomial functions $D_m(t)$ are continuous). This proves Lemma 1.2 by the Criterion of Hurwitz. □

If in Lemma 1.2 the Gramian matrix $(F_{ij}(s))$ is degenerate of type (p,q), then for some $\varepsilon>0$ the Gramian matrix $(F_{ij}(t))$ is of type (p',q') with $p'\ge p$, $q'\ge q$ for all $t\in]s-\varepsilon,s+\varepsilon[$.

Now, let K be in addition real closed, that is, K suffices the Intermediate Value Theorem (IVT) for polynomial functions: If $F\in K[T]$ is a polynomial with coefficients in K such that $F(a)F(b)<0$ for some $a,b\in K$, then F has a zero in $[a,b]$. In other words, the values $F(t)$, $t\in[a,b]$, have the same sign if F has no zero on $[a,b]$. In particular, every polynomial of odd degree has a zero in K. Generally, a field with this property is called a 2-field. Hence, *a real closed field is a 2-field*. Furthermore, every monic polynomial F over a real closed field K has a positive zero in K if $F(0)<0$ (since $F(x)>0$ for "large" x). For the general theory of real closed fields, we refer to Chapter 11 of [8], but we make use of it only in Remark 3.3.

We now consider families of non-degenerate symmetric bilinear forms on n-dimensional K-vector spaces and their Gramian matrices $(R_{ij}(t))_{1\le i,j\le n}$, where $R_{ij}(t)=R_{ij}(t_1,\dots,t_N)$ are rational functions on a subset $A\subseteq K^N$. In this situation the following holds:

1.3 Rigidity Theorem for Quadratic Forms *Let K be a real closed field and let R_{ij}, $1\le i,j\le n$, be rational functions on a line connected subset $A\subseteq K^N$ such that $R_{ij}=R_{ji}$ and $\det((R_{ij}(t))_{1\le i,j\le n})\neq 0$ for all $t\in A$. Then all the matrices $(R_{ij}(t))_{1\le i,j\le n}\in \mathrm{M}_n(K)$, $t\in A$, have the same type (p,q), or equivalently, the same signature $p-q$.*

Proof: It suffices to prove that the signature on a line segment in A is constant. We may parametrize the points on this line segment by the interval $[0,1]\subseteq K$ and assume $R_{ij}=F_{ij}/G_{ij}$ to be rational functions defined on $[0,1]$, where F_{ij},G_{ij} are polynomial functions and G_{ij} does not vanish on $[0,1]$. Expanding the fractions yields a common denominator G. By the Intermediate Value Theorem, the values of G have constant sign on $[0,1]$, say $G>0$ on $[0,1]$. Then, for $t\in[0,1]$ the symmetric matrices $(R_{ij}(t))$ and $(F_{ij}(t))$ have the same type. A linear change of coordinates on K^n turns $(F_{ij}(0))$ into a diagonal matrix $\operatorname{Diag}(a_1,\dots,a_p,b_1,\dots,b_q)$ such that $a_i>0$, $b_j<0$ and $p+q=n$. In particular, the principal minors $D_m(t)=\det((F_{ij}(t))_{1\le i,j\le m}$ are then non-zero polynomials for all $m=0,\dots,n$, and the sequence $D_0(0),D_1(0),\dots,D_m(0)$ has q sign changes. Hence, there are points $0=t_0<t_1<\cdots<t_\ell=1$ such that all $D_m(t)$ are $\neq 0$ on the intervals $[0,t_1[$ and $]t_i,t_{i+1}[$, $i=1,\dots,\ell-1$. On each of these intervals, by IVT, all minors $D_m(t)$ have the same sign and hence, by Hurwitz's Criterion, the matrices $(F_{ij}(t))_{1\le i,j\le n}$ the same type. That the type is constant even on $[0,1]$ follows now from Lemma 1.2. □

Obviously, the validity of the Rigiditiy Theorem 1.3 characterizes the real closed fields in the class of all ordered fields.

§ 2 Finite Algebras over Fields

As explained in the introduction, we have to study finite (commutative) algebras over a field K which occur as fiber algebras of a finite homomorphism of K-algebras, and to look for their K-rational points. These points are in one-to-one correspondence to the maximal ideals of the given K-algebra A with residue class field K, or equivalently, to the K-algebra homomorphisms $A \to K$. We denote the set of these points by $K\text{-Spec}\,A$. It is a subset of the maximal spectrum $\mathrm{Spm}\,A$ of A, that is the set of maximal ideals of A, which itself is a subset of the prime spectrum $\mathrm{Spec}\,A$ of A, that is, the set of prime ideals of A.

If A is a finite K-algebra, i. e. finite as a K-vector space, then $\mathrm{Spm}\,A = \mathrm{Spec}\,A$ (since any finite K-algebra which is an integral domain is already a field). Moreover, $\mathrm{Spm}\,A$ *is a finite set*. This follows immediately from the Chinese Remainder Theorem: If $\mathfrak{m}_i$, $i \in I$, is a finite family of pairwise distinct maximal ideals of A, then the canonical K-algebra homomorphism $A \to \prod_{i\in I} A/\mathfrak{m}_i$ is surjective. In particular, the cardinality of $\mathrm{Spm}\,A$ is at most $\mathrm{Dim}_K A$ (and equality holds if and only if A is isomorphic to the product algebra $K^{\mathrm{Dim}_K A}$).

Now, let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be the (pairwise distinct) maximal ideals of the finite K-algebra A. Then the group of units $A^\times$ of A is $A \setminus \bigcup_{i=1}^r \mathfrak{m}_i$. Further, the canonical homomorphism $A \to \prod_{\rho=1}^r A_{\mathfrak{m}_\rho}$ is injective (where, quite generally, $A_\mathfrak{p}$ denotes the localization of a commutative ring A at a prime ideal $\mathfrak{p} \subseteq A$). In our special case, it is also surjective and hence an isomorphism, cf. Corollary 55.16 of [12]. Therefore, *A is the direct product of the local finite K-algebras $A_\rho := A_{\mathfrak{m}_\rho}$, $\rho = 1, \ldots, r$*, which are called the l o c a l c o m p o n e n t s of A. Furthermore, we get

$$\mathrm{Dim}_K A = \sum_{\rho=1}^{r} \mathrm{Dim}_K A_\rho = \sum_{\rho=1}^{r} \ell(A_\rho) \cdot [K_\rho : K] \,,$$

where, for $\rho = 1, \ldots, r$, K_ρ is the residue class field $A/\mathfrak{m}_\rho$ and $\ell(A_\rho)$ the (finite) length of A_ρ, i. e. the length ℓ of a composition series $0 = \mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_\ell = A_\rho$ with $\mathfrak{a}_{i+1}/\mathfrak{a}_i \cong A/\mathfrak{m}_\rho$, $i = 1, \ldots, \ell - 1$. For example, if K is a 2-field, then $[K_\rho : K]$ is even if K_ρ is a non-trivial field extension of K and, in particular, *$K\text{-Spec}\,A \neq \emptyset$ if $\mathrm{Dim}_K A$ is odd*. Later we will derive directly from this that the degree of a finite field extension of a 2-field is always a power of 2, cf. Example 5.3.

The Jacobson radical $\mathfrak{m}_A := \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ of A coincides with the nil radical $\mathfrak{n}_A$, which is the ideal of all nilpotent elements in A.[1] *The ideal $\mathfrak{m}_A = \mathfrak{n}_A$ is the zero ideal, i.e. A is reduced, if and only if $A = K_1 \times \cdots \times K_r$ is the product of its residue class fields*. If moreover all the field extensions K_ρ of K are separable, then A is called a (finite) s e p a r a b l e K-algebra.

2.1 Example Let A be a finite K-algebra with a p r i m i t i v e e l e m e n t $x \in A$, i.e. a generator of A as a K-algebra. Then $A = K[x] \cong K[X]/\langle \mu_x \rangle$, where μ_x is the m i n i m a l p o l y n o m i a l of x which is monic and generates the kernel of the (surjective) substitution homomorphism $K[X] \to A$, $X \mapsto x$. If $\mu_x = \pi_1^{\alpha_1} \cdots \pi_r^{\alpha_r}$ is the canonical factorization of μ_x in $K[X]$ with pairwise

[1] Note, that for an arbitrary commutative ring A the nil radical $\mathfrak{n}_A$ is the intersection of all prime ideals of A.

distinct monic prime polynomials $\pi_1, \ldots, \pi_r$ and (positive) exponents $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$, then $A_\rho := K[X]/\langle \pi_\rho^{\alpha_\rho} \rangle$ are the local components of A and $K_\rho := K[X]/\langle \pi_\rho \rangle$ its residue class fields, $\rho = 1, \ldots, r$. The K-rational points of A correspond to the linear prime factors of μ_x, i.e. to the zeros of μ_x in K. The radical of A is generated by $\pi_1(x) \cdots \pi_r(x) \in A$ and A is reduced if and only if $\alpha_1 = \cdots = \alpha_r = 1$. A is a separable K-algebra if, moreover, all prime factors $\pi_1, \ldots, \pi_r$ of μ_x are separable prime polynomials. Together, these conditions are equivalent with $\gcd(\mu_x, \mu_x') = 1$, where μ_x' is the derivative of μ_x.

In the theory of solving polynomial equations a primitive element of a finite K-algebra A is often called a r e s o l v e n t of A and its minimal polynomial a r e s o l v e n t p o l y n o m i a l (or a r e s o l v e n t e q u a t i o n) for A.[2] *A finite separable algebra over an infinite field K has always a resolvent*. To prove this P r i m i t i v e E l e m e n t T h e o r e m one may use a (finite) field extension $K \subseteq L$ such that all residue class fields of the L-algebra $A_{(L)} = L \otimes_K A$ coincide with L. (L is then called a s p l i t t i n g f i e l d of A.) Since $A_{(L)}$ is separable over L (by Lemma 3.1 below, for instance), it is isomorphic to the product algebra L^n, $n := \mathrm{Dim}_L A_{(L)} = \mathrm{Dim}_K A$, and therefore has a primitive element. (Any n-tuple in L^n with n pairwise distinct components is a primitive element !) Then the K-algebra itself has also a primitve element (since K is infinite by assumption).

A resolvent of a (finite) Galois field extension of K (which exists by the Primitive Element Theorem) is called a G a l o i s r e s o l v e n t and the resolvent polynomial belonging to it a G a l o i s r e s o l v e n t p o l y n o m i a l.

§ 3 The Trace Form and its Generalizations

Let A be a finite algebra over a field K. A classical tool for studying A is the t r a c e f o r m, which is the symmetric K-bilinear form $\mathrm{tr} : (f,g) \mapsto \mathrm{tr}_K^A(fg)$ on A. Usually, we denote it as the trace itself, by $\mathrm{tr} = \mathrm{tr}_K^A$ (thus, $\mathrm{tr}(f,g) = \mathrm{tr}(fg)$). The decomposition of $A = A_1 \times \cdots \times A_r$ into its local components (cf. Section 2) yields the orthogonal decomposition

$$\mathrm{tr}_K^A = \mathrm{tr}_K^{A_1} \perp \cdots \perp \mathrm{tr}_K^{A_r}$$

of the trace form. The d e g e n e r a t i o n s p a c e $A^\perp = A^{\perp \mathrm{tr}} = \{f \in A \mid \mathrm{tr}(Af) = 0\}$ is an ideal in A.

3.1 Lemma *The radical $\mathfrak{m}_A = \mathfrak{n}_A$ is always contained in the degeneration space $A^\perp$ of the trace form. Both ideals coincide if and only if all the residue class fields of A are separable over K, that is, if and only if the reduction $A_{\mathrm{red}} = A/\mathfrak{n}_A$ is a separable K-algebra. – In particular, the trace form is non-degenerate if and only if A is a separable K-algebra.*

Proof: If $f \in \mathfrak{n}_A$, then $gf \in \mathfrak{n}_A$ for every $g \in A$. Therefore, multiplication with gf is a nilpotent operator on A and $\mathrm{tr}(gf) = 0$. Hence, $\mathfrak{n}_A \subseteq A^\perp$. For the additional statements it suffices to show that the trace form of a reduced finite K-algebra $A = K_1 \times \cdots \times K_r$ is non-degenerate if and only if A is a separable K-algebra. Since $\mathrm{tr}_K^A = \mathrm{tr}_K^{K_1} \perp \cdots \perp \mathrm{tr}_K^{K_r}$, we have to show that for a finite field extension $K \subseteq L$ the trace form tr_K^L is non-degenerate if and only if L is separable over K. But this follows from the well-known fact that the linear form $\mathrm{tr}_K^L : L \to K$ is non-zero if and only if L is separable over K. □

[2] Many authors call also the resolvent polynomial a resolvent.

