The Missing Spectral Basis in Algebra and Number Theory

Garret Sobczyk

For out of olde feldes, as men seith,
Cometh al this newe corne fro yeere to yere;
And out of olde bokes, in good feith,
Cometh al this new science that men lere.
–Chaucer

1. BEGINNINGS In Euclid's *Elements*, Book VII we find

> Proposition 2: Given two numbers not prime to one another, to find their greatest common measure.

Then follows what mathematicians refer to as the Euclidean algorithm [**4**, p. 298]. We need the following consequence of this venerable Proposition. Given r positive integers $h_1, h_2, \ldots, h_r \in \mathbb{N}$ whose greatest common divisor is $1 \in \mathbb{N}$, there exist integers $b_1, b_2, \ldots, b_r \in Z$ with the property that

$$b_1h_1 + b_2h_2 + \cdots + b_rh_r = 1. \tag{1}$$

The justified fame of the Euclidean algorithm derives from the fact that it has a much larger realm of applicability than just the integers. In particular, let $\mathbb{K}$ be any field and let $\mathbb{K}[x]$ be the corresponding integral domain of polynomials over $\mathbb{K}$. Given r polynomials $h_1(x), h_2(x), \ldots, h_r(x) \in \mathbb{K}[x]$ whose greatest common divisor is $1 \in \mathbb{K}$ (no common zeros in $\mathbb{K}$), there exist polynomials $b_1(x), b_2(x), \ldots, b_r(x) \in \mathbb{K}[x]$ with the property that

$$b_1(x)h_1(x) + b_2(x)h_2(x) + \cdots + b_r(x)h_r(x) = 1. \tag{2}$$

The identities (1) and (2), and the striking analogy between them, provide the grist for this article.

2. MODULAR NUMBERS Let $Z_h = \{0, 1, 2, \ldots, h-1\}$ be the *modular number system* modulo h, where $h \in \mathbb{N}$. Of course, the numbers $b \in Z_h$ represent equivalence classes modulo h and addition, multiplication, and equality in Z_h are defined modulo h. Thus, when we write $b + c = d$ and $bc = d$ in Z_h, we mean that $b + c \equiv d \ mod(h)$ and $bc \equiv d \ mod(h)$. The modular number system Z_h is isomorphic to the factor ring $Z/< h >$ for the principal ideal $< h >$ [**2**, p. 248]. By unique factorization, we can write $h = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ where each p_i is a distinct prime factor of h, and we can order the factors $p_i^{m_i}$ so that their multiplicities satisfy $1 \leq m_1 \leq m_2 \leq \cdots \leq m_r$.

For a given $h \in \mathbb{N}$, define $h_i := h/p_i^{m_i}$ for $i = 1, \ldots, r$. Since the h_i have no common factor other than 1, invoking (1) gives

$$b_1h_1 + b_2h_2 + \cdots + b_rh_r = 1. \tag{3}$$

Whereas this equation holds in Z, it is just as valid when interpreted as an identity in Z_h. Defining the numbers $s_i := b_ih_i \in Z_h$, we say that $sb(Z_h) := \{s_1, s_2, \ldots, s_r\}$ is the

spectral basis of Z_h. Noting that $h_i h_j = 0$ in Z_h for $i \neq j$, the following properties of the spectral basis follow immediately from (3) and the definition of s_i:

$$s_1 + s_2 + \cdots + s_r = 1 \quad \text{in} \quad Z_h \tag{4}$$

and

$$s_i^2 = s_i \quad \text{and} \quad s_i s_j = 0 \quad \text{in} \quad Z_h \tag{5}$$

for $i, j = 1, 2, \ldots, r$, and $i \neq j$. We say that the $s_i \in Z_h$ are *mutually annihiliating primitive idempotents* that *partition unity*.

Now suppose that $x \in Z_h$. Multiplying both sides of (4) by x gives

$$x = xs_1 + xs_2 + \cdots + xs_r = \sum_{i=1}^{r} x_i s_i \quad \text{in} \quad Z_h, \tag{6}$$

where $x_i \equiv x \; mod(p_i^{m_i})$ for $i = 1, 2, \cdots, r$. The s_i act as *projections* onto the modular numbers $Z_{p_i^{m_i}}$, since $s_i = b_i h_i$ and $p_i^{m_i} s_i = 0$ in Z_h. Identity (6) is the famous *Chinese Remainder Theorem*, dating back to the 4th Century A.D.

