Structure of Factor Algebras and Clifford Algebra

Garret Sobczyk[1]
Universidad de las Americas
Departamento de Fisico-Matematicas
Apartado Postal #100, Santa Catarina Mártir
72820 Puebla, Pue., México
sobczyk@udlapvms.pue.udlap.mx

Abstract

We construct a number system which is isomorphic to the factor ring of an arbitrary polynomial. If this polynomial is the minimal polynomial of a given linear operator, then its generalized spectral decomposition is immediately determined. The same methods apply to a linear operator over a finite field. Clifford algebra arises when we introduce a *grading* onto the algebra of endomorphisms.

1 Introduction.

The primary concern of this paper is the generalized spectral decomposition or *eigenprojector form* of a linear operator over any field which is a splitting field of its minimal polynomial. In 1847, Augustin Cauchy observed that $\mathbb{C}$ is isomorphic to the factor ring $\mathbb{R}[\lambda]/<\lambda^2+1>$. In section 2, we construct a number system which is isomorphic to the factor ring $\mathbb{C}[\lambda]/<\psi>$ for an arbitrary polynomial ψ. If ψ is the minimal polynomial of a given linear operator, then its eigenprojector form is immediately determined. A novel proof is given based on Cramer's rule applied to a set of consistent operator equations, section 3. The eigenprojector form can be used to derive the classical Jordan form, discovered for positive integer matrices modulo p by C. Jordan in 1870, [1], and extended to any field by Dickson in 1902, [2]. The same methods apply to a linear operator over a finite field, providing it is the splitting field of the minimal polynomial.

[1]This work has been supported in part by a Conacyt grant # 3803-E, and by the Universidad de Las Americas for which I am grateful.

Clifford algebra arises when we introduce a *grading* onto the algebra of endomorphisms. This is done most naturally in the case of $End(\mathbb{C}^{2^n})$ by constructing a simple isomorphism to the corresponding Clifford algebra. We study the consequences of this isomorphism for hermitian operators, and derive a new polar form for Clifford numbers, section 4.

2 The commutative algebra $\mathbb{C}\{m_1, \ldots, m_r\}$.

Let $\{m_1, \ldots, m_r\}$ be a set of r nondecreasing positive integers with only the first h of them $\equiv 1$.

Definition 1 *The set of elements*

$$\{p_j, q_k^t|, 1 \le j \le r,\ \ h+1 \le k \le r,\ \text{ and } 1 \le t < m_k\},$$

define an associative and commutative $(m_1 + \ldots + m_r)$*-dimensional* $\mathbb{C}$*-algebra*

$$\mathbb{C}\{m_1, \ldots, m_r\} \equiv \ span\{p_j, q_k^t\},$$

where the operations of addition and multiplication of the basis elements are determined by

$$\{p_1 + \ldots + p_r = 1,\ p_i p_j = \delta_{ij} p_i,\ q_k^{m_k - 1} \ne 0 \text{ but } q_k^{m_k} = 0,\ q_k p_k = q_k\}.$$

The elements p_j make up a *partition of unity* and are *mutually annihilating idempotents*. The elements q_j are *nilpotents* with the respective *indexes* m_j. The nilpotents q_j are *projectively* related to the corresponding idempotents p_j. We adopt the convention that $q_j \equiv 0$, for $j = 1, \ldots, h$. The algebra $\mathbb{C}\{m_1, \ldots, m_r\}$ is further discussed in [3, p.33], and shown to be isomorphic to the corresponding factor ring $\mathbb{C}[\lambda]/ < \psi >$ where

$$\psi \equiv \psi(\lambda) = (\lambda - \lambda_1)^{m_1} \ldots (\lambda - \lambda_r)^{m_r}, \tag{1}$$

for the distinct complex roots $\lambda_j \in \mathbb{C}$.

3 The eigenprojector form.

We can now establish the *eigenprojector form* of a linear operator:

Theorem 1 *If the minimal polynomial $\psi(\lambda)$ of $a \in End(\mathbb{C}^n)$ is given as in (1), then a can be written in the canonical form*

$$a = \sum_{j=1}^{r} (\lambda_j + q_j) p_j,$$

where p_i and q_i are idempotents and nilpotents which generate a subalgebra of $End(\mathbb{C}^n)$ which is isomorphic to the associative $\mathbb{C}$-algebra $\mathbb{C}\{m_1, \ldots, m_r\}$. Each p_j, q_j is uniquely expressed in terms of a polynomial in a of degree less than $s = m_1 + \ldots + m_r$.