In case K is a field of characteristic zero, A_{red} is always separable over K and $A^{\perp} = \mathfrak{n}_A$. The inclusion $A^{\perp} \subseteq \mathfrak{n}_A$ may be deduced in this case in the following simple way: If $f \in A^{\perp}$, then, in particular, $\mathrm{tr}_K^A(f^n) = 0$ for all $n \in \mathbb{N}^*$. Now, a well-known result in linear algebra states that in characteristic zero a linear operator f on a finite-dimensional vector space V with $\mathrm{tr}(f^n) = 0$ for all $n \in \mathbb{N}^*$ (or at least for all $n = 1, \ldots, \mathrm{Dim}_K V$) is nilpotent.

From the previous Lemma 3.1, we get

$$\mathrm{rank}\, \mathrm{tr}_K^A = \mathrm{Dim}_K(A/\mathfrak{m}_A) = \sum_{\rho=1}^{r} [K_\rho : K] \,,$$

if A_{red} is separable over K. Moreover, if K is an ordered field, then

$$\mathrm{type}\, \mathrm{tr}_K^A = \sum_{\rho=1}^{r} \mathrm{type}\, \mathrm{tr}_K^{K_\rho} \quad \text{and} \quad \mathrm{sign}\, \mathrm{tr}_K^A = \sum_{\rho=1}^{r} \mathrm{sign}\, \mathrm{tr}_K^{K_\rho} \,.$$

Now, we prove the following important and classical criterion for the existence of K-rational points for real closed fields. The Fundamental Theorem of Algebra is not needed for its proof.

3.2 Theorem *Let A be a finite commutative algebra over a real closed field K. Then*

$$\mathrm{sign}\, \mathrm{tr}_K^A = \#K\text{-}\mathrm{Spec}\, A \,.$$

In particular, K is a residue class field of A if and only if $\mathrm{sign}\, \mathrm{tr}_K^A \neq 0$.

Proof: Since $\mathrm{sign}\, \mathrm{tr}_K^K = 1$ and by the formula above, it suffices to show that $\mathrm{sign}\, \mathrm{tr}_K^L = 0$ for every finite field extension $L \neq K$ of K. To prove this, we consider for every $x \in L$, $x \neq 0$, the symmetric bilinear forms $\Phi_x : (f,g) \mapsto \mathrm{tr}_K^L(xfg)$ on L which, like tr_K^L, are non-degenerate. We have $\Phi_1 = \mathrm{tr}_K^L$ and $\Phi_{-1} = -\mathrm{tr}_K^L$. Since $\mathrm{Dim}_K L \geq 2$, the punctured space $L^{\times} = L \setminus \{0\}$ is line connected and, by the Rigidity Theorem for Quadratic Forms 1.3, the signature $\mathrm{sign}\, \Phi_x$ is constant on $L^{\times}$. In particular, $\mathrm{sign}\, \mathrm{tr}_K^L = \mathrm{sign}(-\mathrm{tr}_K^L) = -\mathrm{sign}\, \mathrm{tr}_K^L$, and therefore $\mathrm{sign}\, \mathrm{tr}_K^L = 0$. □

For the real case $K = \mathbb{R}$, Theorem 3.2 is a classical result in linear algebra, cf. Theorem 94.7 of [12], but generally the Fundamental Theorem of Algebra (see Theorem 5.6 below) is used in the proof. It states that the only non-trivial field extension L of a real closed field K is, up to isomorphism, given by the quadratic extension $L = \mathbb{C}_K = K[i] = K[\sqrt{-1}]$ of complex numbers over K. The Gramian matrix of $\mathrm{tr}_K^{\mathbb{C}_K}$ with respect to the basis $1, i$ is given by

$$\begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(i) \\ \mathrm{tr}(i) & \mathrm{tr}(-1) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} .$$

Thus, $\mathrm{type}\, \mathrm{tr}_K^{\mathbb{C}_K} = (1,1)$ and $\mathrm{sign}\, \mathrm{tr}_K^{\mathbb{C}_K} = 0$.

3.3 Remark An arbitrary ordered field K is (order-preservingly) embeddable into a real closed field $\hat{K}$ (see Theorem 11.4 of [8]). Now, if A is a finite K-algebra and if $\hat{A} := \hat{K} \otimes_K A$, then, obviously, $\mathrm{sign}\, \mathrm{tr}_K^A = \mathrm{sign}\, \mathrm{tr}_{\hat{K}}^{\hat{A}}$ and hence by Theorem 3.2,
$\mathrm{sign}\, \mathrm{tr}_K^A = \#\mathrm{Hom}_{\hat{K}\text{-alg}}(\hat{A}, \hat{K}) = \#\mathrm{Hom}_{K\text{-alg}}(A, \hat{K})$ *is the number of $\hat{K}$-valued points of A.*

The statement of Theorem 3.2 may be generalized to some extent. For this, we start again with a finite algebra A over an arbitrary field K. As well as for the trace form, one can associate to any K-linear form $\alpha : A \to K$ the symmetric bilinear form

$$\Phi_\alpha : A \times A \longrightarrow K\,, \quad (f,g) \longmapsto \alpha(fg)\,.$$

This defines a K-linear embedding of the dualizing module

$$E := E_{A|K} := \mathrm{Hom}_K(A,K)$$

into the space of symmetric bilinear forms on A. The elements of the image are called generalized trace forms on A. Note that E is also an A-module by $(g\alpha)(f) = \alpha(fg)$ for $\alpha \in E$, $g,f \in A$. Thus, $\Phi_\alpha(f,g) = (g\alpha)(f) = (f\alpha)(g)$. The degeneration space $A^{\perp\alpha}$ of Φ_α is the *largest ideal of A contained in* $\ker\alpha$. If $\overline{\alpha} : A/A^{\perp\alpha} \to K$ denotes the linear form on $\overline{A} := A/A^{\perp\alpha}$ induced by α, then $\mathrm{rank}\,\Phi_\alpha = \mathrm{rank}\,\Phi_{\overline{\alpha}}$. If, in addition, K is an ordered field then $\underline{\mathrm{type}}\,\Phi_\alpha = \mathrm{type}\,\Phi_{\overline{\alpha}}$ and $\mathrm{sign}\,\Phi_\alpha = \mathrm{sign}\,\Phi_{\overline{\alpha}}$. The bilinear form $\Phi_{\overline{\alpha}}$ is non-degenerate on $\overline{A}$. In general, Φ_α is non-degenerate if and only if $f\alpha \neq 0$ for all $f \in A \setminus \{0\}$, that is, if $A\alpha \subseteq E$ is a free A-submodule of rank one. Since $\mathrm{Dim}_K E = \mathrm{Dim}_K A$, even the equality $A\alpha = E$ holds, i.e. α is an A-base of E. A finite K-algebra is called a Frobenius algebra if it possesses such a K-linear form α for which Φ_α is non-degenerate or, equivalently, if $E \cong A$ as A-modules. For instance, *$A/A^{\perp\alpha}$ is a Frobenius algebra for every $\alpha \in E$.*

With these notions, we can formulate now the announced partial generalization of Theorem 3.2 which will be an important argument in the constructions of the following sections:

3.4 Theorem *Let α be a K-linear form on a finite commutative algebra A over a real closed field K. If* $\mathrm{sign}\,\Phi_\alpha \neq 0$*, then A has a K-rational point, i.e. K-*$\mathrm{Spec}\,A \neq \emptyset$.

Proof: Since $\mathrm{sign}\,\Phi_\alpha = \mathrm{sign}\,\Phi_{\overline{\alpha}}$ for the induced $\overline{\alpha}$ on $\overline{A} = A/A^{\perp\alpha}$, we may assume that $\Phi_{\overline{\alpha}}$ is non-degenerate. We consider the family of non-degenerate symmetric bilinear forms $\Phi_{f\alpha}$, $f \in A^\times = A \setminus (\mathfrak{m}_1 \cup \cdots \cup \mathfrak{m}_r)$, where $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ denote the maximal ideals of A. If $A/\mathfrak{m}_\rho \neq K$ for every $\rho = 1, \ldots, r$, then all $\mathfrak{m}_\rho$ have at least codimension 2 in A, and therefore $A^\times$ is line connected by Lemma 1.1. By the Rigidity Theorem 1.3, then all $\Phi_{f\alpha}$, $f \in A^\times$, have the same signature. In particular, $\mathrm{sign}\,\Phi_\alpha = \mathrm{sign}\,\Phi_{-\alpha} = -\mathrm{sign}\,\Phi_\alpha$, hence $\mathrm{sign}\,\Phi_\alpha = 0$. Contradiction! □

The preceding result yields in particular: If L is a non-trivial finite field extension of a real closed field K and $\alpha : L \to K$ is a K-linear form on L, then $\mathrm{sign}\,\Phi_\alpha = 0$.[3]

§ 4 The Algebraic Mapping Degree

The mapping degree of differential topology may also be described in purely algebraic terms. Here we do it only for finite polynomial mappings of affine spaces. This is sufficient for the purposes of this article. The basic results used for our construction are

[3] By Theorem 5.7, the only possibility is $L = \mathbb{C}_K = K[\sqrt{-1}]$.

provided by the article [11]. For another algebraic approach to the mapping degree in the real case ($K = \mathbb{R}$) see [4].

We are interested in the Vieta mappings. These are special polynomial mappings

$$T : K^N \longrightarrow K^N\ , \quad x \longmapsto y = T(x)\ .$$

Here, K is a field and $y = T(x) = (T_1(x), \ldots, T_N(x))$ with polynomials $T_1, \ldots, T_N \in K[X] = K[X_1, \ldots, X_N]$ in N variables, $N \in \mathbb{N}$. We interpret K^N as the set of K-rational points of $K[X]$ and $K[Y] = K[Y_1, \ldots, Y_N]$, respectively. Then T is the restriction of the mapping τ^* to the set of K-rational points, where

$$\tau^* = \operatorname{Spec}\tau : \operatorname{Spec} K[X] \longrightarrow \operatorname{Spec} K[Y]$$

is the functorial mapping $\mathfrak{p} \mapsto \tau^{-1}\mathfrak{p}$ corresponding to the K-algebra homomorphism

$$\tau : K[Y] \longrightarrow K[X]\ , \quad Y_i \longmapsto T_i\ , i = 1, \ldots, N\ .$$

If T is a Vieta mapping, then τ becomes a finite homomorphism, i.e. $K[X]$ is a finite $K[Y]$-module via τ, cf. Section 5.

Therefore, *we assume from now on that $P := K[X]$ is a finite algebra over $Q := K[Y]$, i.e. that P is a finite Q-module via τ*. Then we also say that $T : K^N \to K^N$ is a finite polynomial mapping.[4]

Under these assumptions, τ is injective and P is a projective Q-module of finite rank $[K(X) : K(Y)] =: n$. When convenient, we shall identify the indeterminates Y_i with the images $\tau(Y_i) = T_i$, $i = 1, \ldots, N$. The degree $n = [K(X) : K(Y)]$ is called the sheet number of τ (or of τ^*, or of T). Very often it is also called the degree of the mapping. By the solution of Serre's problem on projective modules over polynomial algebras over fields, P is even a free Q-module. In the situations we are focussing on, this can always be seen directly, and Q-bases of P can be computed effectively (mainly because we are in graded situations).

A K-rational point $y = (y_1, \ldots, y_N) \in K^N$ corresponds to the maximal ideal

$$\mathfrak{m}_y = \langle Y_1 - y_1, \ldots, Y_N - y_N \rangle \in \operatorname{Spm} Q \subseteq \operatorname{Spec} Q$$

and the fiber $T^{-1}(y)$ is the set of K-rational points of the fiber algebra

$$P(y) := P_{\mathfrak{m}_y}/\mathfrak{m}_y P_{\mathfrak{m}_y} = P/\mathfrak{m}_y P = P/\langle T_1 - y_1, \ldots, T_N - y_N \rangle = K \otimes_Q P$$

(where K is considered as a Q-algebra via $Q \to K$, $Y_i \mapsto y_i$). In particular, *y belongs to the image of $T : K^N \to K^N$ if and only if K-Spec $P(y) \neq \emptyset$*. The K-algebra $P(y)$ is finite of dimension n if $\tau : Q \to P$ is finite of degree n.

4.1 Example Let us assume that K is a 2-field and that the sheet number $n = [K(X) : K(Y)]$ of the finite polynomial mapping $T : K^N \to K^N$ is odd. Then all fiber algebras $P(y)$, $y \in K^N$, of T are of dimension n and therefore have K-rational points, cf. Section 2. Hence, we have proved: *Let K be a 2-field. Then a finite polynomial mapping $T : K^N \to K^N$ of odd sheet number is always surjective*.