The modular number systems Z_{p^m}, modulo a power of a prime, play a particularly important role in number theory because all modular problems reduce to problems involving the powers of a prime. In dealing with such problems, it is best to represent numbers $c \in Z_{p^m}$ in terms of the p-adic number basis

$$c = (c_{m-1}\, c_{m-2}\, \ldots\, c_1\, c_0)_p := \sum_{i=0}^{m-1} c_i p^i, \tag{7}$$

where each digit $c_i \in Z_p$.

Using p-adic notation, it is easy to understand that a number $b \in Z_{p^m}$ is divisible by p^k if and only if $b = (b_{m-1} \ldots b_k 0 \ldots 0)_p$. Also, b is not divisible by p^{k+1} if $b_k \neq 0$. The *Euler phi function* or *totient function* $\phi(c)$, for $c \in \mathbb{N}$, is the number of positive integers b, $1 \leq b < c$, such that $\gcd(b, c) = 1$. It follows that if $p \in \mathbb{N}$ is a prime, then $\phi(p^m) = (p-1)p^{m-1}$.

A very basic result of number theory is *Fermat's Theorem:* $b^{\phi(p)} \equiv 1 \; mod(p)$ where p is any prime number and $\gcd(p, b) = 1$. Fermat's theorem is an immediate consequence of the fact that the non-zero elements of the finite field Z_p under multiplication form a group of order $\phi(p) = p - 1$, and the Theorem of Lagrange, which tells us that the order of each element of a group must divide the order of the group.

We can now directly solve for the idempotents s_i. Multiplying each side of (4) by h_i and using (5) gives

$$h_i s_i = h_i \quad \text{in} \quad Z_h,$$

which is readily solved for s_i in Z_h, giving $s_i = (h_i^{-1} \; mod \; p_i^{m_i}) h_i$ for each $i = 1, 2, \ldots, r$. Sometimes, it is useful to define the *nilpotents* $q_i := p_i s_i$ in Z_h, for $i = 1, 2, \ldots, r$. The nilpotent q_i has the *index of nilpotency* m_i, i.e., $q_i^{m_i - 1} \neq 0$ but $q_i^{m_i} = 0$ in Z_h. By the *generalized spectral basis* of Z_h we mean the set

$$gsb(Z_h) := \{s_1, q_1, \ldots, q_1^{m_1 - 1}, s_2, q_2, \ldots, q_2^{m_2 - 1}, \ldots, s_r, q_r, \ldots, q_r^{m_r - 1}\} \tag{8}$$

For example, consider $h = 360 = 5 \cdot 3^2 \cdot 2^3$, for which $h_1 = 3^2 \cdot 2^3$, $h_2 = 5 \cdot 2^3$, and $h_3 = 5 \cdot 3^2$. The spectral basis for Z_{360} consists of 3 primitive idempotents satisfying (4) and (5). To find s_1, multiply $s_1 + s_2 + s_3 = 1$ by $h_1 = 3^2 \cdot 2^3 = 72$, and use the congruences following (6) to get

$$72s_1 = 2s_1 = 72 \quad \text{in} \quad Z_{360},$$

or $16s_1 = s_1 = 8 \cdot 72 = 216$. For s_2, we have

$$5 \cdot 2^3 s_2 = 40 \quad \text{in} \quad Z_{360},$$

or $4s_2 = 40$, so that $s_2 = -8s_2 = -80 = 280$. Finally, $s_3 = 1 - s_1 - s_2 = 225$ in Z_{360}. The spectral basis for Z_{360} is thus

$$\{s_1 = 216, s_2 = 280, s_3 = 225\}.$$

An arbitrary $c \in Z_{360}$ can now be written as

$$c = cs_1 + cs_2 + cs_3 = (c_1)_5 s_1 + (c_2 c_3)_3 s_2 + (c_4 c_5 c_6)_2 s_3,$$

where $c_1 \in Z_5$, $c_2, c_3 \in Z_3$, and $c_4, c_5, c_6 \in Z_2$. The generalized spectral basis of Z_{360} is

$$gsb(Z_{360}) = \{s_1, s_2, q_2, s_3, q_3, q_3^2\} = \{216, 280, 120, 225, 90, 180\}.$$

The multiplication table for the generalized spectral basis of Z_{360} is given in Table 1.

TABLE 1. Multiplication table for $gsb(Z_{360})$.

