

$SU_I(2, F[z, 1/z])$ FOR F A SUBFIELD OF \mathbf{C}

DAVID POLLEN

INTRODUCTION

Let F be a subfield of \mathbf{C} closed under complex conjugation, and denote by $U(2, F[z, 1/z])$ the multiplicative group of two-by-two unitary matrices over the ring $F[z, 1/z]$ where $|z| = 1$. Let $SU_I(2, F[z, 1/z])$ be the subgroup of such unitary matrices with determinant equal to the constant polynomial 1 and which are equal to the identity matrix upon evaluation at $z = 1$.

The main result is the Unique Factorization Theorem for $SU_I(2, F[z, 1/z])$, which expresses each element as an unique product of a minimal number of simple factors in $SU_I(2, F[z, 1/z])$. Since these factors are free of relations, it follows that $SU_I(2, F[z, 1/z])$ is a (nonabelian) free group generated by the factors.

Besides having interesting algebraic and topological properties from the standpoint of pure mathematics, these unitary groups have application to the theory of Quadrature Mirror Filter banks and to the theory of "wavelets" with compact support especially in parameterizing various classes of QMF banks and wavelet families.

After this manuscript was completed, the author's attention was drawn to reference [V], which derives (nonunique) factorizations of the groups $U(d, \mathbf{R}[z, 1/z])$ and $U(d, \mathbf{C}[z, 1/z])$ for $d \geq 2$. Reference [V], part of the extensive QMF literature, concentrates mainly on the application of these factorizations to design QMF banks for particular digital signal processing problems.

The theory of wavelets with compact support provides both a generalization of and an analytical viewpoint of QMF theory. Wavelets with compact support were recently discovered by Ingrid Daubechies as described in [D1] and [D2].

BASIC DEFINITIONS AND NOTATIONS

In \mathbf{C} , the field of complex numbers, denote the complex conjugation action by an overscore. Let F be a subfield of \mathbf{C} *closed under complex conjugation*. The simplest examples of F will be \mathbf{Q} , \mathbf{R} , and \mathbf{C} itself.

Received by the editors April 21, 1989.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 20G15, 22E65.

©1990 American Mathematical Society

Let z be an indeterminant, a variable whose values are limited to the circle, the complex numbers of norm one. Form the ring of circular Laurent polynomials in z with coefficients in F , denoted $F[z, 1/z]$. The elements of this ring are *finite* sums of the form

$$h(z) = \sum_{k=-N}^N h_k z^k \quad \text{for } h_k \in F \text{ and } N \geq 0.$$

Equip $F[z, 1/z]$ with a natural conjugation operation denoted \sim , which takes the complex conjugate of elements of F and the reciprocal of occurrences of z since, as required above, $|z|^2 = z\bar{z} = 1 \Leftrightarrow \bar{z} = 1/z$. So

$$\widetilde{h(z)} = \left(\overline{\sum_{k=-N}^N h_k z^k} \right) = \sum_{k=-N}^N \bar{h}_k z^{-k} = \sum_{k=-N}^N \bar{h}_{-k} z^k.$$

The restriction that $z\bar{z} = 1$ may seem unnatural and uninspired. Note that in the case where $i \in F$, $F[z, 1/z]$ is in the well-known ring of trigonometric polynomials. Defining indeterminants $c = (z + 1/z)/2$ and $s = (z - 1/z)/(2i)$, we see $z = c + is$ and $1/z = c - is$; hence $z\bar{z} = 1 \Leftrightarrow s^2 + c^2 = 1$. We intend to think of the variables s and c as the sine and cosine functions. As a ring, $F[z, 1/z]$ is isomorphic to $F[s, c]/(s^2 + c^2 - 1, sc - cs)$ when $i \in F$.

A measure of the size of elements of $F[z, 1/z]$ is given by the Laurent degree denoted deg , which is in $\{0\} \cup \mathbf{N}$. For $h(z) \in F[z, 1/z]$, $\text{deg}(h(z))$ is the smallest number d such that the coefficients of the z^k terms in $h(z)$ are zero for all $|k| > d$. For example,

$$\begin{aligned} \text{deg}(h(z)) = 0 & \quad \text{iff } h(z) \in F \subseteq F[z, 1/z], \\ \text{deg}(z^{-2} + 3 + 2z) = 2, & \quad \text{and } \text{deg}(z^{-3} + z^5) = 5. \end{aligned}$$

For any $h_1(z)$ and $h_2(z)$

$$\text{deg}(h_1(z) \pm h_2(z)) \leq \max(\text{deg}(h_1(z)), \text{deg}(h_2(z)))$$

and

$$\text{deg}(h_1(z)h_2(z)) \leq \text{deg}(h_1(z)) + \text{deg}(h_2(z)),$$

with equality almost always occurring. Finally, note

$$\text{deg}(\widetilde{h(z)}) = \text{deg}(h(z)).$$

For any ring R with a conjugation operation \sim , let $S^0(R) \subseteq R$ be the subset of elements x such that $x\bar{x} = 1$. Note $S^0(R)$ has a natural induced multiplicative group structure. For example, $S^0(\mathbf{R}) = \{-1, 1\}$. It can be easily seen that $S^0(F[z, 1/z]) \approx S^0(F) \times \mathbf{Z}$ as a group. Also let $S^1(R) \subseteq R \times R$ be the subset of elements (x, y) such that $x\bar{x} + y\bar{y} = 1$. Note that $S^1(\mathbf{R})$ is the circle.