We continue discussing finite polynomial mappings $T : K^N \to K^N$ for arbitrary fields K. According to [11], with the help of the finite K-algebra homomorphism $\tau : Q \to P$

[4] If the field K is finite the polynomials $T_1, \ldots, T_N \in K[X]$ are not uniquely determined by the mapping $T : K^N \to K^N$. Therefore, we assume tacitely that first the algebra homomorphism τ is given and that T is derived from it.

a canonical P-base of the P-module $E := E_{P|Q} = \mathrm{Hom}_Q(P,Q)$ can be constructed in the following way:[5] The kernel of the multiplication mapping $\mu_P : P \otimes_K P \to P$ (with $F \otimes G \mapsto FG$) is obviously generated by the polynomials $X_1 \otimes 1 - 1 \otimes X_1, \ldots, X_N \otimes 1 - 1 \otimes X_N$. It contains the elements $T_1 \otimes 1 - 1 \otimes T_1, \ldots, T_N \otimes 1 - 1 \otimes T_N$. Thus, we have representations

$$T_j \otimes 1 - 1 \otimes T_j = \sum_{i=1}^{N} A_{ij}(X_i \otimes 1 - 1 \otimes X_i) \ , \quad j = 1, \ldots, N,$$

with (in general not uniquely determined) coefficients $A_{ij} \in P \otimes_K P$. But the canonical image

$$\Delta \in P \otimes_Q P = P \otimes_K P / \langle T_1 \otimes 1 - 1 \otimes T_1, \ldots, T_N \otimes 1 - 1 \otimes T_N \rangle$$

of the determinant

$$B := \det(A_{ij})_{1 \le i,j \le N} \in P \otimes_K P$$

is unique (because both sequences $T_1 \otimes 1 - 1 \otimes T_1, \ldots, T_N \otimes 1 - 1 \otimes T_N$ and $X_1 \otimes 1 - 1 \otimes X_1, \ldots, X_N \otimes 1 - 1 \otimes X_N$ are regular sequences in the polynomial algebra $P \otimes_K P$). Since P is a finite projective Q-module, the canonical homomorphism $\kappa : P \otimes_Q P \to \mathrm{Hom}_Q(E,P)$ (with $F \otimes G \mapsto (\alpha \mapsto \alpha(F)G)$) is an isomorphism, and $\theta = \theta_{P|Q} = \kappa(\Delta) : E \to P$ is moreover P-linear and bijective (Theorem 3.3, [11]). Then, the desired natural P-base of E is given by the Q-linear form

$$\eta := \theta^{-1}(1) : P \to Q \ .$$

Clearly, η depends not only on τ, but also on the choice of generators $X_1, \ldots, X_N$ of P and, since $T_i = \tau(Y_i)$, on the generators $Y_1, \ldots, Y_N$ of Q. Whenever we want to point out this dependence, we write η_Y^X or η_T^X instead of η.

As described in Section 3, we associate to η the symmetric bilinear form $\Phi_\eta : P \times P \to Q$ with $\Phi_\eta(F,G) := \eta(FG)$, which is a perfect duality. If $F_1, \ldots, F_n$ is a Q-base of P and

$$\Delta = \sum_{r=1}^{n} F_r \otimes F_r^* \in P \otimes_Q P$$

then

$$\Phi_\eta(F_r, F_s^*) = \eta(F_r F_s^*) = \delta_{rs} \ , \quad 1 \le r,s \le n,$$

i.e. $F_1^*, \ldots, F_n^*$ is the dual base of $F_1, \ldots, F_n$ with respect to Φ. If

$$F_r = \sum_{t=1}^{n} f_{tr} F_t^* \ , \quad f_{tr} \in Q \ , \ r = 1, \ldots, n,$$

the Gramian matrix of Φ_η with respect to the base $F_1, \ldots, F_n$ is given by

$$(f_{rs})_{1 \le r,s \le n} \in \mathrm{GL}_n(Q) \ .$$

(Necessarily, one also has $\Delta = \sum_{r=1}^{n} F_r^* \otimes F_r$.) For every $y \in K^N$ the induced K-linear form $\eta(y) : P(y) \to K$ is a $P(y)$-base of $E(y) = \mathrm{Hom}_K(P(y),K)$ and $\Phi_{\eta(y)}$ is a non-degenerate symmetric bilinear form on the fiber algebra $P(y)$. Its Gramian matrix, using the residue classes of $F_1, \ldots, F_n$ as K-base of $P(y)$, is

$$(f_{rs}(y))_{1 \le r,s \le n} \in \mathrm{GL}_n(K) \ .$$

Now, let K be a real closed field. Then the signature of the form $\Phi_{\eta(y)}$ is, by the Rigidity Theorem 1.3, independent of the K-rational point $y \in K^N$.

[5] That such a P-base exists is a priori clear since E is a reflexive P-module of rank 1 and P is factorial.

4.2 Definition Let K be a real closed field and let $T : K^N \to K^N$, $x \mapsto y = T(x)$, be a finite polynomial mapping with corresponding finite K-algebra homomorphism $\tau : K[Y] \to K[X]$. Then the mapping degree

$$\delta_Y^X(T) = \delta_Y^X(\tau)$$

of T (or of τ) is the constant signature $\operatorname{sign}\Phi_{\eta(y)}$ of the symmetric bilinear forms $\Phi_{\eta(y)}$ on the fiber algebras $P(y)$, $y \in K^N$, described above.

4.3 Remark *In the situation of* Definition 4.2 *the mapping degree can be defined for an arbitrary ordered field K*, because in this more general situation the symmetric bilinear forms $\Phi_\eta(y)$, $y \in K^N$, also have constant signature. To prove this, one may choose an arbitrary real closed field extension $\hat{K}$ of K (cf. Remark 3.3) and consider the canonical extension $\hat{T} : \hat{K}^N \to \hat{K}^N$ defined by the same polynomials as T with corresponding $\hat{K}$-algebra homomorphism $\hat{\tau} := \hat{K} \otimes_K \tau : \hat{K}[Y] \to \hat{K}[X]$. It follows that, for an arbitrary extension $K \subseteq L$ of ordered fields, the mapping degrees of τ and its extension $T_{(L)} : L^N \to L^N$ coincide. In particular, the mapping degree $\delta_X^Y(T)$ is the signature of the symmetric matrix $(f_{rs})_{1\le r,s\le n} \in \mathrm{GL}_n(K(Y))$ from above, where the rational function field $K(Y)$ is equipped with an arbitrary order which extends the order of K and turns $K(Y)$ into an ordered field.

The following important result will be used frequently. For its proof, see Theorem 4.2 of [11].

4.4 Lemma *Let $\tau : K[Y] \to K[X]$ be, as above, a finite homomorphism of polynomial algebras over K in N variables. Then*

$$\mathrm{tr}_Q^P = \mathcal{J} \cdot \eta_Y^X \,,$$

where

$$\mathcal{J} := \frac{\partial(T_1,\ldots,T_N)}{\partial(X_1,\ldots,X_N)} = \frac{\partial(\tau(Y_1),\ldots,\tau(Y_N))}{\partial(X_1,\ldots,X_N)}$$

denotes the functional determinant of τ (with respect to the coordinates X and Y).

Lemma 4.4 implies

$$\mathrm{tr}_K^{P(y)} = \mathcal{J}(y) \cdot \eta(y) \,, \quad y \in K^N \,,$$

where $\mathcal{J}(y)$ denotes the residue class of $\mathcal{J}$ in the fiber algebra $P(y)$.

An immediate consequence is the following theorem which shows that, in case $K = \mathbb{R}$, the algebraic mapping degree according to Defintion 4.2 coincides with the topological mapping degree, cf. Theorem 11.C.5 of [17], for instance. Recall that a finite polynomial mapping $T : \mathbb{R}^N \to \mathbb{R}^N$ can also be considered as an analytical proper mapping of oriented real analytical manifolds.

4.5 Theorem *Let K be a real closed field and let $T : K^N \to K^N$, $x \mapsto y = T(x)$, be a finite polynomial mapping with corresponding finite K-algebra homomorphism $\tau : K[Y] \to K[X]$ and with functional determinant $\mathcal{J} = \partial(T_1,\ldots,T_N)/\partial(X_1,\ldots,X_N) \in K[X]$. Furthermore, let $y \in K^N$ be a point such that T is unramified in all points $x \in T^{-1}(y)$, that is, $\mathcal{J}(x) \neq 0$ for all $x \in T^{-1}(y)$. Then,*

$$\delta_Y^X(T) = \sum_{x \in T^{-1}(y)} \operatorname{sign}\mathcal{J}(x) \,.$$

Since $\mathcal{J} \neq 0$ and hence $\mathrm{N}_{K[Y]}^{K[X]}(\mathcal{J}) \neq 0$, we have

$$T(\mathrm{V}_K(\mathcal{J})) \subseteq \mathrm{V}_K(\mathrm{N}_{K[Y]}^{K[X]}(\mathcal{J})) \subset K^N ,$$

where $\mathrm{V}_K(\mathcal{J}) = \{x \in K^N \mid \mathcal{J}(x) = 0\}$. Thus, there are always points $y \in K^N$ satisfying the required assumption of Theorem 4.5.

Proof of Theorem 4.5: Let $y \in K^N$ be as in the theorem. By Definition 4.2, we have to show

$$\operatorname{sign} \Phi_{\eta(y)} = \sum_{x \in T^{-1}(y)} \operatorname{sign} \mathcal{J}(x) .$$

For this, we consider the decomposition $A = A_1 \times \cdots \times A_r$ of the fiber algebra $A = P(y) = P/\mathfrak{m}_y P$ in its local components. Corresponding to this, there are decompositions $\eta(y) = (\eta_1, \ldots, \eta_r)$, $\mathrm{tr}_K^A = (\mathrm{tr}_K^{A_1}, \ldots, \mathrm{tr}_K^{A_r})$ and $\mathcal{J}(y) = (\mathcal{J}(y)_1, \ldots, \mathcal{J}(y)_r)$ of $\eta(y)$, tr_K^A and of the residue class of the functional determinant $\mathcal{J}(y)$. Hence, $\Phi_{\eta(y)} = \Phi_{\eta_1} \oplus \cdots \oplus \Phi_{\eta_r}$ and $\operatorname{sign} \Phi_{\eta(y)} = \operatorname{sign} \Phi_{\eta_1} + \cdots + \operatorname{sign} \Phi_{\eta_r}$. By Theorem 3.2, $\operatorname{sign} \Phi_{\eta_i} = 0$ for all components A_i with residue class field $\neq K$. The components with residue class field K correspond to the points $x \in T^{-1}(y) \subseteq K^N$. Since, by assumption, T is unramified in these points, these components all coincide with K. By the above decomposition of A and Lemma 4.4, $\mathrm{tr}_K^{A_i} = \mathcal{J}(y)_i \eta_i$ for $i = 1, \ldots, r$. Hence, if A_i is the component associated to a point $x \in T^{-1}(y)$, then $\mathcal{J}(y)_i = \mathcal{J}(x)$ and $\mathrm{tr}_K^{A_i} = \mathcal{J}(x)\eta_i$, and therefore $1 = \operatorname{sign} \mathrm{tr}_K^{A_i} = \operatorname{sign} \mathcal{J}(x) \cdot \operatorname{sign} \eta_i$. Thus, $\operatorname{sign} \eta_i = \operatorname{sign} \mathcal{J}(x)$. Then, $\sum_{i=1}^r \operatorname{sign} \eta_i = \sum_{x \in T^{-1}(y)} \operatorname{sign} \mathcal{J}(x)$ as stated. □

We emphasize that in Theorem 4.5 we only assume that $\tau : K[Y] \to K[X]$ is unramified in the K-rational points of the fiber algebra $P(y)$.