$\cdot$	s_1	s_2	q_2	s_3	q_3	q_3^2
s_1	s_1	0	0	0	0	0
s_2	0	s_2	q_2	0	0	0
q_2	0	q_2	0	0	0	0
s_3	0	0	0	s_3	q_3	q_3^2
q_3	0	0	0	q_3	q_3^2	0
q_3^2	0	0	0	q_3^2	0	0

Since a number

$$c = \sum_{i=1}^{r} (c_{i(m_i-1)} \cdots c_{i0})_{p_i} s_i \in Z_h$$

is relatively prime to h if and only if $c_{i0} \neq 0 \; mod(p_i)$ for $i = 1, \ldots, r$, it follows that the Euler totient is given by

$$\phi(h) = \prod_{i=1}^{r} (p_i - 1) p_i^{m_i - 1}$$

for the composite number $h = \prod_{i=1}^{r} p_i^{m_i}$. Since the product of any two elements $x, y \in Z_h$ that are relatively prime to h is also relatively prime to h, it follows that

all the elements in Z_h that are relatively prime to h form a multiplicative group of order $\phi(h)$, called the *U-group* $U(h)$ [**2**, p. 154]. Once again, appealing to the Theorem of Lagrange for groups, we have Euler's generalization of Fermat's Theorem that $b^{\phi(h)} \equiv 1 \; mod(h)$ for each $b \in Z_h$ such that $\gcd(b, h) = 1$ [**7**, p. 33].

Employing the spectral basis, we also have an easy formula for finding the inverse of $b \in Z_h$. We have

$$b^{-1} = \sum_{i=1}^{r} (b_{i(m_i-1)} \cdots b_{i0})_{p_i}^{-1} s_i,$$

so the problem of finding $b^{-1} \in Z_h$ is reduced to the problem of finding the inverse in each of the prime power modular number systems $Z_{p_i^{m_i}}$.

3. MODULAR POLYNOMIALS Now that we understand the modular numbers Z_h, we can give a completely analogous treatment of the modular polynomial ring $\mathbb{K}[x]_h := \mathbb{K}[x]/{<}h(x){>}$ of the polynomial $h \equiv h(x)$ over an arbitrary field $\mathbb{K}$. Recall that addition and multiplication of polynomials in $\mathbb{K}[x]_h$ is done $mod(h(x))$, using the Euclidean algorithm for polynomials. Thus, for $f(x), \; g(x) \in \mathbb{K}[x]_h$, $f(x) \cdot g(x) \equiv r(x) \; mod(h(x))$ if

$$f(x) \cdot g(x) = q(x)h(x) + r(x),$$

where $r(x) = 0$ or $deg(r(x)) < deg(h(x))$. In particular, we are thinking about the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the Galois finite number fields of order p^n for prime numbers $p \in \mathbb{N}$, denoted by $\mathcal{G}(p^n)$.

Let $h(x) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$, where each $p_i^{m_i} := (x - x_i)^{m_i}$ is a *prime factor* for distinct $x_i \in \mathbb{K}$. Also, we order the factors of the $m := \sum_{i=1}^{r} m_i$ degree polynomial $h(x)$ so that the multiplicities of the roots x_i satisfy the inequalities $1 \leq m_1 \leq m_2 \leq \cdots \leq m_r$. Defining the polynomials $h_i(x) := h(x)/p_i^{m_i}(x)$, we see that the greatest common divisor of the $h_i(x)$ is $1 \in \mathbb{K}[x]$, and therefore we can invoke (2) to conclude that there exists polynomials $b_i(x) \in \mathbb{K}[x]$ that satisfy

$$b_1(x)h_1(x) + b_2(x)h_2(x) + \cdots + b_r(x)h_r(x) = 1. \tag{9}$$

Whereas (9) holds in $\mathbb{K}[x]$, it remains equally valid when interpreted as an identity in the modular polynomial ring $\mathbb{K}[x]_{h(x)}$. Defining the polynomials $s_i := s_i(x) = b_i(x)h_i(x) \in \mathbb{K}[x]_h$, we say that that $sb(\mathbb{K}[x]_h) := \{s_1, s_2, \ldots, s_r\}$ is the *spectral basis* of the factor ring of polynomials $\mathbb{K}[x]_h$ over the field $\mathbb{K}$. The spectral basis of $\mathbb{K}[x]_h$ satisfies exactly the same algebraic rules as the spectral basis of modular numbers,

$$s_1(x) + s_2(x) + \cdots + s_r(x) = 1 \quad \text{in} \quad \mathbb{K}[x]_h \tag{10}$$

and

$$s_i^2(x) = s_i(x) \quad \text{and} \quad s_i(x)s_j(x) = 0 \quad \text{in} \quad \mathbb{K}[x]_h, \tag{11}$$

for $i, j = 1, 2, \ldots, r$ and $i \neq j$; this follows easily from (9) and the definition of $s_i(x)$. We say that the $s_i(x) \in \mathbb{K}[x]_h$ are *mutually annihiliating primitive idempotents* that *partition unity*.