Proof. We *construct* a $\mathbb{C}\{m_1, \ldots, m_r\}$ algebra of idempotents and nilpotents for a by using the rules specified in Definition 1, and showing consistency. We begin by writing

$$a^0 \equiv 1 = \quad p_1 \quad + \quad p_2 \quad + \quad \ldots \quad + \quad p_r,$$

$$a = (\lambda_1 + q_1)p_1 \; + \; (\lambda_2 + q_2)p_2 \; + \; \ldots + \; (\lambda_r + q_r)p_r.$$

Using Definition 1, we then take successive powers of a to complete $s = m_1 + m_2 + \ldots + m_r$ powers of a, getting

$$a^2 = (\lambda_1 + q_1)^2 p_1 + (\lambda_2 + q_2)^2 p_2 + \ldots + (\lambda_r + p_r)^r p_r$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$a^{s-1} = (\lambda_1 + q_1)^{s-1} p_1 + (\lambda_2 + q_2)^{s-1} p_2 + \ldots + (\lambda_r + q_r)^{s-1} p_r$$

The powers of each $(\lambda_j + q_j)^k$ can be easily computed, getting

$$(\lambda_j + q_j)^k = \lambda_j^k + \binom{k}{1} \lambda_j^{k-1} q_j + \ldots + \binom{k}{m_j - 1} \lambda_j^{k-m_j+1} q_j^{m_j-1},$$

where $\binom{k}{j}$ are the usual binomial coefficients for $j \leq k$, and $\binom{k}{j} \equiv 0$ for $j > k$. When each of these expansions is substituted back into the successive powers of a computed above, we are led to a system of operator equations which are linear in

$$\{p_1, q_1, q_1^2, \ldots q_1^{m_1-1}; \ldots; p_r, q_r, q_r^2, \ldots, q_r^{m_r-1}\}.$$

Just as for the corresponding system of linear equations, the above system of *operator* equations will be *consistent* and have a *unique* solution if the determinant $det(C)$ of the coefficient matrix C of the unknown operators is nonvanishing. But C is just the confluent Vandermonde matrix given by

$$\begin{pmatrix} 1 & 0 & \ldots & 1 & \ldots & 1 & 0 & \ldots \\ \lambda_1 & 1 & \ldots & \lambda_j & \ldots & \lambda_r & 1 & \ldots \\ \vdots & & & & \vdots & & & \\ \lambda_1^{s-1} & (s-1)\lambda_1^{s-2} & \ldots & \lambda_j^{s-1} & \ldots & \lambda_r^{s-1} & (s-1)\lambda_r^{s-2} & \ldots \end{pmatrix}$$

where the horizontal entries starting with λ_j^k are successively determined by the formula

$$\frac{1}{h!}\frac{d^h}{d\lambda^h}\lambda^k|_{\lambda=\lambda_j}$$

for $h = 0, 1, \ldots, m_j - 1$, see [4, p. 60]. The *determinant* of the confluent Vandermonde matrix C is

$$det(C) = \prod_{i<j}(\lambda_j - \lambda_i)^{m_i m_j} \neq 0,$$

since the roots λ_i for $i = 1, \ldots, r$ are all distinct. Since this determinant is non-vanishing, the system of operator equations is consistent. It can therefore be uniquely solved, by using Cramer's rule, for the operator unknowns of idempotents and nilpotents in $End(\mathbb{C}^n)$ in terms of polynomials in a of degree $\leq s - 1$.

Q.E.D.

The above theorem was proved in its present form in [5]. It is repeated here for completeness and because it appears to be computationally more efficient than the classical approach based upon the partial fraction decomposition of $1/\psi(\lambda)$.[2] We also want to make the observation that the proof remains valid when $\mathbb{C}$ is replaced by a possibly *finite* splitting field of the minimal polynomial ψ; this occurs when studying algebras of endomorphisms over a finite field. Of course, in the case of a finite field, the coefficients of the confluent Vandermonde matrix must be appropriately modified.