A direct consequence of Theorem 4.5 is the following multiplication formula

$$\delta_Z^X(S \circ T) = \delta_Y^X(T)\, \delta_Z^Y(S)$$

for the mapping degree of the composition

$$K^N \xrightarrow{T} K^N \xrightarrow{S} K^N , \quad x \longmapsto y = T(x) , \; y \longmapsto z = S(y) ,$$

of two finite polynomial mappings $T, S : K^N \to K^N$. To show this, one chooses a point $z \in K^N$ such that the functional determinant

$$\frac{\partial((S \circ T)_1, \ldots, (S \circ T)_N)}{\partial(X_1, \ldots, X_N)} = \left(\frac{\partial(S_1, \ldots, S_N)}{\partial(Y_1, \ldots, Y_N)} \right) (T_1, \ldots, T_N) \cdot \frac{\partial(T_1, \ldots, T_N)}{\partial(X_1, \ldots, X_N)}$$

does not vanish at all the points of the fiber $(S \circ T)^{-1}(z) = T^{-1}(S^{-1}(z))$. The multiplication formula implies in particular that, if T or S is an isomorphism, we have

$$\delta_Z^X(S \circ T) = \operatorname{sign} \left(\frac{\partial(T_1, \ldots, T_N)}{\partial(X_1, \ldots, X_N)} \right) \delta_Z^Y(S)$$

or

$$\delta_Z^X(S \circ T) = \delta_Y^X(T) \operatorname{sign} \left(\frac{\partial(S_1, \ldots, S_N)}{\partial(Y_1, \ldots, Y_N)} \right) .$$

One of the most important consequences of Theorem 3.4 in connection with the mapping degree is the following theorem, which corresponds to a well-known result in real analysis:

4.6 Theorem *Let K be a real closed field and let $T : K^N \to K^N$ be a finite polynomial mapping. If the mapping degree $\delta(T)$ of T is $\neq 0$, then T is surjective.*

§ 5 The Mapping Degree of the Vieta Mappings

We want to apply the last Theorem 4.6 to the Vieta mappings. As in the introduction, $\mathbf{m} = (m_1, \ldots, m_r)$ denotes an r-tuple of positive integers and $|\mathbf{m}| = m_1 + \cdots + m_r$. With this notation, the Vieta mapping is given by

$$\mathrm{V}_{\mathbf{m}} : K^{\mathbf{m}} = K^{m_1} \times \cdots \times K^{m_r} \longrightarrow K^{|\mathbf{m}|} ,$$

where an r-tuple $(F_1, \ldots, F_r)$ of monic polynomials of degrees $m_1, \ldots, m_r$, respectively, is mapped to their product $F_1 \cdots F_r$. Thereby, we identify an m-tuple $(x_1, \ldots, x_m) \in K^m$ with the monic polynomial

$$Z^m - x_1 Z^{m-1} + \cdots + (-1)^m x_m \in K[Z] .$$

5.1 Example The most classical case is the mapping

$$\mathrm{V}_{(1,\ldots,1)} : K \times \cdots \times K \longrightarrow K^r$$

with $m_1 = \cdots = m_r = 1$ and $|\mathbf{m}| = r$. For arbitrary elements $x_1, \ldots, x_r$ in a commutative ring we have

$$\prod_{i=1}^{r} (Z - x_i) = Z^r - \mathrm{S}_1(x) Z^{r-1} + \cdots + (-1)^r \mathrm{S}_r(x) ,$$

where

$$\mathrm{S}_i(x) = \mathrm{S}_i(x_1, \ldots, x_r) = \sum_{\mathcal{R} \subseteq [1,r], \#\mathcal{R} = i} x^{\mathcal{R}} , \quad x^{\mathcal{R}} := \prod_{j \in \mathcal{R}} x_j$$

is the i-th elementary symmetric function in $x = (x_1, \ldots, x_r)$.[6] Hence, the K-algebra homomorphism

$$\upsilon_{(1,\ldots,1)} : K[Y_1, \ldots, Y_r] \longrightarrow K[X_1, \ldots, X_r] ,$$

which corresponds to $\mathrm{V}_{(1,\ldots,1)}$ maps Y_i to the elementary symmetric function $S_i := \mathrm{S}_i(X_1, \ldots, X_r)$ of the indeterminates $X_1, \ldots, X_r$, $i = 1, \ldots, r$. This is a finite homomorphism of degree $[K(X) : K(Y)] = r!$ as considered in the previous section. A standard $K[Y]$-base of $K[X]$ is given by

$$X_1^{\nu_1} \cdots X_r^{\nu_r} , \quad 0 \leq \nu_i \leq r - i , \; i = 1, \ldots, r .$$

This is easily proved by induction on r. For the induction step one has to show that for the Vieta mapping $\mathrm{V}_{(1,r)} : K \times K^r \to K^{r+1}$ the corresponding K-algebra homomorphism $\upsilon_{(1,r)} : K[Y_1, \ldots, Y_{r+1}] \to K[X_1; V_1, \ldots, V_r]$ with $Y_i \mapsto X_1 V_{i-1} + V_i$, $i = 1, \ldots, r+1$, ($V_0 := 1$, $V_{r+1} := 0$) is finite and that $1, X_1, \ldots, X_1^{r-1}$ is a base of $K[X_1; V_1, \ldots, V_r]$ over $K[Y_1, \ldots, Y_{r+1}]$, cf. also [12], Theorem 54.13.

We note that the algebra homomorphism $\upsilon_{(1,\ldots,1)}$ is a homogeneous homomorphism of graded algebras if we define $\deg X_i = 1$ and $\deg Y_i = i$ for all $i = 1, \ldots, r$. The Poincaré series of $K[X]$ and $K[Y]$ are $(1-t)^{-r}$ and $\prod_{i=1}^{r} (1 - t^i)^{-1}$, respectively. The j-th coefficient of the Poincaré series

$$\mathcal{P}_{K[X]/\langle S \rangle} = \prod_{i=1}^{r} \frac{1 - t^i}{1 - t} = \prod_{i=1}^{r} (1 + t + \cdots + t^{i-1})$$

of the fiber algebra $K[X]/\langle S \rangle$ over $y = 0 \in K^r$, $S := (S_1, \ldots, S_r)$, is the number of elements of degree j in any homogeneous $K[Y]$-base of $K[X]$.

[6] For arbitrary integers $r \leq s$ we denote by $[r,s]$ the $\mathbb{Z}$-interval $\{t \in \mathbb{Z} \mid r \leq t \leq s\}$.

Later we shall use the fact that $K[S]$ is the algebra of invariants for the canonical operation of the symmetric group $\mathfrak{S}_r$ on the polynomial algebra $K[X]$, i.e. $K[X]^{\mathfrak{S}_r} = K[S]$. This is known as (a special case of) the Main Theorem on Elementary Symmetric Functions and has been used (as an obvious (?) result) at least since the time of Newton. These invariant theoretical aspects of the Vieta mappings are discussed more intensively in [2].

The general Vieta mapping $\mathrm{V}_{\mathbf{m}}$ is the composition of the mappings

$$\mathrm{V}_{(m_1 \cdots m_i, m_{i+1})} \times \mathrm{id}_{K^{m_{i+2}} \times \cdots \times K^{m_r}} , \quad i = 1, \ldots, r-1 .$$

Therefore, we will usually restrict our considerations to the case $r = 2$ and set then $k := m_1$, $\ell := m_2$, $m := k + \ell$. Furthermore, we denote by $U = (U_1, \ldots, U_k)$, $V = (V_1, \ldots, V_\ell)$ and $W = (W_1, \ldots, W_m)$ the variables for the coordinate functions on K^k, K^ℓ and K^m, respectively. Then the Vieta mapping

$$\mathrm{V}_{(k,\ell)} : K^k \times K^\ell \longrightarrow K^m , \quad (F, G) \longmapsto FG ,$$

corresponds to the K-algebra homomorphism $\upsilon_{(k,\ell)} : K[W] \to K[U;V]$ with

$$\upsilon_{(k,\ell)}(W_\mu) = \sum_{\kappa+\lambda=\mu} U_\kappa V_\lambda , \quad \mu = 1, \ldots, m ,$$

where we set $U_0 = V_0 = 1$ and $U_\kappa = V_\lambda = 0$ for $\kappa \notin [0,k]$ and $\lambda \notin [0,\ell]$.

To understand the homomorphism $\upsilon_{(k,\ell)}$ we interpret U, V and W as follows: We choose new indeterminates $X = (X_1, \ldots, X_m)$ and set $U_\kappa := \mathrm{S}_\kappa(X_1, \ldots, X_k)$, $V_\lambda := \mathrm{S}_\lambda(X_{k+1}, \ldots, X_m)$,$W_\mu := \mathrm{S}_\mu(X_1, \ldots, X_m)$ (see Example 5.1 above). Then all algebras we are considering here are graded subalgebras of the graded polynomial algebra $K[X]$ with $\deg X_\mu = 1$, $\deg U_\kappa = \kappa$, $\deg V_\lambda = \lambda$ and $\deg W_\mu = \mu$, and the homomorphism $\upsilon_{(k,\ell)}$ is identified with the canonical inclusion mapping $K[W] \hookrightarrow K[U;V] \subseteq K[X]$. By Example 5.1, the algebra $K[X]$ is free over $K[W]$ of rank $m!$ and free over $K[U;V]$ of rank $k!\,\ell!$. From this we may derive directly:

5.2 Lemma *The algebra $K[U;V]$ is free over $K[W]$ of rank $\binom{m}{k} = \binom{m}{\ell}$, i.e. the Vieta mapping $\mathrm{V}_{(k,\ell)}$ is finite with sheet number $\binom{m}{k}$. The Poincaré series of the fiber algebra $K[U;V]/\langle W \rangle$ over $w = 0 \in K^m$ is*

$$\mathcal{P}_{K[U;V]/\langle W \rangle} = \begin{bmatrix} m \\ k \end{bmatrix} := \frac{(1-t^m)\cdots(1-t^{m-k+1})}{(1-t)\cdots(1-t^k)} .$$

A family of homogeneous polynomials in $K[U;V]$ is a $K[W]$-base if and only if the family of their residue classes in $K[U;V]/\langle W \rangle$ is a K-base of this algebra (see the following proof). Therefore the j-th coefficient of the Poincaré series $\begin{bmatrix} m \\ k \end{bmatrix}$ is the number of elements of degree j in any homogeneous $K[W]$-base of $K[U;V]$. Further, we remark that the polynomials $\begin{bmatrix} m \\ k \end{bmatrix}$ in Lemma 5.2 are sometimes called the Gauss polynomials.

Proof of Lemma 5.2: Since $[K(X) : K(W)] = m!$ and $[K(X) : K(U;V)] = k!\,\ell!$, the degree formula for field extensions yields $[K(U;V) : K(W)] = \binom{m}{k}$. Hence, $K[U;V]$ is a $K[W]$-module of rank $\binom{m}{k}$. Furthermore, because $K[X]/\langle W \rangle$ is a free $K[U;V]/\langle W \rangle$-module, we get $\mathcal{P}_{K[X]/\langle W \rangle} = \mathcal{P}_{K[X]/\langle U;V \rangle} \mathcal{P}_{K[U;V]/\langle W \rangle}$, hence

$$\mathcal{P}_{K[U;V]/\langle W \rangle} = \frac{\mathcal{P}_{K[X]/\langle W \rangle}}{\mathcal{P}_{K[X]/\langle U;V \rangle}} = \frac{(1-t)\cdots(1-t^m)}{(1-t)\cdots(1-t^k)(1-t)\cdots(1-t^\ell)} = \begin{bmatrix} m \\ k \end{bmatrix}$$

and, in particular, $\mathrm{Dim}_K K[U;V]/\langle W\rangle = \mathcal{P}_{K[U;V]/\langle W\rangle}(1) = \binom{m}{k}$. By the Nakayama Lemma for graded modules, any system of homogeneous polynomials in $K[U;V]$ whose residue classes in $K[U;V]/\langle W\rangle$ form a K-base of this algebra is a (minimal) system of generators of the $K[W]$-module $K[U;V]$ with rank $\binom{m}{k}$. Then such a minimal system of generators is necessarily a $K[W]$-base. □

Incidentally, it is possible to find explicitly with combinatorial methods a homogeneous $K[W]$-base of $K[U;V]$, but we do not need it. From Lemma 5.2 we obtain the following general result: *The Vieta mapping* $\mathrm{V}_{\mathbf{m}} : K^{\mathbf{m}} \to K^{|\mathbf{m}|}$ *is a finite polynomial mapping with sheet number equal to the polynomial coefficient* $\binom{|\mathbf{m}|}{\mathbf{m}} = \binom{|\mathbf{m}|}{m_1,\ldots,m_r}$. *The fiber algebra over* $0 \in K^{|\mathbf{m}|}$ *has Poincaré series* $\left[\begin{smallmatrix}|\mathbf{m}|\\ \mathbf{m}\end{smallmatrix}\right] = \left[\begin{smallmatrix}|\mathbf{m}|\\ m_1,\ldots,m_r\end{smallmatrix}\right]$, which is a generalized Gauss polynomial (in the same way that the polynomial coefficient $\binom{|\mathbf{m}|}{\mathbf{m}} = \binom{|\mathbf{m}|}{m_1,\ldots,m_r}$ is a generalized binomial coefficient).

5.3 Example An immediate corollary of Lemma 5.2 is the following result: *If K is a 2-field, i.e. if every prime polynomial over K of degree > 1 has even degree, then the degree of every prime polynomial is a power of* 2. By Example 4.1, the Vieta mapping $\mathrm{V}_{(k,\ell)} : K^k \times K^\ell \to K^m$, $m := k+\ell$, is surjective if its sheet number $\binom{m}{k}$ is odd. Now, let $m = 2^\alpha n$, $\alpha \in \mathbb{N}$, $n > 1$ odd, so that m is not a power of 2. To prove the corollary, it is enough to show that there is a $k \in \mathbb{N}^*$, $0 < k < m$, such that $\binom{m}{k}$ is odd. Now, over the field $\mathbb{F}_2 = \mathbb{Z}/\mathbb{Z}2$ we have $(1+t)^m = (1+t)^{2^\alpha n} = (1+t^{2^\alpha})^n = 1 + nt^{2^\alpha} + \cdots$ and hence $k := 2^\alpha$ is a possible choice. – Of course, the above result over a 2-field K is equivalent to the statement that the degree of any finite field extension of K is a power of 2. This can also be shown using Galois (and group) theory. We leave this as an exercise to the reader. – Adopting a proposal of E. Artin, it follows rather easily from the result of this example that the field $\mathbb{C}_K$ of complex numbers over a real closed field K is algebraically closed, cf. Theorem 5.7: Let L be a finite algebraic extension of $\mathbb{C}_K$. We have to show $L = \mathbb{C}_K$. For this we may moreover assume that L is Galois over $\mathbb{C}_K$. By the result of this example, the degree $[L : \mathbb{C}_K]$ is a power of 2 and hence the Galois group $\mathrm{Gal}_{\mathbb{C}_K}(L)$ a finite 2-group. If this group is non-trivial, then it has a subgroup of index 2, which has as its field of invariants a quadratic extension of $\mathbb{C}_K$. But this is impossible: One sees immediately that any quadratic equation over $\mathbb{C}_K$ has a solution in $\mathbb{C}_K$ (using the property of K that any positive number in K has a square root in K). – For further properties of 2-fields see [16].