Every polynomial $f(x) \in \mathbb{K}[x]_h$ has the form $f(x) = b_1 + b_2x + \cdots + b_{m-1}x^{m-1}$ for $b_i \in \mathbb{K}$. For this reason, we sometimes refer to the the elements of $\mathbb{K}[x]_h$ as *polynomial numbers*. The modular polynomials $\mathbb{K}[x]_h$, under addition, have the structure of

an m-dimensional vector space over $\mathbb{K}$ with the *standard basis* $\{1, x, x^2, \ldots, x^{m-1}\}$. This means that every polynomial $f(x) \in K[x]_h$ can be expressed as a unique linear combination of the powers of x. The *hyperbolic numbers*, studied in [**8**], have the structure of a polynomial number system.

If we now multiply both sides of (10) by $f(x)$, we get

$$f(x) = f(x)s_1(x) + f(x)s_2(x) + \cdots + f(x)s_r(x) = \sum_{i=1}^{r} f_i(x)s_i \quad \text{in} \quad \mathbb{K}[x]_h, \quad (12)$$

where

$$f_i(x) \equiv f(x) \; mod \; (x - x_i)^{m_i}. \quad (13)$$

The polynomials $f_i(x)$ defined in (13) are just the first m_i terms of the Taylor series expansion of $f(x)$ around the point $x = x_i$. In effect, we are just expanding $f(x)$ in a Taylor series piecewise around the different points in the spectrum of $f(x)$.

The modular polynomials of the form $\mathbb{K}[x]_{(x-x_0)^m}$ for $x_0 \in \mathbb{K}$, play exactly the same role in the theory of modular polynomials that numbers modulo the power of a prime play in number theory; modular polynomial problems reduce to problems involving a power $(x - x_0)^m$ of the prime factor $(x - x_0)$.

We can now solve for the idempotents $s_i(x)$ in (10). Multiplying each side of (10) by $h_i(x)$ and using (11) gives

$$h_i(x)s_i(x) = h_i(x) \quad \text{in} \quad \mathbb{K}[x]_h, \quad (14)$$

which can be solved readily in $\mathbb{K}[x]_h$ for $s_i(x)$, getting

$$s_i(x) = [h_i(x)^{-1} \; mod \; (x - x_i)^{m_i}]h_i(x)$$

for each $i = 1, 2, \ldots, r$. It is also useful to define the nilpotents

$$q_i(x) := (x - x_i)s_i(x) \quad \text{in} \quad \mathbb{K}[x]_h, \quad (15)$$

for $i = 1, 2, \ldots, r$. The nilpotent $q_i(x)$ has *index of nilpotency* m_i in $\mathbb{K}[x]_h$. By the *generalized spectral basis* of $\mathbb{K}[x]_h$ we mean

$$gsb(\mathbb{K}[x]_h) := \{s_1, q_1, \ldots, q_1^{m_1-1}, s_2, q_2, \ldots, q_2^{m_2-1}, \ldots, s_r, q_r, \ldots, q_r^{m_r-1}\}. \quad (16)$$

For $x \in \mathbb{K}[x]_h$, using (12) and (15) we get the important *generalized spectral decomposition*

$$x = \sum_{i=1}^{r}(x - x_i + x_i)s_i = \sum_{i=1}^{r}(x_i + q_i)s_i \quad \text{in} \quad \mathbb{K}[x]_h, \quad (17)$$

which we apply in Section 4 to a linear operator.

