1. The key lemma

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **30 (1984)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

L'Enseignement Mathématique, t. 30 (1984), p. 85-94

A LINEAR ALGEBRA PROOF OF CLIFFORD'S THEOREM

by W. J. Gordon

One of the central results in the theory of algebraic curves is the Riemann-Roch theorem. This theorem guarantees that for divisors D of large degree on a curve the dimension of the associated linear system $| D |$ and the degree of the divisor differ by a constant, the genus of the curve. Clifford's theorem complements Riemann-Roch, by giving information about $\dim | D |$ when the degree of D is small.

The standard modern proof of the Riemann-Roch theorem is a cohomological, scheme-theoretic one. However, elementary proofs are often given because of the importance of the result in the classical theory of algebraic curves. In contrast, Clifford's theorem, which complements Riemann-Roch and provides useful information about hyperelliptic curves, is usually given only a scheme-theoretic proof, and so is not widely known.

In this paper, I give an elementary proof of Clifford's theorem. First I prove a key result, Clifford's lemma, which has the flavor of linear algebra although it is actually a result in algebraic geometry. Clifford's lemma and the Riemann-Roch theorem provide an easy proof of the first part of Clifford's theorem; the other two parts follow by linear algebra arguments.

The proof of the third part of the theorem depends only on facts about divisors on hyperelliptic curves. This proof emphasizes the view of a hyperelliptic curve as a double covering of the projective line. In contrast, the usual proof relies on the characterization of hyperelliptic curves in terms of the canonical morphism $C \to \mathbf{P}_{g-1}$.

1. The key lemma

For this section, let K be a field and let A, B, and C be vector spaces over K. Let r, and s, denote the dimensions of the vector spaces A and B.

Definition. The K-bilinear map $\varphi : A \times B \to C$ is *bi-injective* if the induced maps $\varphi(a, \ ) : B \to C$ and $\varphi(\ , b) : A \to C$ are injective whenever

$a \neq 0$ and $b \neq 0$. Equivalently, φ is bi-injective if $\varphi(a, b) = 0$ implies a or b is zero.

The image of the bi-injective map $\varphi: A \times B \to C$ is not in general a vector subspace of C, but this image contains an s-dimensional family, $\mathscr{F} = \{A_b = \varphi(A, b) \mid b \in B\}$, of r-dimensional vector subspaces of C. Since C contains this family $\mathscr{F}$, one would expect that $\dim C$ is at least $r + s$. This is not the case at all! One has

CLIFFORD'S LEMMA. *Let K be algebraically closed, and let $\varphi: A \times B \to C$ be bi-injective. Then*

$$\dim C \geqslant r + s - 1 .$$

Example 1. The lower bound given can occur. For example, let $P_n = \{\text{polynomials in } K[x] \text{ of degree} \leqslant n\}$. Then multiplication of polynomials defines a bi-injective map $\mu: P_r \times P_s \to P_{r+s}$, for which equality holds in Clifford's Lemma.

Example 2 (Schanuel). If K is not algebraically closed the result is false. Namely, let F be an extension field of E, of degree $n > 1$. Then the multiplication map $\mu: F \times F \to F$ is a bi-injective map of E-vector spaces, yet Clifford's Lemma would imply

$$\dim F = n > 2 \dim F - 1 = 2n - 1 .$$

(This example shows that the Lemma is not actually a result of linear algebra.)

Proof of Clifford's Lemma. Assume that $\dim C = t \leqslant r + s - 2$. Let $\{a_1, ..., a_r\}$ be a basis for A, $\{b_1, ..., b_s\}$ one for B, and $\{c_1, ..., c_t\}$ one for C. I will show that there are elements $a \in A$, $b \in B$ both nonzero for which $\varphi(a, b) = 0$. Writing $a = \sum_{ij} \alpha_i a_i$ and $b = \sum \beta_j b_j$, bilinearity shows that

$$\varphi(a, b) = \sum_{ij} \alpha_i \beta_j \varphi_{ij} \quad \text{where} \quad \varphi_{ij} = \varphi(a_i, b_j) = \sum_k \lambda_k^{ij} c_k .$$