We return to the case $r = 2$ and, with regard to Theorem 4.5, determine the functional determinant $\mathcal{J} = \partial(W_1,\ldots,W_m)/\partial(U_1,\ldots,U_k;V_1,\ldots,V_\ell)$. The transpose of the Jacobian matrix is a Sylvester matrix with determinant

$$\begin{vmatrix} 1 & V_1 & \cdots & V_\ell & & \\ & \ddots & \ddots & & \ddots & \\ & & 1 & V_1 & \cdots & V_\ell \\ 1 & U_1 & \cdots & U_k & & \\ & \ddots & \ddots & & \ddots & \\ & & 1 & U_1 & \cdots & U_k \end{vmatrix} = \mathrm{Res}\,(\mathsf{F},\mathsf{G})$$

where

$$\mathsf{F} := X^k - U_1X^{k-1} + \cdots + (-1)^k U_k\,, \quad \mathsf{G} := X^\ell - V_1X^{\ell-1} + \cdots + (-1)^\ell V_\ell\,.$$

(The submatrix containing the entries V_λ consists of k rows, and that containing the

entries U_κ consists of ℓ rows.) Thus,

$$\mathcal{J}(F,G) = \mathrm{Res}(F,G)$$

for two monic polynomials $(F,G) \in K^k \times K^\ell$. In particular, $\upsilon_{(k,\ell)}$ is unramified in (F,G) if and only if the polynomials F and G are coprime. Furthermore, *if $H \in K^m$ is a monic separable polynomial of degree m*, cf. Example 2.1, *then $\upsilon_{(k,\ell)}$ is unramified in all points of the fiber* $\mathrm{V}_{(k,\ell)}^{-1}$. For such a polynomial H, the mapping $\upsilon_{(k,\ell)}$ is also unramified in the non-K-rational points of the fiber over H, i.e. the fiber over H is a separable K-algebra. For this, one extends the K-algebra homomorphism $\upsilon_{(k,\ell)}$ to an L-algebra homomorphism, where L is a splitting field of the fiber algebra, and observes that H remains separable over any extension field of K. For the general Vieta mapping we derive from this:

5.4 Lemma *The value of the functional determinant of the Vieta mapping $\mathrm{V}_{\mathbf{m}} : K^{\mathbf{m}} \to K^{|\mathbf{m}|}$ in the point $(F_1,\ldots,F_r)$ is $\prod_{1\le i<j\le r}\mathrm{Res}(F_i,F_j)$, and $\upsilon_{\mathbf{m}}$ is unramified in $(F_1,\ldots,F_r)$ if and only if the polynomials $F_1,\ldots,F_r$ are pairwise coprime. – If $H \in K^{|\mathbf{m}|}$ is a monic separable polynomial, then $\upsilon_{\mathbf{m}}$ is unramified in all points of its fiber over H (including the non-K-rational points), i.e. the fiber algebra over H is a (finite) separable K-algebra.*

A special case of Lemma 5.4 is the (well-known) formula for the functional determinant of the classical Vieta mapping $\mathrm{V}_{(1,\ldots,1)} : K^r \to K^r$

$$\prod_{1\le i<j\le r}\mathrm{Res}(X-X_i,X-X_j) = \prod_{1\le i<j\le r}(X_i-X_j) = (-1)^{\binom{r}{2}}\mathcal{V}(X_1,\ldots,X_r)\ ,$$

where $\mathcal{V}(X_1,\ldots,X_r)$ denotes the Vandermonde determinant.

With the help of Theorem 4.5, we now compute the mapping degree of $\upsilon_{(k,\ell)}$ for a (real closed) ordered field K. For this, we can use, by Lemma 5.4, the fiber over the (separable) polynomial $H := \prod_{i=1}^m (X-i) \in K[X]$. For a subset $\mathcal{R} \subseteq [1,m]$ define $H_\mathcal{R} := \prod_{i\in\mathcal{R}}(X-i)$. The preimages of H under $\mathrm{V}_{(k,\ell)}$ are given by the pairs $(H_\mathcal{R}, H_{\mathcal{R}'})$, $\mathcal{R} \subseteq [1,m]$, $\#\mathcal{R} = k$, $\mathcal{R}' := [1,m] \setminus \mathcal{R}$. Thus, by Theorem 4.5,

$$\delta_{(k,\ell)} = \sum_{\#\mathcal{R}=k} \mathrm{sign}\,\mathrm{Res}\,(H_\mathcal{R}, H_{\mathcal{R}'})\ .$$

Since $\mathrm{Res}\,(H_\mathcal{R}, H_{\mathcal{R}'}) = \prod_{(i,j)\in\mathcal{R}\times\mathcal{R}'}(i-j)$, we get

$$\begin{aligned}\mathrm{sign}\,\mathrm{Res}\,(H_\mathcal{R}, H_{\mathcal{R}'}) &= \mathrm{sign}\begin{pmatrix} 1 & \cdots & \ell & \ell+1 & \cdots & \ell+k \\ j_1 & \cdots & j_\ell & i_1 & \cdots & i_k \end{pmatrix} \\ &= (-1)^{\Sigma\mathcal{R}' - \binom{\ell+1}{2}} = (-1)^{\Sigma\mathcal{R} - \binom{k+1}{2} - k\ell}\end{aligned}$$

if $\mathcal{R} = \{i_1,\ldots,i_k\}$, $1 < i_1 < \cdots < i_k$, $\mathcal{R}' = \{j_1,\ldots,j_\ell\}$, $j_1 < \cdots < j_\ell$, and $\Sigma\mathcal{R} := \sum_{i\in\mathcal{R}} i$. Hence,

$$(-1)^{\binom{k+1}{2}+k\ell}\,\delta_{(k,\ell)} = \sum_{\#\mathcal{R}=k}(-1)^{\Sigma\mathcal{R}}\ .$$

In order to determine this value consider the polynomial

$$\Phi(z,t) = \sum_{\mathcal{R}\subseteq[1,m]} z^{\Sigma\mathcal{R}} t^{\#\mathcal{R}} = (1+zt)(1+z^2t)\cdots(1+z^mt)\ .$$

The coefficient of t^k in the polynomial $\Phi(-1,t) = (1-t^2)^{[m/2]}(1-t)^{m-2[m/2]}$ therefore equals the difference between the number of subsets $\mathcal{R}$ with $\#\mathcal{R} = k$ and even sum $\sum\mathcal{R}$ and those $\mathcal{R}$ with $\#\mathcal{R} = k$ and odd sum $\sum\mathcal{R}$. It follows

$$(-1)^{\binom{k+1}{2}+k\ell}\,\delta_{(k,\ell)} = \begin{cases} (-1)^{k/2}\binom{m/2}{k/2}, & \text{if } k,\ell \equiv 0\,(2)\,, \\ 0, & \text{if } k,\ell \equiv 1\,(2)\,, \\ (-1)^{[k/2]+1}\binom{[m/2]}{[k/2]}, & \text{if } k \equiv 1\,(2)\,,\ \ell \equiv 0\,(2)\,, \\ (-1)^{k/2}\binom{[m/2]}{k/2}, & \text{if } k \equiv 0\,(2)\,,\ \ell \equiv 1\,(2)\,. \end{cases}$$

These formulas can be summarized in the following way:

5.5 Theorem *Let K be a (real closed) ordered field. Then the mapping degree $\delta_{(k,\ell)}$ of the Vieta mapping $\mathrm{V}_{(k,\ell)}$, $k,\ell \in \mathbb{N}^*$, vanishes if and only if $k,\ell \equiv 1\,(2)$. Otherwise, one has*

$$\delta_{(k,\ell)} = \binom{[(k+\ell)/2]}{[k/2]}\,.$$

Theorem 5.5 combined with Theorem 4.6 shows that for a real closed field the mappings $\mathrm{V}_{(2,\ell)}$ are always surjective. We have proved the Fundamental Theorem of Algebra in its original version.[7]

5.6 Fundamental Theorem of Algebra *Every polynomial of degree ≥ 2 over a real closed field K has a quadratic factor in $K[X]$.*

Theorem 5.6 is certainly equivalent to the statement that every irreducible polynomial over a real closed field K has degree ≤ 2. Since, furthermore, any positive number in a real closed field K has a square root in K, for any prime polynomial $\pi \in K[X]$ of degree 2, the quadratic field extension $K[X]/\langle\pi\rangle$ is isomorphic to the field $\mathbb{C}_K = K[i] = K[\sqrt{-1}] \cong K[X]/\langle X^2+1\rangle$ of complex numbers over K, and this is, up to isomorphism, the only non-trivial algebraic field extension of K. Hence, Theorem 5.6 is equivalent to the following version:

5.7 Fundamental Theorem of Algebra (Complex Version) *Let K be a real closed field K. Then the field $\mathbb{C}_K = K[i] = K[\sqrt{-1}]$ of complex numbers over K is algebraically closed.*

Theorem 5.5 together with the multiplicativity of the mapping degree for compositions (cf. remark after Theorem 4.5) gives the following formula for the mapping degree $\delta_{\mathbf{m}} = \delta_{(m_1,\ldots,m_r)}$, $r \in \mathbb{N}^*$, of an arbitrary Vieta mapping $\mathrm{V}_{\mathbf{m}}$ (we use the notation $[\mathbf{m}/2] := ([m_1/2],\ldots,[m_r/2])$):

$$\delta_{\mathbf{m}} = \prod_{i=1}^{r-1} \delta_{(m_1+\cdots+m_i,m_{i+1})} = \begin{cases} \binom{|[\mathbf{m}/2]|}{[\mathbf{m}/2]}, & \text{if } m_i \equiv 1\,(2) \text{ for at most one } i\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

In particular, the mapping degree $\delta_{\mathbf{m}}$ is always non-negative and does not change when the components of $\mathbf{m} = (m_1,\ldots,m_r)$ are permuted. The last formula together with Theorem 4.6 implies that over a real closed field K the *Vieta mapping* $\mathrm{V}_{\mathbf{m}} : K^{\mathbf{m}} \to K^{|\mathbf{m}|}$ *is surjective if the tuple* $\mathbf{m}$ *has at most one odd component*.

[7] The purely topological aspects of this proof in case $K = \mathbb{R}$ are described in [14].

5.8 Remark The Fundamental Theorem of Algebra in its complex version 5.7 also follows directly from the interpretation of a polynomial mapping $T : \mathbb{C}_K^N \to \mathbb{C}_K^N$ over the complex numbers $\mathbb{C}_K$ of an ordered field K as a polynomial mapping $\rho^*(T) : K^{2N} \to K^{2N}$ (due to the identification $\mathbb{C}_K = K \oplus Ki = K \times K$). If T is finite, *this corresponding mapping over K is also finite and furthermore has a positive mapping degree and hence is surjective*. This method was already used by S. Eilenberg and I. Niven, cf. [3].

We are only interested in the affine case.[8] Then, passing from a mapping over $\mathbb{C}_K$ to one over K can be described algebraically in the following way: The extension functor $B \rightsquigarrow \mathbb{C}_K \otimes_K B$ from the category of K-algebras to the category of $\mathbb{C}_K$-algebras possesses a left-adjoint functor $A \rightsquigarrow \rho(A)$ from the category of $\mathbb{C}_K$-algebras to the category of K-algebras. Thus,

$$\mathrm{Hom}_{K\text{-alg}}(\rho(A), B) = \mathrm{Hom}_{\mathbb{C}_K\text{-alg}}(A, \mathbb{C}_K \otimes_K B)$$

for arbitrary $\mathbb{C}_K$-algebras A and K-algebras B. In other words: For every $\mathbb{C}_K$-algebra A there is a K-algebra $\rho(A)$ and a $\mathbb{C}_K$-algebra homomorphism $\chi_A : A \to \mathbb{C}_K \otimes_K \rho(A)$ such that to any K-algebra B and any $\mathbb{C}_K$-algebra homomorphism $\psi : A \to \mathbb{C}_K \otimes_K B$ there is a unique K-algebra homomorphism $\varphi : \rho(A) \to B$ with $\psi = (\mathbb{C}_K \otimes \varphi) \circ \chi_A$. In particular,

$$K\text{-}\mathrm{Spec}\,\rho(A) = \mathrm{Hom}_{K\text{-alg}}(\rho(A), K) = \mathrm{Hom}_{\mathbb{C}_K\text{-alg}}(A, \mathbb{C}_K) = \mathbb{C}_K\text{-}\mathrm{Spec}\,A\ .$$

The covariant functor $A \rightsquigarrow \rho(A)$ associates to a $\mathbb{C}_K$-algebra homomorphism $\alpha : C \to D$ the K-algebra homomorphism $\rho(\alpha) : \rho(C) \to \rho(D)$ with $\chi_D \circ \alpha = (\mathbb{C}_K \otimes \rho(\alpha)) \circ \chi_C$. Both, α and $\rho(\alpha)$ induce the same mapping from $\mathbb{C}_K$-Spec $D = K$-Spec $\rho(D)$ into $\mathbb{C}_K$-Spec $C = K$-Spec $\rho(C)$.