For example, let us find the spectral basis for the modular polynomial ring $\mathbb{R}[x]_h$ for $h(x) = (x - 4)(x - 1)^2$. We define $h_1 := h(x)/(x - 4) = (x - 1)^2$ and $h_2 := h(x)/(x - 1)^2 = x - 4$. To find s_1, we multiply $s_1 + s_2 = 1$ by h_1 to get

$$9s_1 = (x - 4 + 3)^2 s_1 = (x - 1)^2 s_1 = (x - 1)^2,$$

which implies that $s_1 = \frac{1}{9}(x-1)^2$. It is then a simple matter to calculate

$$s_2 = 1 - s_1 = -\frac{1}{9}(x+2)(x-4)$$

and

$$\begin{aligned} q_2 = (x-1)s_2 &= -\frac{1}{9}(x+2)(x-1)(x-4) \\ &= -\frac{1}{9}(x-1+3)(x-1)(x-4) = -\frac{1}{3}(x-1)(x-4) \end{aligned}$$

in $\mathbb{R}[x]_h$. It is also instructive to multiply $s_1 + s_2 = 1$ by $h_2 = (x-4)$ and solve directly for s_2. We get

$$[-3 + (x-1)]s_2 = (x-4)s_2 = x - 4 \quad \text{in} \quad \mathbb{R}[x]_{(x-4)(x-1)^2}.$$

Multiplying both sides of this identity by the conjugate expression $-3 - (x-1) = -x - 2$, and simplifying, gives

$$[9 - (x-1)^2]s_2 = 9s_2 = -(x+2)(x-4) \quad \Leftrightarrow \quad s_2 = -\frac{1}{9}(x+2)(x-4),$$

in agreement with our earlier result.

An arbitrary polynomial $f(x) \in \mathbb{R}[x]_{(x-4)(x-1)^2}$ can now be expressed in the generalized spectral basis

$$\{s_1, s_2, q_2\} = \left\{ \frac{1}{9}(x-1)^2,\ -\frac{1}{9}(x+2)(x-4),\ -\frac{1}{3}(x-1)(x-4) \right\}. \tag{18}$$

We find that

$$f(x) = f(4)s_1 + [f(1) + f'(1)q_2]s_2.$$

In particular, the spectral decomposition of $x \in \mathbb{R}[x]_h$ is given by

$$x = 4s_1 + (1 + q_2)s_2.$$

Table 2 gives the multiplication tables for the standard basis and the generalized spectral basis (18) of $\mathbb{R}[x]_{(x-4)(x-1)^2}$. The generalized spectral basis is valuable precisely because its multiplication table is so simple. Note that Table 2 b) makes up a sub-block of Table 1.

TABLE 2. a) The standard basis.

$\cdot$	1	x	x^2
1	1	x	x^2
x	x	x^2	$6x^2 - 9x + 4$
x^2	x^2	$6x^2 - 9x + 4$	$25x^2 - 50x + 24$

b) The spectral basis.

$\cdot$	s_1	s_2	q_2
s_1	s_1	0	0
s_2	0	s_2	q_2
q_2	0	q_2	0

Interpolation polynomials One important application of the spectral basis of the modular polynomials $\mathbb{R}[x]_h$ is to calculate the *Hermite interpolation polynomial* of any function $f(x)$ that is analytic at the spectral points $\{x_1, x_2, \ldots, x_r\} \in \mathbb{R}$. The Hermite interpolation polynomial $g(x) \in \mathbb{R}[x]_h$ of $f(x)$ is

$$\begin{aligned} g(x) &:= f\left(\sum_{j=1}^{r}(x_j + q_j)s_j\right) = \sum_{j=1}^{r} f(x_j + q_j)s_j \\ &= \sum_{j=1}^{r}\left[f(x_j) + \frac{f'(x_j)}{1!}q_j(x) + \cdots + \frac{f^{(m_j-1)}(x_j)}{(m_j-1)!}q_j^{m_j-1}(x)\right]s_j(x) \\ &= \sum_{j=1}^{r}\left[f(x_j) + \frac{f'(x_j)}{1!}(x-x_j) + \cdots + \frac{f^{(m_j-1)}(x_j)}{(m_j-1)!}(x-x_j)^{m_j-1}\right]s_j(x) \\ &\equiv \sum_{j=1}^{r}\left[\frac{f^{(m_j-1)}(x_j)}{(m_j-1)!}, \ldots, \frac{f'(x_j)}{1!}, f(x_j)\right]_{x-x_j} s_j(x) \end{aligned} \tag{19}$$

To find the interpolation polynomial $g(x)$, we use the spectral decomposition of $x \in \mathbb{R}[x]_h$, (17), and evaluate $f(x)$ by expanding in a Taylor series about the spectral points x_j. An equivalent, but much more complicated, formula can be found in [**3**, p. 101] and also in [**1**, p. 175]. Also, see [**12**] and [**13**] for an up-to-date treatment of interpolation polynomials in a more general setting.