The eigenprojector form of the operator a, as given in theorem 1, makes it easy to evaluate any analytic function defined on the spectrum of the operator; we find

$$f(a) = f[\sum_j (\lambda_j + q_j)p_j] = \sum_j f(\lambda_j + q_j)p_j, \tag{2}$$

where

$$f(\lambda_j + q_j) = f(\lambda_j) + f'(\lambda_j)q_j + \ldots + \frac{1}{(m_j - 1)!} f^{(m_j-1)}(\lambda_j) q_j^{m_j-1},$$

ref. [3, p.38]. The reader may compare our method with the more complicated method of jets described in [6, p.160], or the classical methods of [7, p. 104].

The classical Jordan normal form of a linear operator can be constructed from the eigenprojector form by extracting Jordan chains from the nilpotent elements q_i, but we will not do this here. We content ourself with the remark that if it is only desired to evaluate a function of an operator, then the eigenprojector form is sufficient for the task as we have just seen in formula (2).

4 Clifford Algebra

There is a deep relationship between Clifford algebras and algebras of endomorphisms on a finite dimensional vector space. In particular, there is an algebra isomorphism between the real Clifford algebra $Cl_{k,k+1}$ and the complex matrix algebra $M_{\mathbb{C}}(2^k)$, where $Cl_{p,q}$ denotes the real Clifford algebra of a quadratic form with the signature (p,q).

[2] In another paper the author shows that the determinant of the *modified* confluent Vandermonde matrices that arise in the application of Cramer's rule, can be directly calculated from the well known formula for the Vandermonde determinant.

The algebra isomorphism between the real Clifford algebra $Cl_{k,k+1}$ of a quadratic form with the signature $(k, k+1)$ and the complex matrix algebra $M_C(2^k)$ can be expressed by

$$\begin{pmatrix} u_{+\ldots+} & e_1 u_{-+\ldots+} & \ldots & e_\lambda^{-1} u_{sgns} & \ldots & e_{1\ldots k}^{-1} u_{-\ldots-} \\ e_1 u_{+\ldots+} & u_{-+\ldots+} & \ldots & e_1 e_\lambda^{-1} u_{sgns} & \ldots & e_1 e_{1\ldots k}^{-1} u_{-\ldots-} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ e_\lambda u_{+\ldots+} & e_\lambda e_1 u_{-+\ldots+} & \ldots & u_{sgns} & \ldots & e_\lambda e_{1\ldots k}^{-1} u_{-\ldots-} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ e_{1\ldots k} u_{+\ldots+} & e_{1\ldots k} e_1 u_{-+\ldots+} & \ldots & e_{1\ldots k} e_\lambda^{-1} u_{sgns} & \ldots & u_{-\ldots-} \end{pmatrix} \qquad (3)$$

The Clifford numbers in the matrix make up a 2^{2k}-dimensional basis of the Clifford algebra $Cl_{k,k+1}$ over elements in the center of the form $x + yj$, where $x, y \in \mathbb{R}$ and j is a unit $(2k+1)$-vector with $j^2 = -1$; the position of each element corresponds to a matrix with a 1 in the same position and zeros everywhere else. The elements u_{sgn} are 2^k mutually annihiliating primitive idempotents, and the elements $e_1, \ldots, e_k$ are orthonormal basis vectors with square $+1$ generating $Cl_{k,0}$. The e_λ represents a product of the generating e_i's corresponding to the *ordered* index set λ, for example for $\lambda = \{1, 2, k\}$, $e_\lambda \equiv e_1 e_2 e_k$. The elements e_λ *conjugate commute* with the idempotent elements u_{sgn}, for example $e_{12k}\ u_{+++\ldots++} = u_{--+\ldots+-}\ e_{12k}$. A more detailed discussion of this isomorphism can be found in [8].

Clifford algebra can be used in the study of a linear operator on the complex space $\mathbb{C}^n$ both *extrinsically* and *intrinsically*. In the extrinsic approach, the space $\mathbb{C}^n$ upon which the operator operates is made into the Clifford algebra $Cl(\mathbb{C}^n)$ over the complex numbers, [9]. In the intrinsic approach, the Clifford algebra structure of the algebra of endomorphisms itself is exploited, [5].