The $\mathbb{C}_K$-algebra $\rho(A)$ may be described explicitly as follows: One has

$$\rho(A) = (A \otimes_{\mathbb{C}_K} A)^\kappa \subseteq A \otimes_{\mathbb{C}_K} \overline{A}\ ,$$

where $\overline{A}$ denotes the anti-$\mathbb{C}_K$-algebra of A (with the scalar multiplication $(z,a) \mapsto \overline{z}a$ instead of $(z,a) \mapsto za$), $\kappa : A \otimes_{\mathbb{C}_K} A \to A \otimes_{\mathbb{C}_K} A$ the inversion $x \otimes y \mapsto y \otimes x$ of the factors (this "conjugation" is an involutive anti-$\mathbb{C}_K$-algebra endomomorphism of $A \otimes_{\mathbb{C}_K} A$), $(A \otimes_{\mathbb{C}_K} A)^\kappa$ the K-algebra of κ-invariants, and $\chi_A : A \to \mathbb{C}_K \otimes_K \rho(A) = A \otimes_{\mathbb{C}_K} A$ is the canonical embedding. Moreover, to $\psi : A \to \mathbb{C}_K \otimes_K B$ one associates the K-algebra homomorphism $\varphi : \rho(A) \to B$ which is the restriction of the induced $\mathbb{C}_K$-algebra homomorphism $A \otimes_{\mathbb{C}_K} \overline{A} \to \mathbb{C}_K \otimes_K B, x \otimes y \mapsto \psi(x)\overline{\psi(y)}$, to the algebra of invariants $\rho(A) = (A \otimes_{\mathbb{C}_K} A)^\kappa \to (\mathbb{C}_K \otimes_K B)^\kappa = B$. (The conjugation κ on $\mathbb{C}_K \otimes_K B$ is $\kappa \otimes B$ with the conjugation κ of $\mathbb{C}_K$.)

If $A := \mathbb{C}_K[Z_1, \ldots, Z_N] = \mathbb{C}_K[Z]$ is a polynomial algebra in N variables, then

$$A \otimes_{\mathbb{C}_K} \overline{A} = \mathbb{C}_K[Z_1, \overline{Z}_1, \ldots, Z_N, \overline{Z}_N] = \mathbb{C}_K[Z; \overline{Z}]$$

is a polynomial algebra in $2N$ variables with $Z_j = Z_j \otimes 1$ and $\overline{Z}_j = \kappa(Z_j) = 1 \otimes Z_j$, $j = 1, \ldots, N$. Thus, $zZ_j = Z_j \otimes 1$ and $z\overline{Z}_j = 1 \otimes \overline{z}Z_j$. Hence, $\kappa(F(Z; \overline{Z})) = \overline{F}(\overline{Z}; Z)$, where the polynomial denoted by $\overline{F}$ is obtained from F by conjugating the coefficients. Therefore,

$$\rho(A) = (A \otimes_{\mathbb{C}_K} \overline{A})^\kappa = K[X_1, Y_1, \ldots, X_N, Y_N] = K[X; Y]$$

with

$$X_j = \frac{1}{2}(Z_j + \overline{Z}_j)\ ,\ Y_j = \frac{1}{2i}(Z_j - \overline{Z}_j)\ ,\ Z_j = X_j + iY_j\ ,\ \overline{Z}_j = X_j - iY_j\ .$$

To a polynomial mapping $T : \mathbb{C}_K^N \to \mathbb{C}_K^N, z \mapsto w = T(z)$, belonging to the $\mathbb{C}_K$-algebra homomorphism $\tau : \mathbb{C}_K[W] \to \mathbb{C}_K[Z], W_j \mapsto T_j$, $j = 1, \ldots, N$, corresponds the polynomial mapping

$$\rho^*(T) : K^{2N} = \mathbb{C}_K^N \longrightarrow \mathbb{C}_K^N = K^{2N}\ ,$$

where

$$(x,y) = (x_1, y_1, \ldots, x_N, y_N) = (x_1 + iy_1, \ldots, x_N + iy_N) = (z_1, \ldots, z_N) = z$$

[8] For a more general discussion of the following construction see [13, Section 3.2.1].

is mapped to

$$\begin{aligned} w = T(z) &= (T_1(z),\dots,T_N(z)) = (T_1(x_1+iy_1),\dots,T_N(x_N+iy_N)) \\ &= (u_1(x,y)+iv_1(x,y),\dots,u_N(x,y)+iv_N(x,y)) \\ &= (u_1,v_1,\dots,u_N,v_N) = (u,v)\ . \end{aligned}$$

The corresponding K-algebra homomorphism

$$\rho(\tau) : K[U_1,V_1,\dots,U_N,V_N] \longrightarrow K[X_1,Y_1,\dots,X_N,Y_N]$$

is defined by $U_j \mapsto \frac{1}{2}\,(T_j(Z)+\overline{T}_j(\overline{Z}))$ and $V_j \mapsto \frac{1}{2i}\,(T_j(Z)-\overline{T}_j(\overline{Z}))$. It follows easily that

$$\begin{aligned} \frac{\partial(U_1,V_1,\dots,U_N,V_N)}{\partial(X_1,Y_1,\dots,X_N,Y_N)} &= \frac{\partial(T_1(Z),\dots,T_N(Z))}{\partial(Z_1,\dots,Z_N)} \cdot \frac{\partial(\overline{T}_1(\overline{Z}),\dots,\overline{T}_N(\overline{Z}))}{\partial(Z_1,\dots,Z_N)} \\ &= \frac{\partial(T_1,\dots,T_N)}{\partial(Z_1,\dots,Z_N)} \cdot \overline{\frac{\partial(T_1,\dots,T_N)}{\partial(Z_1,\dots,Z_N)}}\ . \end{aligned}$$

In particular, $\rho^*(T)$ is unramified in (x,y) if and only if T is unramified in z. In this case the functional determinant of $\rho^*(T)$ is the norm of the functional determinant of T and is therefore positive. For obvious reasons, $\tau : \mathbb{C}_K[W] \to \mathbb{C}_K[Z]$ is finite if and only if $\rho(\tau) : K[U,V] \to K[X,Y]$ is finite. The sheet number of $\rho(\tau)$ equals the square of the sheet number of τ. With these notations we obtain from Theorem 4.6:

5.9 Theorem *Let K be a real closed field and $\mathbb{C}_K = K[i]$ its field of complex numbers. Let $T : \mathbb{C}_K^N \to \mathbb{C}_K^N$ be a finite polynomial mapping with respect to the $\mathbb{C}_K$-algebra homomorphism $\tau : \mathbb{C}_K[W] \to \mathbb{C}_K[Z]$, $W_j \mapsto T_j(Z)$, $j = 1,\dots,N$. Then the mapping degree of the associated polynomial mapping $\rho^*(T) : K^{2N} \to K^{2N}$ is positive. In particular, T is surjective. – More precisely, the mapping degree equals the number of points of a fiber $T^{-1}(w)$, $w \in \mathbb{C}_K^N$, if τ is unramified in every point of this fiber.*

Of course, if K is only an ordered field and $T : \mathbb{C}_K^N \to \mathbb{C}_K^N$ is a finite polynomial mapping, the mapping degree of T is also positive. For this, one embeds K into a real closed field according to Remark 4.3 and applies Theorem 5.9. In any case, we also call the mapping degree of $\rho^*(T) : K^{2N} \to K^{2N}$ the mapping degree of T.

Theorem 5.9 is the geometric description of the fact that $\mathbb{C}_K$ is algebraically closed if K is real closed. Most directly, if $T \in \mathbb{C}_K[Z]$ is a polynomial of degree $n \in \mathbb{N}^*$ in one variable, the polynomial mapping $T : \mathbb{C}_K \to \mathbb{C}_K$, $z \mapsto T(z)$, is finite with sheet number n, and surjective by Theorem 5.9. In particular, *T has a zero in $\mathbb{C}_K$*. In the more general situation of Theorem 5.9, *the mapping degree is a posteriori the sheet number n of τ*. Since $\rho(\tau) : K[U;V] \to K[X;Y]$ has sheet number n^2 every fiber of $\rho(\tau)^* : \mathbb{A}_K^{2N} \to \mathbb{A}_K^{2N}$ ($\mathbb{A}_K^{2N} = \operatorname{Spec} K[X;Y]$ respectively, $\mathbb{A}_K^{2N} = \operatorname{Spec} K[U;V]$) over an unramified point $w \in \mathbb{C}_K^N = K^{2N}$ contains, in addition to the n K-rational points in K^{2N}, $n(n-1)/2$ further points with residue class field $\mathbb{C}_K$, the so-called complex points of the fiber.

A special case is given by the Vieta mappings $\mathrm{V}_{\mathbf{m}} : \mathbb{C}_K^{\mathbf{m}} \to \mathbb{C}_K^{|\mathbf{m}|}$, $\mathbf{m} = (m_1,\dots,m_r) \in (\mathbb{N}^*)^r$, $r \in \mathbb{N}^*$, over $\mathbb{C}_K$. If K is an ordered field, their mapping degrees coincide with their sheet numbers $\binom{|\mathbf{m}|}{\mathbf{m}}$ as mentioned before. Furthermore, if K is real closed, they are surjective.

§ 6 Euler's "Proof" of the Fundamental Theorem of Algebra

As described in the introduction, in his attempt to prove the Fundamental Theorem of Algebra, Euler considers the Vieta mappings $\mathrm{V}_{(k,k)} : K^k \times K^k \to K^{2k}$, $(F,G) \mapsto H = FG$,

where $k = 2^\gamma$ is a non-trivial 2-power, $\gamma \in \mathbb{N}^*$, and tries to show that these mappings are surjective for real closed fields K. Of course, this is a consequence of Theorem 4.6, since, by Theorem 5.5, the mapping degree $\delta_{(2^\gamma,2^\gamma)} = \binom{2^\gamma}{2^{\gamma-1}}$ of $V_{(k,k)}$ is positive. Euler proves only the following: There is a polynomial $E \in K[W_1,\ldots,W_{2k}]$, $E \neq 0$, such that every point $H \in K^{2k}$ (i.e. every monic polynomial of degree $2k$) with $E(H) \neq 0$ belongs to the image of $V_{(k,k)}$ (i.e. is a product of two monic polynomials of degree k). That is, Euler proves the Fundamental Theorem of Algebra only for the "generic case", cf. Theorem 6.1 below. This is the point which Gauss criticizes the most in his doctoral thesis [7] on the Fundamental Theorem of Algebra from 1799 and which he regards as the main gap of Euler's proof. For him there is no reason why the polynomials H with $E(H) = 0$ should also belong to the image of $V_{(k,k)}$.

First, we note that the surjectivity of $V_{(k,k)} : K^k \times K^k \to K^{2k}$ for all $k = 2^\gamma > 1$ and for all real closed fields K implies the Fundamental Theorem of Algebra, i.e. the fact that every non-constant polynomial over K possesses a factor of degree ≤ 2.

1. It suffices to show that every polynomial of degree 2^γ, $\gamma > 1$, is the product of polynomials of degree ≤ 2, since for an arbitrary polynomial $F \in K[X]$ the product $X^\nu \cdot F$ is of degree 2^γ for a suitable ν. If $X^\nu \cdot F$ is the product of polynomials of degree ≤ 2 then so is F.

2. The result that every polynomial of degree $k = 2^\gamma$, $\gamma > 1$, is the product of polynomials of degree ≤ 2 then follows easily by induction on γ, where one uses the surjectivity of $V_{(k,k)}$ for the induction step.

For the proof of the Fundamental Theorem of Algebra, it is obviously enough to show that every non-constant *separable* polynomial, i.e. every non-constant polynomial with no multiple factors, is the product of polynomials of degree ≤ 2. Therefore, it suffices to show that *every monic separable polynomial of degree* $2k$, $k = 2^\gamma > 1$, *belongs to the image of* $V_{(k,k)} : K^k \times K^k \to K^{2k}$. In Step 1, one considers instead of F a polynomial $(X-a_1)\cdots(X-a_\nu)F$ with pairwise distinct $a_1,\ldots,a_\nu$ that are not zeros of F. Then $(X-a_1)\cdots(X-a_\nu)F$ is separable if F is. We already know, by Example 5.3, that the degree of a prime polynomial over a real closed field (which is a 2-field) is a power of 2. Thus, it is even enough to show that the prime polynomials (which are separable in characteristic zero) belong to the image of $V_{(k,k)}$, $k = 2^\gamma$, $\gamma \in \mathbb{N}^*$.