For example, let $h(x) = (x-4)(x-1)^2$ in $\mathbb{R}[x]_h$. The $gsb(\mathbb{R}[x]_h) = \{s_1, s_2, q_2\}$ was found in (18). Let $f(x)$ be any function for which the values $f(4)$, $f(1)$, and $f'(1)$ are well defined. Then the interpolation polynomial $g(x) \in \mathbb{R}[x]_h$ of $f(x)$ is given by

$$g(x) = f(4)s_1(x) + [f(1) + f'(1)q_2]s_2(x).$$

Figures 1 and 2 show the graphs of $f(x)$ and its interpolation polynomial $g(x)$ for $f(x) = 1/(x-2)$, and $f(x) = \sin(x)$.

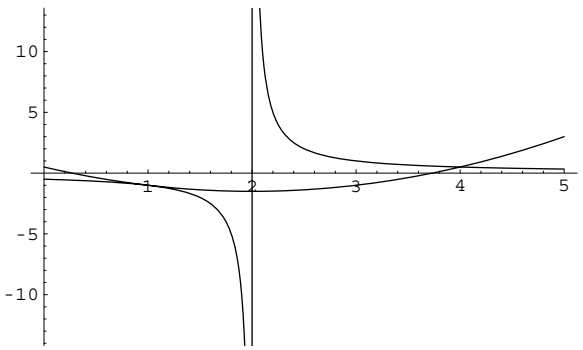

Figure 1. $f(x) = \dfrac{1}{x-2}$, $\quad g(x) = \dfrac{1}{2}s_1 - s_2 - q_2 = \dfrac{1}{2}\left(x^2 - 4x + 1\right)$

4. THE ALGEBRA OF A LINEAR OPERATOR Let $\mathcal{V}$ be an n-dimensional complex vector space, and let $End(\mathcal{V})$ denote the algebra of all *linear operators* or *endomorphisms* $f : \mathcal{V} \to \mathcal{V}$. By the algebra $\mathcal{A}(f)$ of a linear operator $f \in End(V)$, we

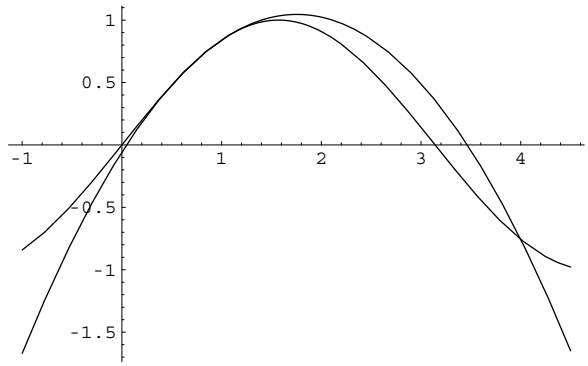

Figure 2. $f(x) = \sin x, \quad g(x) = \sin 4s_1 + \sin 1s_2 + \cos 1q_2$

mean the subalgebra of $End(\mathcal{V})$ generated by sums and powers of f. The *characteristic polynomial* of f is

$$\varphi_f(x) := \det(x - f) = \prod_{i=1}^{r} (x - x_i)^{n_i}, \tag{20}$$

where the x_i are the distinct *eigenvalues* of f in $\mathbb{C}$ and where the degree of φ is $n := deg(\varphi) = \sum_{i=1}^{r} n_i$. The *minimal polynomial* of f is the unique monic polynomial of minimal degree such that $\psi(f)\mathbf{x} = 0$ for all $\mathbf{x} \in \mathcal{V}$. The minimal polynomial ψ is closely related to the characteristic polynomial of f. We have

$$\psi(x) = \prod_{i=1}^{r} (x - x_i)^{m_i},$$

where each $1 \leq m_i \leq n_i$ and the n_i are given in (20).

The generalized spectral decomposition The crucial role of the minimal polynomial $\psi(x)$ of an operator f is a consequence of the natural isomorphism between the subalgebra $\mathcal{A}(f) \subset End(\mathcal{V})$, and the modular polynomials $\mathbb{C}[x]_\psi$. The isomorphism is most simply specified by $f \in \mathcal{A}(f) \leftrightarrow x \in \mathbb{C}[x]_\psi$. Using (17), the isomorphism between $\mathcal{A}(f)$ and $\mathbb{C}[x]_\psi$ implies that f has the *generalized spectral decomposition*

$$f = \sum_{i=1}^{r} (x_i + q_i) s_i. \tag{21}$$

The *idempotents* s_i and the *nilpotents* q_i are polynomials in f, and satisfy all the now-familiar rules modulo the polynomial $\psi(x)$. We say that the set $\{p_1, q_1, \ldots, p_r, q_r\}$ forms the *spectral basis* of the operator f.