Then, $\varphi(a, b) = 0$ if and only if

$$(*) \qquad \sum_{ij} \alpha_i \beta_j \lambda_k^{ij} = 0 \quad \text{for} \quad k = 1, ..., t .$$

Since a and b are nonzero, their coordinate tuples $(\alpha_1, ..., \alpha_r)$ and $(\beta_1, ..., \beta_s)$ can be viewed as points in the projective spaces $\mathbf{P}_{r-1}$ and $\mathbf{P}_{s-1}$. The Segré embedding $\sigma: \mathbf{P}_{r-1} \times \mathbf{P}_{s-1} \to \mathbf{P}_{rs-1}$ given by

$$\sigma((\alpha_1, ..., \alpha_r), (\beta_1, ..., \beta_s)) = (\alpha_1\beta_1, ..., \alpha_1\beta_s, \alpha_2\beta_1, ..., \alpha_2\beta_s, ..., \alpha_r\beta_s)$$

is a projective morphism establishing an isomorphism between $\mathbf{P}_{r-1} \times \mathbf{P}_{s-1}$ and the image $\mathscr{S} = \sigma(\mathbf{P}_{r-1} \times \mathbf{P}_{s-1})$. [4, Ex I.2.14] Once I label the coordinates of $\mathbf{P}_{rs-1}$ as $(z_{11}, ..., z_{1s}, z_{21}, ..., z_{2s}, ..., z_{rs})$, $\mathscr{S}$ can be identified with the algebraic subset of $\mathbf{P}_{rs-1}$ cut out by the polynomials

$$\{z_{ij}\, z_{pq} - z_{iq}z_{pj} \mid 1 \leqslant i, p \leqslant r \text{ and } 1 \leqslant j, q \leqslant s\}\,.$$

$\mathscr{S}$ is an algebraic subvariety of $\mathbf{P}_{rs-1}$, of dimension $r + s - 2$.

In $\mathbf{P}_{rs-1}$ we can also consider the algebraic subvariety $\mathscr{T}$ cut out by the polynomials $\{\sum_{ij} z_{ij}\lambda_k^{ij} \mid 1 \leqslant k \leqslant t\}$. Since $\mathscr{T}$ is cut out by $t \leqslant r + s - 2$ equations and $\dim \mathscr{S} = r + s - 2$, $\mathscr{S}$ and $\mathscr{T}$ have a nonempty intersection, all of whose components have dimension at least $(r+s-2) - t$, which is $\geqslant 0$. [4, p. 48] However, any intersection point of $\mathscr{S}$ and $\mathscr{T}$ corresponds to a pair of points $(\alpha_1, ..., \alpha_r) \in \mathbf{P}_{r-1}, (\beta_1, ..., \beta_s) \in \mathbf{P}_{s-1}$ satisfying (*). The corresponding points $a = \Sigma\, \alpha_i a_i \in A$, $b = \Sigma\, \beta_j b_j \in B$ are nonzero, yet $\varphi(a, b) = 0$. Since this contradicts the bi-injectivity of φ, I have shown that

$$\dim C \geqslant r + s - 1\,. \qquad \square$$

The assumption that K is algebraically closed was only needed to guarantee that $\mathscr{S} \cap \mathscr{T}$, which by dimension theory corresponds locally to a proper ideal, was nonempty. Hilbert's Nullstellensaltz shows that any proper ideal in a polynomial ring over an algebraically closed field cuts out at least one point.

2. A BRIEF RESUME OF DIVISORS ON CURVES

In this section, I will establish notation for divisors, and state the Riemann-Roch theorem. Let C be a nonsingular projective algebraic curve defined over an algebraically closed field K. C is contained in some projective space $\mathbf{P}_N$ over K, and a (closed) *point* of C is any closed point $(p_0, ..., p_N)$ of $\mathbf{P}_N$ at which all the polynomials cutting out C vanish. The *group of divisors on* C is the free abelian group generated by the points of C. Any divisor can be written in the form

$$N = \Sigma\, n_P \cdot P$$

where the n_P are integers, almost all zero. The *degree* of N is the integer $\deg N = \Sigma\, n_P$. The divisor N is *effective* if all the n_P are $\geqslant 0$; this is written as $N \succ 0$. I write $D \succ E$ to mean $D - E \succ 0$.