We now show how the theory of hermitian operators on a unitary space U can be carried over to corresponding properties of Clifford numbers. We restrict ourselves to the Clifford algebras $Cl_{k,k+1}$, although our methods apply more generally to any Clifford algebra equipped with the hermitian structure given below.

Let $\{e_1, \ldots, e_k, f_1, \ldots, f_{k+1}\}$ be an orthonormal basis of *anticommuting* vectors generating the Clifford algebra $Cl_{k,k+1}$, the first k satisfying $e_i^2 = 1$, and $k+1$ satisfying $f_i^2 = -1$. By the positive definite *hermitian conjugation* on $Cl_{k,k+1}$, we mean the antiautomorphism defined on the generators by

$$e_i^* = e_i, \quad \text{and} \quad f_j^* = -f_j$$

for $i = 1, \ldots, k$ and $j = 1, \ldots, k+1$, and extended to the whole algebra. Our hermitian conjugation in $Cl_{k,k+1}$ is defined to correspond exactly to hermitian conjugation in the isomorphic matrix algebra (3).[3] Note that the *unit pseudoscalar* element $j \equiv e_1 f_1 e_2 f_2 \ldots e_k f_k f_{k+1}$ (sometimes denoted by J), in the center Z of the real Clifford algebra $Cl_{k,k+1}$, is identified with the imaginary number $i^2 = -1$.

For $a, b \in Cl_{k,k+1}$, we have the familiar properties:

H1. $(a+b)^* = a^* + b^*$,

H2. $(ab)^* = b^* a^*$,

H3. $(a^*)^* = a$,

H4. $< aa^* >_0 \geq 0$, and $= 0$ only if $a = 0$ *(positive definite).*

The notation $< x >_0$ used in H4, means 'take the *real* or 0-vector part' of the Clifford number $x \in Cl_{k,k+1}$. For example, if $x = x_0 1 + \sum_{0 \notin \lambda} x_\lambda e_\lambda \in Cl_{k,k+1}$ where $x_0, x_\lambda \in I\!R$, then $< x >_0 = x_0$

The trivial proofs of the following property and theorems demonstrates the simple arguments that are made possible when a grading and an hermitian conjugation are introduced on a linear space of endomorphisms.

Property 1 *If $p \in Cl_{k,k+1}$ is a hermitian projection, i.e., $p^* = p = p^2$, then $< p >_0 \geq 0$.*

Proof. Since $p^2 = pp^*$, it immediately follows by $H4$ that $< p >_0 = < p^2 >_0 = < pp^* >_0 \geq 0$.

Q.E.D.

By theorem 1, any element $a \in Cl_{k,k+1}$ has the eigenprojector form $a = \sum (\lambda_i + q_i) p_i$. We can use the graded structure of the Clifford algebra to show that if a is hermitian, then each $q_i \equiv 0$. We have

[3] Our terminology is somewhat at variance with that found in the literature. For a discussion of the issues involved, see [10].

Theorem 2 *If a is hermitian then a has the simple structure $a = \sum \lambda_i p_i$.*

Proof. Since $a = a^*$ each q_i is expressible in terms of a *real* polynomial in a, from which it follows that $q_i = q_i^*$. Suppose that some $q = q_i$ has an index of nilpotency $m > 1$. It then trivially follows by $H4$ that

$$0 =< q^{2(m-1)} >_0 =< q^{m-1}(q^{m-1})^* >_0$$

forcing $q^{m-1} = 0$ and contradicting that $m > 1$. It follows that $m = 1$ for each q_i so that $q_i = q_i^1 = 0$ and a has simple structure.

Q.E.D.

Corollary 1 *If $a \in Cl_{k,k+1}$, then $aa^* = \sum_j \lambda_j p_j$ where $\lambda_j \geq 0$ and the p_j's are mutually annihiliating hermitian projections.*

Proof. Since aa^* is hermitian, we need only show that the λ_j's are non-negative. This follows using the positive definiteness H4, and property 1 to get

$$< (p_j a)(p_j a)^* >_0 =< p_j a a^* p_j >_0 =< \lambda_j p_j >_0 = \lambda_j < p_j >_0 \geq 0,$$

which implies that $\lambda_j \geq 0$.

Q.E.D.