Various forms of the generalized spectral decomposition of a linear operator are known ([**3**, p. 177], [**6**, Section 6.1, p. 401]) but they are certainly under-utilized, perhaps because of the clumsy form in which they are often presented. In [**9**] and [**10**], the spectral decomposion of a linear operator is used to derive the Jordan canonical form, and other basic canonical forms of a linear operator. The generalized spectral decomposition (21) of f is *uniquely* determined by either the characteristic or the minimal polynomial of f (up to an ordering of the s_i's). Let us conclude this section by showing the utility of the generalized spectral decomposition for a simple example.

Consider the matrix

$$F = \begin{pmatrix} -28 & 37 & -21 \\ -46 & 60 & -33 \\ -38 & 49 & -26 \end{pmatrix}, \tag{22}$$

whose characteristic and minimal polynomial are

$$\det(xI_3 - F) = (x-4)(x-1)^2,$$

where I_3 is the 3×3 identity matrix. From (18), the spectral basis $\{s_1, s_2, q_2\}$ is

$$s_1 = \frac{1}{9}(x-1)^2, \ s_2 = -\frac{1}{9}(x+2)(x-4), \text{ and } q_2 = -\frac{1}{3}(x-1)(x-4).$$

Replacing x by F in each of the spectral polynomials, we get the *spectral matrices*

$$S_1 = \frac{1}{9}(F - I_3)^2 = \begin{pmatrix} -7 & 9 & -5 \\ -14 & 18 & -10 \\ -14 & 18 & -10 \end{pmatrix}, \quad S_2 = I_3 - S_1 = \begin{pmatrix} 8 & -9 & 5 \\ 14 & -17 & 10 \\ 14 & -18 & 11 \end{pmatrix},$$

and

$$Q_2 = (F - I_3)S_2 = \begin{pmatrix} -8 & 10 & -6 \\ -4 & 5 & -3 \\ 4 & -5 & 3 \end{pmatrix}.$$

Expressing F in its spectral basis, we find the *generalized spectral decomposition*

$$F = 4S_1 + (I_3 + Q_2)S_2. \tag{23}$$

The spectral decomposition gives

$$F^{-1} = \frac{1}{4}S_1 + \frac{1}{I_3 + Q_2}S_2 = \frac{1}{4}S_1 + (I_3 - Q_2)S_2 = \frac{1}{4}\begin{pmatrix} 57 & -67 & 39 \\ 58 & -70 & 42 \\ 26 & -34 & 22 \end{pmatrix}.$$

We can also calculate $\sqrt{F}$ easily:

$$\sqrt{F} = \sqrt{4}S_1 + \sqrt{I_3 + Q_2}S_2 = 2S_1 + (I_3 + \frac{1}{2}Q_2)S_2 = \frac{1}{2}\begin{pmatrix} -20 & 28 & -16 \\ -32 & 43 & -23 \\ -24 & 31 & -15 \end{pmatrix}.$$

Having the spectral basis of the matrix F also greatly simplifies the problem of finding a basis of *generalized eigenvectors* of the matrix F. Letting $C = \{v_1, v_2, v_3\}$ be the matrix consisting of the first column vectors of the matrices S_1, Q_2, and S_2, respectively, gives a similarity

$$C^{-1}FC = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

that reduces F to its Jordan canonical form. We can check that the column vectors of C have the properties of a basis of generalized eigenvectors by noting that for $e_1 := (1 \quad 0 \quad 0)^T$,

$$v_1 = S_1 e_1, \quad v_2 = Q_2 e_1 = Q_2 S_2 e_1 = Q_2 v_3, \quad v_3 = S_2 e_1$$

and directly applying the spectral decomposition (23) of F to these vectors.

Our example (22) is nonderogatory and therefore rather special. For a more general matrix, for example, a matrix with only a single eigenvalue but with more than one elementary divisor [**3**, p. 142], the selection of a generalized basis of eigenvectors from the spectral decomposition (21) is slightly more involved [**10**, p. 184]. However, for many applications the generalized spectral decomposition (21) gives sufficiently detailed information about the linear operator.