For $K = \mathbb{R}$, Euler's gap is easily resolved: As mentioned before, the mapping $V_{(k,k)} : \mathbb{R}^k \times \mathbb{R}^k \to \mathbb{R}^{2k}$ is proper and, in particular, a closed mapping (with respect to the strong topologies). This is an immediate consequence of the Theorem of Bolzano-Weierstrass (which Euler, likewise d'Alembert, may have considered without further ado as self-evident or as an axiom (in the pre-Hilbert sense)). Since the complement of the zero set of any polynomial $F \in \mathbb{R}[W_1,\ldots,W_{2k}]$, $F \neq 0$, is dense in $\mathbb{R}^{2k}$, the set $D_{\mathbb{R}}(E) = \{H \in \mathbb{R}^{2k} \mid E(H) \neq 0\}$ for the polynomial E from above is also dense in $\mathbb{R}^{2k}$. Therefore, the image of $V_{(k,k)}$, which is a closed set and contains $D_{\mathbb{R}}(E)$, coincides with $\mathbb{R}^{2k}$.

To fill Euler's gap for an arbitrary real closed field with *purely algebraic* methods, we propose the following rather elementary method: As mentioned before, it suffices to show that every *separable* polynomial $H \in K^{2k}$ belongs to the image of $V_{(k,k)} : K^k \times$

$K^k \to K^{2k}$. The set of all separable polynomials in K^{2k} is also the complement of a zero set of a non-zero polynomial in $K[W_1,\dots,W_{2k}]$, namely of the discriminant D of the universal polynomial $\mathsf{H} := X^{2k} - W_1X^{2k-1} + W_2X^{2k-2} - \cdots + W_{2k}$, which is, up to sign, the Sylvester determinant $\mathsf{D} = (-1)^{\binom{n}{2}} \operatorname{Res}(\mathsf{H},\mathsf{H}')$.

For every separable polynomial $H_0 \in K^{2k}$, the fiber algebra of $\mathrm{V}_{(k,k)}$ over H_0 is separable, by Lemma 5.4. Therefore, its trace form is non-degenerate. By Theorem 3.2, it suffices to show that the signature of this trace form does not vanish. By Euler's result, this is true if $E(H_0) \neq 0$. Assume $E(H_0) = 0$. Then, by Lemma 1.2, there is a neighborhood of H_0 in K^{2k} such that the trace form of the fiber algebra of each H in this neighborhood has the same signature as in H_0. Since there are points H in this neighborhood with $E(H) \neq 0$, this common signature is non-zero, namely the number of K-rational points in this specific fiber over H, cf. Theorem 3.2.

We now give the proof of the announced theorem of Euler, which, together with the preceding considerations, also yields a proof of the Fundamental Theorem of Algebra:

6.1 Theorem ([5], Theorème 7, 1749) *Let K denote a real closed field and $k = 2^\gamma$ with $\gamma \in \mathbb{N}^*$. Then there is an (explicitly determinable) polynomial $E \in K[W_1,\dots,W_{2k}]$, $E \neq 0$, such that all $w \in K^{2k}$ with $E(w) \neq 0$ belong to the image of the Vieta mapping $\mathrm{V}_{(k,k)} : K^k \times K^k \to K^{2k}$.*

Proof: We shall give Euler's original direct proof (in modern language) to point out Euler's significant contributions to the proof of the Fundamental Theorem of Algebra. The proof demonstrates his excellent skills in calculation and reveals fundamental ideas that turned out to be important for the development of algebra in general and had an especially profound impact on invariant theory and field theory up to Galois theory.

Euler studies the finite extension

$$\upsilon_{(k,k)} : K[W_1,\dots,W_{2k}] \to K[U_1,\dots,U_k;V_1,\dots,V_k]$$

of polynomial algebras associated to the Vieta mapping $\mathrm{V}_{(k,k)} : K^k \times K^k \to K^{2k}$. As we have already described in Section 5, he interprets the indeterminates U, V and W as the elementary symmetric functions: $U_\kappa = \mathrm{S}_\kappa(X_1,\dots,X_k)$, $V_\lambda = \mathrm{S}_\lambda(X_{k+1},\dots,X_{2k})$ and $W_\mu = \mathrm{S}_\mu(X_1,\dots,X_{2k})$, $1 \leq \kappa,\lambda \leq k$, $1 \leq \mu \leq 2k$, where $X_1,\dots,X_{2k}$ is a new system of indeterminates. According to this interpretation, we denote in the following the indeterminates $W_1,\dots,W_{2k}$ by $S_1,\dots,S_{2k}$ and specific values $w_1,\dots,w_{2k} \in K$ of $W_1,\dots,W_{2k}$ by $s_1,\dots,s_{2k}$. Then $\upsilon_{(k,k)}$ is identified with the canonical embedding $K[S] \subseteq K[U;V]$ and $K[U;V]$ is canonically embedded into $K[X]$. Altogether we have the chain

$$K[S] \subseteq K[U;V] \subseteq K[X]$$

of finite extensions and the associated chain

$$K(S) \subseteq K(U;V) \subseteq K(X)$$

of their quotient fields. The K-algebra $K[X]$ is free of rank $k!k!$ over $K[U;V]$, and $K[U;V]$ is free of rank $n := \binom{2k}{k}$ over $K[S]$, cf. Lemma 5.2. The symmetric group $\mathfrak{S}_{2k}$ operates canonically on $K[X]$ with $K[S]$ as algebra of invariants. On the other hand, $K[U;V]$ is the algebra of invariants of $K[X]$ under the operation of the group $\mathfrak{S}_k \times \mathfrak{S}_k$, which is

canonically embedded in $\mathfrak{S}_{2k}$ (the second factor is identified with the permutation group $\mathfrak{S}(\{k+1,\dots,2k\}) \subseteq \mathfrak{S}_{2k}$).

First, we note that

$$n = \frac{(2k)!}{k!k!} = 2\binom{2k-1}{k-1} = 2m\ ,$$

where the factor $m := \binom{2k-1}{k-1} = \binom{2^{\gamma+1}-1}{2^\gamma-1}$ *is odd*. Incidentally, *all* binomial coefficients $\binom{2^{\gamma+1}-1}{\nu}$, $0 \le \nu \le 2^{\gamma+1}-1$, are odd, since over $\mathbb{Z}/\mathbb{Z}2$

$$(1+t)^{2^{\gamma+1}-1} = \frac{(1+t)^{2^{\gamma+1}}}{1+t} = \frac{1+t^{2^{\gamma+1}}}{1+t} = \sum_{\nu=0}^{2^{\gamma+1}-1} t^\nu\ .$$

As Euler, we use now a resolvent, i. e. a primitive element of the field extension $K(S) \subseteq K(U;V)$, cf. Example 2.1. Such a resolvent is given by

$$\begin{aligned} Z := U_1 - V_1 &= \mathrm{S}_1(X_1,\dots,X_k) - \mathrm{S}_1(X_{k+1},\dots,X_{2k}) \\ &= X_1 + \cdots + X_k - X_{k+1} - \cdots - X_{2k} = 2U_1 - S_1\ . \end{aligned}$$

Indeed, $Z \in K[X]$ has the n conjugates $X_{\mathcal{R}} - X_{\mathcal{R}'}$, $\mathcal{R} \subseteq [1,2k]$, $\#\mathcal{R} = k$ with respect to the symmetric group $\mathfrak{S}_{2k}$. Here, for an arbitrary subset $\mathcal{S} \subseteq [1,2k]$ we denote by $\mathcal{S}'$ its complement $[1,2k] \setminus \mathcal{S}$ and define $X_{\mathcal{S}} := \sum_{i\in\mathcal{S}} X_i$, so that $Z = X_{[1,k]} - X_{[k+1,2k]}$. Note that $\sigma(X_{\mathcal{S}} - X_{\mathcal{S}'}) = X_{\sigma\mathcal{S}} - X_{\sigma\mathcal{S}'} = X_{\sigma\mathcal{S}} - X_{(\sigma\mathcal{S})'}$ for arbitrary $\mathcal{S} \subseteq [1,2k]$, $\sigma \in \mathfrak{S}_{2k}$. Hence,

$$\mathrm{R}(S;T) = \prod_{\#\mathcal{R}=k} (T - (X_{\mathcal{R}} - X_{\mathcal{R}'})) \in K[S][T] \subseteq K(S)[T]$$

is the resolvent polynomial of Z and $K(U;V) = K(S)[Z]$. In particular, the coefficients $U_1,\dots,U_k,V_1,\dots,V_k$ of the factors $X^k - U_1X^{k-1} + \cdots + U_k$, $X^k - V_1X^{k-1} + \cdots + V_k$ of their product $X^{2k} - S_1X^{k-1} + \cdots + S_{2k}$ are polynomials in Z with *rational* functions in $S_1,\dots,S_{2k}$ as coefficients.[9]

The subalgebra $K[S][Z] \subseteq K[U;V]$ is "generically" equal to $K[U;V]$. But because $k \ge 2$, it never coincides with $K[U;V]$. The deviation can be described explicitly: The powers Z^{j-1}, $j = 1,\dots,n$, are linear combinations of a fixed $K[S]$-base $B_1,\dots,B_n$ of $K[U;V]$,

$$Z^{j-1} = \sum_{i=1}^{n} A_{ij}B_i\ , \quad j = 1,\dots,n\ ,$$

and the non-zero transition determinant

$$E := \det(A_{ij})_{1\le i,j\le n} \in K[S]$$

(of degree $\binom{2k-1}{k-1}(\binom{2k}{k} - k^2 - 1) = m(n-k^2-1) \equiv 1(2)$) describes the support of the $K[S]$-module $K[U;V]/K[S][Z]$. In particular, for a point $s = (s_1,\dots,s_{2k}) \in K^{2k}$ the fiber algebra

$$K[U;V]/\mathfrak{m}_s K[U;V] = K[U;V]/(S-s)K[U;V]$$

[9] In order to prove that $\mathrm{R}(S;T)$ is the minimal polynomial of $Z = X_{[1,k]} - X_{[k+1,2k]}$, i.e. that any polynomial $C(S;T) \in K(S)[T]$ with $C(S;Z) = 0$ is a multiple of $\mathrm{R}(S;T)$, it would be enough to observe that $0 = \sigma(C(S;Z)) = C(S;\sigma Z) = C(S;X_{\sigma[1,k]} - X_{\sigma[k+1,2k]})$ for every $\sigma \in \mathfrak{S}_{2k}$. – Euler used U_1 instead of Z as a resolvent and made in addition a Tschirnhaus transformation, which in the end yields (essentially) the same resolvent as Z.

coincides with the fiber algebra

$$K[S][Z]/\mathfrak{m}_s K[S][Z] \cong K[T]/\langle \mathrm{R}(s;T)\rangle$$

if (and only if) $E(s) \neq 0$. Theorem 6.1 is therefore a direct consequence of the following lemma. □

6.2 Lemma *The resolvent polynomial* $\mathrm{R}(s;T)$ *has a zero in* K *for every* $s=(s_1,\ldots,s_{2k})\in K^{2k}$.

Proof: Since

$$\begin{aligned}\mathrm{R}(S;-T) &= \prod_{\#\mathcal{R}=k}(-T-(X_{\mathcal{R}}-X_{\mathcal{R}'})) = \prod_{\#\mathcal{R}=k}(T+(X_{\mathcal{R}}-X_{\mathcal{R}'}))\\ &= \prod_{\#\mathcal{R}=k}(T-(X_{\mathcal{R}'}-X_{\mathcal{R}})) = \mathrm{R}(S;T)\end{aligned}$$

the resolvent polynomial is a polynomial in T^2:

$$\mathrm{R}(S;T) = \widetilde{\mathrm{R}}(S;T^2)\ .$$

(The polynomial $\widetilde{\mathrm{R}}(S;\widetilde{T}) \in K[S][\widetilde{T}]$ is of degree $m=n/2$ in $\widetilde{T}$ and is the resolvent polynomial of $\widetilde{Z} := Z^2 = (U_1-V_1)^2$.) The constant term of $\mathrm{R}(S;T)$ (and $\widetilde{\mathrm{R}}(S;\widetilde{T})$) is of the form $-C^2$ with $C\in K[S]$. Indeed,

$$\mathrm{R}(S;0) = \prod_{\#\mathcal{R}=k}(X_{\mathcal{R}}-X_{\mathcal{R}'}) = \prod_{1\in\mathcal{R}}(X_{\mathcal{R}}-X_{\mathcal{R}'})\cdot\prod_{1\notin\mathcal{R}}(X_{\mathcal{R}}-X_{\mathcal{R}'}) = -\prod_{1\in\mathcal{R}}(X_{\mathcal{R}}-X_{\mathcal{R}'})^2$$

since the number of subsets $\mathcal{R}\subseteq[1,2k]$ with $1\in\mathcal{R}$ $\#\mathcal{R}=k$, is $\binom{2k-1}{k-1} = m \equiv 1(2)$. Furthermore,