We can now prove the following *polar form* for $a \in Cl_{k,k+1}$.

Theorem 3 *Every* $a \in Cl_{k,k+1}$ *can be repesented in the polar form* $a = h_1 u = h_1 \exp(jh_2)$*, where* h_1 *and* $h_2 = -j\log(u)$ *are hermitian.*

Proof. The proof follows along the same lines as the corresponding decomposition of a linear operator given in [7, p. 276]. We will proceed immediately to the more interesting singular case.

Note that $aa^* = h_1^2$, where $h_1 = \sum \sqrt{\lambda_j} p_j$ for $\lambda_j \geq 0$ and mutually orthogonal hermitian projections p_j, by corollary 1 and (2). We now calculate

$$(a^* p_j a)^2 = a^* p_j a a^* p_j a = \lambda_j a^* p_j a = \lambda_j^2 p_j'.$$

If one $\lambda_i = 0$ for some i, then set $p_i' = 1 - \sum_{j \neq i} p_j'$. It follows that p_j and $1 - p_j$, and p_j' and $1 - p_j'$ are orthogonal hermitian projections with the same ranks that have complete sets of mutually orthonormal eigenvectors, respectively. The unitary transformation u is constructed to map the corresponding orthornormal sets of eigenvectors of p_j' with eigenvalues 1 into the the corresponding orthonormal sets of eigenvectors of p_j with eigenvalues 1 for each j. Thus, if $b_1, b_2, \ldots, b_t \in U$ is an orthonormal set of the projection p_j with eigenvalues 1, that is $p_j b_i = b_i$ for $i = 1, \ldots, t$, and $b_1', b_2', \ldots, b_t'$ is the orthonormal set of the corresponding projection p_j' with eigenvalues 1, then $ub_j' \equiv b_j$.

It follows that the hermitian projections p_j' and p_j are related by $up_j' = p_j u$, where u is a *unitary* element. By using (2), we can write $u = \exp(jh_2)$ where $h_2 \equiv -j\log(u)$ is hermitian. It is easy to check that $a = h_1 u$ is the desired polar form since

$$ap_j' = h_1 u p_j' = h_1 p_j u = \sqrt{\lambda_j} p_j u$$

for each j as is required.

Q.E.D.

ACKNOWLEDGMENT

The author would like to take this opportunity to thank the organizers of the Fourth Conference of the International Linear Algebra Society, held at Erasmus University, 15-19 August 1994, for an excellent conference. The author also wishes to thank the referee for his comments leading to improvements in the manuscript.

References

[1] C. Jordan, *Traité de Substitutions*, (Paris, 1870), p. 114.

[2] Dickson, Am J. Math, **24** (1902), 101-8.

[3] G. E. Sobczyk 1993, Jordan Form in Clifford Algebras, *Clifford Algebras and their Applications in Mathematical Physics*, Proceedings of the Third International Clifford Algebras Workshop, Edited by Fred Brackx, Richard Delanghe, and Herman Serras, Kluwer, Dordrecht, 1993.

[4] H.W. Turnbull and A.C. Aitken, An Introduction to the Theory of Canonical Matrices, Dover Publications, Inc., 1969.

[5] G. Sobczyk, "Clifford Algebra Techniques in Linear Algebra", in CLIFFORD ALGEBRAS AND SPINOR STRUCTURES, editors: Pertti Lounesto and Rafal Ablamowicz, A Volume dedicated to the memory of Albert Crumeyrolle, Kluwer, (To appear).

[6] G.E. Shilov, Linear Algebra, Dover Pub., Inc., New York 1977.

[7] F.R. Gantmacher, Matrix Theory, Vol. 1, Chelsea Publishing Company, New York, 1960.

[8] G. Sobczyk, Unipotents, Idempotents, and a Spinor Basis for Matrices, *Advances in Applied Clifford Algebras* Vol. 2, No. 1 (1992), 53-62.

[9] D. Hestenes, G. Sobczyk, Clifford Algebra to Geometric Calculus: A Unified Language for Mathematics and Physics, Kluwer, Dordrecht, 1984.

[10] P. Lounesto, Scalar Product of Spinors and an Extension of Brauer-Wall Groups, *Foundations of Physics*, **11** (1981), 721-740.