5. GEOMETRIC EXTENSION OF THE CONCEPT OF NUMBER Historically, the complex numbers $\mathbb{C} := \mathbb{R}[x]/ < x^2 + 1 >$ arose in the early 16th century in solving cubic equations [**11**, p. 62]. At first they were considered unnatural, if not downright imaginary. It was only much later in the 19th century that Gauss demonstrated his fundamental theorem of algebra, and the bountiful complex analysis blossomed. The hyperbolic numbers $\mathbb{H} := \mathbb{R}[x]/ < x^2 - 1 >$, mentioned earlier, might also seem unnatural because we introduce new square roots of unity when they already exist in $\mathbb{R}$, i.e., ± 1. In [**8**], the hyperbolic numbers are developed alongside their sister complex numbers, and they are also shown to have utility in solving the general cubic equation.

The *complex polynomial numbers* $\mathbb{C}[x]_h := \mathbb{C}[x]/ < h(x) >$ where

$$h(x) = \prod_{i=1}^{r} (x - x_i)^{m_i}$$

for distinct $x_i \in \mathbb{C}$, seem to offer promise of a framework for a complex polynomial number analysis related to but not equivalent to the theory of analytic functions of several complex variables.

It is possible to consider polynomials $h(x)$ that have irreducible prime factors whose roots are not all in $\mathbb{K}$. The resulting theory gives a decomposition equivalent to the *first natural normal form*, [**3**, p. 192]. However, since any field can always be extended to a complete field, the much simpler theory developed here can still be applied in the extended field.

The real number system can be geometrically extended to include the concept of direction. The resulting *geometric algebra* has been proposed as a unified language for mathematics and physics in [**5**]. Indeed, the importance of the minimal polynomial came to light in this more general setting in answering the question of when an arbitrary element of a geometric algebra possesses a square root. It was only later that the connection to the classical theory of primary matrix functions, Frobenius covariants, and Schwerdtfeger's formula was brought to the author's attention [**6**, p. 438]. Discussion of the geometric interpretation of the spectral basis of a geometric number will have to wait for another day.

ACKNOWLEDGMENT The author gratefully acknowledges support given by INIP of the Universidad de las Américas-Puebla.

REFERENCES

1. P. J. Davis, *Interpolation and Approximation*, Dover Publications, New York, 1975.
2. J. A. Gallian, *Contemporary Abstract Algebra*, 4^{th} ed., Houghton Mifflin Company, Boston, 1998.
3. F. R. Gantmacher, *Theory of Matrices*, translated by K. A. Hirsch, Chelsea Publishing Co., New York, 1959.
4. T. L. Heath, *Euclid's Elements, Vol. 2*, 2nd ed., Dover Publications, New York, 1956.

5. D. Hestenes and G. Sobczyk, *Clifford Algebra to Geometric Calculus: A Unified Language for Mathematics and Physics*, 2 ed., Kluwer, Dordrecht, 1992.
6. R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, New York, 1991.
7. I. N. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, 4^{th} ed., John Wiley & Sons, New York, 1980.
8. G. Sobczyk, Hyperbolic Number Plane, *College Math. J.* 26 (1995) 268–280.
9. G. Sobczyk, The Generalized Spectral Decomposition of a Linear Operator, *College Math. J.* 28 (1997) 27–38.
10. G. Sobczyk, Spectral integral domains in the classroom, *Aportaciones Matematicas*, Serie Comunicaciones Vol. 20 (1997) 169–188.
11. D. J. Struik, *A Source Book in Mathematics, 1200–1800*, Harvard University Press, Cambridge, 1969.
12. L. Verde-Star, An Algebraic Approach to Convolutions and Transform Methods, *Adv. Appl. Math.* 19 (1997) 117–143.
13. L. Verde-Star, Approximation and Optimization, in *Proceedings of ICAOR: International Conference on Approximation and Optimization (Romania)*, I, Transilvania Press, 1997, pp. 121–138.

GARRET SOBCZYK received his Ph.D. in mathematics from Arizona State University in 1971 under the direction of David Hestenes, and is a veteran of two academic crunches. He actively witnessed the last gasp of communism during six years of post doctoral work in Poland in the late 1970's and early 1980's, sponsored by the Polish Academy of Science and an Exchange Program with University of New York at Stony Brook. During the past 8 years he has been living with his Polish wife in Mexico, under the quiet shadow of the Great Pyramid of Cholula, doing teaching and research at the beautiful Universidad de las Américas–Puebla. He now patiently awaits the thunder of mathematical pyramids in the coming reorganization from the bottom up.
Universidad de las Américas-Puebla, Departamento de Físico-Matemáticas, AP 321, Cholula 72820, Puebla, México
sobczyk@mail.udlap.mx