$$C := \prod_{1\in\mathcal{R}}(X_{\mathcal{R}}-X_{\mathcal{R}'})$$

is invariant under the operation of $\mathfrak{S}_{2k}$, i.e. $C\in K[S]$.[10] The equality $\sigma C = C$ is obvious for $\sigma\in\mathfrak{S}_{2k}$ with $\sigma 1 = 1$. Hence, it is enough to show that $\tau C = C$ for the transposition $\tau := <1,2>$. For this, let $\mathcal{S}$ and $\mathcal{T}$ denote subsets of $[3,2k]$ of cardinality $k-2$ and $k-1$, respectively, and let $\mathcal{S}^c$, $\mathcal{T}^c$ be the complements $[3,2k]\setminus\mathcal{S}$, $[3,2k]\setminus\mathcal{T}$ of $\mathcal{S}$ and $\mathcal{T}$ in $[3,2k]$, respectively. Then

$$\begin{aligned}\tau C &= \prod_{1\in\mathcal{R}}(X_{\tau\mathcal{R}}-X_{(\tau\mathcal{R})'})\\ &= \prod_{\mathcal{S}}(X_1+X_2+X_{\mathcal{S}}-X_{\mathcal{S}^c})\cdot\prod_{\mathcal{T}}(X_2+X_{\mathcal{T}}-X_1-X_{\mathcal{T}^c})\\ &= \prod_{\mathcal{S}}(X_1+X_2+X_{\mathcal{S}}-X_{\mathcal{S}^c})\cdot\prod_{\mathcal{T}}(X_1+X_{\mathcal{T}}-X_2-X_{\mathcal{T}^c}) = C\end{aligned}$$

because the number $\binom{2k-2}{k-1} = 2\binom{2k-3}{k-2}$ of subsets $\mathcal{T}\subseteq[3,2k]$ with $\#\mathcal{T}=k-1$ is even. It follows that for any $s\in K^{2k}$ the constant term $-C^2(s)$ of the monic polynomial $\mathrm{R}(s;T)\in K[T]$ is ≤ 0. Hence, $\mathrm{R}(s;T)$ has a zero (≥ 0) in K by the Intermediate Value Theorem. This proves the lemma. □

[10] Euler's insufficient argumentation for $C\in K[S]$ is one of the (minor) points of criticism, which Gauss mentions in his doctoral thesis, cf. the introduction.

6.3 Remark Of course, to find a $t \in K$, which satisfies the equation $\mathrm{R}(s;t) = 0$ of degree $n = 2m$, one solves first the equation $\widetilde{\mathrm{R}}(s;\widetilde{t}) = 0$ of degree m. If $\widetilde{t} \geq 0$ is a solution in K of the last equation, then $t = \pm \left(\widetilde{t}\right)^{1/2}$ are solutions of $\mathrm{R}(s;t) = 0$.

6.4 Example We illustrate the proof of Theorem 6.1 for $\gamma = 1$, $k = 2$. In this case

$$U_1 = X_1 + X_2 \,, \quad U_2 = X_1 X_2 \,, \quad V_1 = X_3 + X_4 \,, \quad V_2 = X_3 X_4 \,,$$

and the generic polynomial is given by

$$\prod_{i=1}^{4} (X - X_i) = X^4 - S_1 X^3 + S_2 X^2 - S_3 X + S_4 = (X^2 - U_1 X + U_2)\,(X^2 - V_1 X + V_2)$$

with

$$S_1 = U_1 + V_1 \,, \quad S_2 = U_1 V_1 + U_2 + V_2 \,, \quad S_3 = U_1 V_2 + U_2 V_1 \,, \quad S_4 = U_2 V_2 \,.$$

The chosen resolvent $Z := U_1 - V_1 = 2U_1 - S_1$ has the minimal polynomial

$$\mathrm{R}\,(S;T) = \widetilde{\mathrm{R}}\,(S;T^2) \,,$$

where

$$\begin{aligned}
&\widetilde{\mathrm{R}}\,(S;\widetilde{T}) = \\
&= (\widetilde{T} - (X_1 + X_2 - X_3 - X_4)^2)\,(\widetilde{T} - (X_1 - X_2 + X_3 - X_4)^2)\,(\widetilde{T} - (X_1 - X_2 - X_3 + X_4)^2) \\
&= \widetilde{T}^3 - (3S_1^2 - 2^3 S_2)\widetilde{T}^2 + (3S_1^4 - 2^4 S_1^2 S_2 + 2^4 S_1 S_3 + 2^4 S_2^2 - 2^6 S_4)\widetilde{T} - (S_1^3 - 4S_1 S_2 + 8S_3)^2
\end{aligned}$$

is the resolvent polynomial of the (cubic) resolvent Z^2.

To compute the polynomial $E \in K[S]$ of Theorem 7.1, we choose the $K[S]$-base $1, U_1, U_1^2, U_1^3, U_1^4, U_2$ of $K[U;V]$. (It is easy to see that their residue classes form a K-base of $K[U;V]/\langle S\rangle K[U;V]$.) From the relations

$$S_3 = U_1^3 - S_1 U_1^2 - 2U_1 U_2 + S_2 U_1 + S_1 U_2 \,, \quad S_4 = U_1^2 U_2 - S_1 U_1 U_2 - U_2^2 + S_2 U_2$$

and

$$S_4 U_1 - S_3 U_2 = U_1 U_2^2 - S_1 U_2^2$$

we obtain successively, modulo $\sum_{j=0}^{4} K[S]\,U_1^j$, the congruences

$$U_1 U_2 \equiv \frac{1}{2} S_1 U_2 \,, \quad U_1^2 U_2 \equiv \frac{1}{2} S_1 U_1 U_2 \equiv \frac{1}{4} S_1^2 U_2 \,,$$

$$U_2^2 \equiv U_1^2 U_2 - S_1 U_1 U_2 + S_2 U_2 \equiv \left(-\frac{1}{4} S_1^2 + S_2\right) U_2 \,,$$

$$U_1 U_2^2 \equiv S_1 U_2^2 - S_3 U_2 \equiv \left(-\frac{1}{4} S_1^3 + S_1 S_2 - S_3\right) U_2 \,,$$

$$U_1^3 U_2 \equiv S_1 U_1^2 U_2 + U_1 U_2^2 - S_2 U_1 U_2 \equiv \left(\frac{1}{2} S_1 S_2 - S_3\right) U_2$$

and hence

$$U_1^5 \equiv 2U_1^3 U_2 - S_1 U_1^2 U_2 \equiv \left(-\frac{1}{4} S_1^3 + S_1 S_2 - 2S_3\right) U_2 \,.$$

Therefore, the determinant of the matrix which expresses the elements $1, U_1, U_1^2, U_1^3, U_1^4, U_1^5$ in the $K[S]$-base $1, U_1, U_1^2, U_1^3, U_1^4, U_2$ is given by

$$-\frac{1}{4} S_1^3 + S_1 S_2 - 2S_3 \,.$$

Since $Z = 2U_1 - S_1$, this yields the desired determinant for $1, Z, Z^2, Z^3, Z^4, Z^5$:

$$E = -2^{13}(S_1^3 - 4S_1 S_2 + 8S_3) \,.$$

From this description of E one can derive directly that *every* polynomial $X^4 - s_1X^3 + s_2X^2 - s_3X + s_4$ of degree 4 over a real closed field is the product of two quadratic polynomials. Namely, applying a Tschirnhaus transformation one may assume that $s_1 = 0$. Thus, if $E(s) = -2^{13} \cdot 8s_3 \neq 0$, then Theorem 7.1 can be applied, and if $E(s) = 0$, then $s_3 = 0$ and $X^4 + s_2X^2 + s_4$ is a product of two quadratic polynomials for trivial reasons. Further, we remark that (for $k = 2$) one can conclude a priori that the zero set of E coincides with the zero set of the constant term of the resolvent polynomial $\mathrm{R}(S;T)$.

References

[1] J.-B. le Rond d'Alembert: *Recherches sur le calcul intégral*. In: Histoire de l'Académie Royale des Sciences et Belle Lettres, Année MDCCXLVI, Berlin, 1748, 182-224.

[2] S. Böttger: *Über die Invarianten endlicher Permutationsgruppen und die Galois-Theorie allgemeiner Gleichungen*. Diplomarbeit, Ruhr-Universität Bochum, 2006.

[3] S. Eilenberg, I. Niven: *The "fundamental theorem of algebra" for quaternions*. In: Bulletin of the American Mathematical Society 50, 1944, 246-248.

[4] D. Eisenbud, H. I. Levine: *The topological degree of a finite C^∞-map germ*. In: Lecture Notes in Mathematics 525, 1976, 90-98.

[5] L. Euler: *Recherches sur les racines imaginaires des équations*. In: Mémoires de l'Académie des Sciences de Berlin 5 (1749), 1751, 222-288. Reprinted in: Leonhardi Euleri: *Opera Omnia* 6, First series: Opera Mathematica, Leipzig, 1921, 78-147.

[6] F. G. Frobenius: *Rede auf L. Euler*. Reprint in: F.G. Frobenius: *Gesammelte Abhandlungen*, Vol. III, Springer, Berlin, 1968, 732-735.

[7] C. F. Gauss: *Demonstratio Nova Theorematis Omnem Functionem Algebraicam Rationalem Integram Unius Variabilis in Factores Reales Primi vel Secundi Gradus Resolvi Posse.* Doctoral Thesis, Helmstedt, 1799, 1-30. Reprint in: C.F. Gauss: *Werke*, Vol. 3, Georg Olms, Hildesheim 1973. English Translation by E. Fandreyer: http://www.fitchburgstate.edu/library/archives/manuscripts/documents/Theorem.pdf

[8] N. Jacobson: *Basic Algebra, Vol. 2*. W.H. Freeman & Co., San Francisco, 1980.

[9] D. P. Patil, U. Storch: *Introduction to Algebraic Geometry and Commutative Algebra*. IISc Lecture Notes Series 1, IISc Press and World Scientific, Singapore, 2010.

[10] R. Remmert: *Fundamentalsatz der Algebra*. In: H.-D. Ebbinghaus et al. (Hg.): *Zahlen*. Springer, Berlin, ^{2}1988, 79-99.

[11] G. Scheja, U. Storch: *Über Spurfunktionen bei vollständigen Durchschnitten*. Journal für die Reine und Angewandte Mathematik 278/279, 1975, 174-190.

[12] G. Scheja, U. Storch: *Lehrbuch der Algebra, Teil 2*. Teubner, Stuttgart, 1988.

[13] J.-P. Serre: *Topics in Galois Theory*. Research Notes in Mathematics, A K Peters, Natick MA, ^{2}2007.

[14] A. R. Shastri: *Mapping Degree and a Proof of the Fundamental Theorem of Algebra*. Manuscript IIT Bombay, December 2009, 1-11.

[15] A. Speiser: *Über den Fundamentalsatz der Algebra*. In: Leonhardi Euleri: *Opera Omnia* 29, First series: Opera Mathematica, Lausanne, 1956, VIII-IX.

[16] U. Storch: *Der Satz von Borsuk-Ulam und der Hilbertsche Nullstellensatz - und vice versa*. In: L. Hefendehl-Hebeker, S. Hußmann (Hg.): *Mathematikdidaktik zwischen Fachorientierung und Empirie*. Festschrift für Norbert Knoche, Franzbecker, Hildesheim, 2003, 214-228.

[17] U. Storch, H. Wiebe: *Lehrbuch der Mathematik, Band 4*. Spektrum Akademischer Verlag, Heidelberg, 2011.

Received 17 January 2011; Revised 07 February 2011

Dr Simone Böttger, completed Undergraduate degree in Mathematics ('Vordiplom') at the Ruhr-Universität Bochum in 2001. DAAD student abroad for six month at the Indian Institute of Science in Bangalore. 2006 Master in Mathematics ('Diplom') at the Ruhr-Universität Bochum. Master thesis: 'On the invariants of finite permutation groups and the Galois theory of the general equation'. Advisor: Uwe Storch. 2006 - 2009 Phd position within the cooperation project NAWI-Graz at the Karl-Franzens Universität. Phd student and scholarship holder of the Colloquium 'Combinatorial structures in algebra and topology' at the Universität Osnabrück. Thesis (in progress): 'Monoids with absorbing elements and their associated algebras'. Advisor: Holger Brenner.

U w e S t o r c h studied Mathematics, Physics and Mathematical Logic at the Universität Münster and Heidelberg from 1960 till 1966 and received Ph. D. from Universität Münster in 1966. In 1972 Habilitation at the Ruhr-Universität Bochum. From 1974 till 1981 and from 1981 till 2005 he was a Full Professor at the Universität Osnabrück and at the Ruhr-Universität Bochum, respectively, holding chairs on Algebra and Geometry. Currently he is Professor Emeritus at the Ruhr-Universität Bochum. He has been a Visiting Professor at Tata Institute of Fundamental Research, Mumbai, Indian Institute of Science, Bangalore and several universities in Europe and USA. His research interests are mainly in Algebra, particularly the algebraic aspects of Complex Analytic Geometry, Commutative Algebra and Algebraic Geometry.