Let $U(2, F[z, 1/z])$ be the group of two-by-two unitary matrices with elements in the ring $F[z, 1/z]$. Since this is a group of unitary matrices, the

inverse of an element equals its adjoint (denoted by \dagger) obtained by applying the \sim conjugate to the transpose of the matrix, i.e., $U^\dagger = \widetilde{U}^T$. Let $SU(2, F[z, 1/z])$ be the kernel of the natural determinant group epimorphism from $U(2, F[z, 1/z])$ onto $S^0(F[z, 1/z])$. Let $U_I(2, F[z, 1/z])$ be the kernel of the natural evaluate z at 1 group epimorphism from $U(2, F[z, 1/z])$ onto $U(2, F)$. Define

$$SU_I(2, F[z, 1/z]) = SU(2, F[z, 1/z]) \cap U_I(2, F[z, 1/z]);$$

all three of these groups are normal subgroups of $U(2, F[z, 1/z])$. This group is the subgroup of $U(2, F[z, 1/z])$ whose elements have determinant 1 and which equal I at $z = 1$, where I denotes the identity matrix. It is with the structure of $SU_I(2, F[z, 1/z])$ that this paper is mainly concerned. For $M(z)$ a unitary matrix, we will often suppress the argument and simply write M .

The degree defined on $F[z, 1/z]$ can be extended to $U(2, F[z, 1/z])$. If C is a unitary matrix, the four entries C_{00}, C_{01}, C_{10} , and C_{11} are in $F[z, 1/z]$. We define the matrix degree

$$\text{deg}(C) = \max(\text{deg}(C_{00}), \text{deg}(C_{01}), \text{deg}(C_{10}), \text{deg}(C_{11})).$$

Note,

$$\text{deg}(C) = 0 \quad \text{iff } C \in U(2, F) \subseteq U(2, F[z, 1/z]);$$

$$\text{deg}(C^{-1}) = \text{deg}(C) \quad \text{since } C^{-1} = C^\dagger.$$

For D another unitary matrix

$$\text{deg}(CD) \leq \text{deg}(C) + \text{deg}(D).$$

Proposition 1 (Decomposition Theorem for $U(2, F[z, 1/z])$). *For every element $M \in U(2, F[z, 1/z])$ there exist unique $A \in U(2, F)$, $B = \begin{pmatrix} 1 & 0 \\ 0 & z^k \end{pmatrix} \in U(2, F[z, 1/z])$ with $k \in \mathbf{Z}$, and $C \in SU_I(2, F[z, 1/z])$ such that $M = ABC$.*

Proof. This theorem follows directly from definitions. Let $A = M(1)$. We now want to factor $N = A^\dagger M$ as $N = BC$.

If

$$N = \begin{pmatrix} N_{00} & N_{01} \\ N_{10} & N_{11} \end{pmatrix}$$

then let

$$C = \begin{pmatrix} N_{00} & N_{01} \\ -\widetilde{N_{01}} & \widetilde{N_{00}} \end{pmatrix}.$$

Note C is unitary since N is. Let

$$B = NC^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & b(z) \end{pmatrix}.$$

Since B is unitary, $b(z) \in S^0(F[z, 1/z])$. Note $N \in U_I(2, F[z, 1/z])$. So, C, C^\dagger , and B are likewise. Thus $b(1) = 1$. So $b(z) = z^k$ for some $k \in \mathbf{Z}$. Verifying that C is in $SU_I(2, F[z, 1/z])$ will finish the proof since $BC = N$, but this follows by the construction of C .

Proposition 2 (Structure of elements of $SU_I(2, F[z, 1/z])$). *Let*

$$M \in SU_I(2, F[z, 1/z]).$$

Then

$$M = \begin{pmatrix} \widetilde{M}_{00} & \widetilde{M}_{01} \\ -\widetilde{M}_{01} & \widetilde{M}_{00} \end{pmatrix}.$$

As a result, we have the topological homeomorphism:

$$SU_I(2, F[z, 1/z]) \xrightarrow{\sim} S^1(F[z, 1/z])$$

given by $M \mapsto (M_{00}, M_{01})$.

Theorem 1 (Finite order elements in $SU_I(2, F[z, 1/z])$). *If*

$$M \in SU_I(2, F[z, 1/z]), \quad p \in \mathbf{Z}, \quad \text{and} \quad M^p = I,$$

then $M = I$.

Proof. We need only investigate the case $F = \mathbf{C}$. Consider $SU(2; \mathbf{C})$. For fixed p , look at the subset of elements of $SU(2, \mathbf{C})$ of order p . It is seen that I is one of many such elements but that the path component of I contains only I (simple exercise).

M can be regarded as a continuous map from the circle of possible complex values for z into the subset of $SU(2, \mathbf{C})$ of elements of order p . Since $M(1) = I$, the image of M under this map must always be I by the above paragraph and by path connectedness of the circle.

Hence $M = I$.

Warning: for the continuity of M to hold in the above proof it is *essential* to use finite Laurent series. When infinite Laurent series are allowed, M need not be continuous in z and Theorem 1 fails since $SU_I(2, F[[z, 1/z]])$ has nontrivial finite order elements!

Remark. Theorem 1 is a trivial corollary of Theorem 3. We present the above proof of Theorem 1 here for its value as a proof technique.

Definition. Let

$$\text{Factors}(F) \subseteq SU_I(2, F[z, 1/z])$$

be the $X = \begin{pmatrix} p(z) & q(z) \\ -\bar{q}(z) & \bar{p}(z) \end{pmatrix}$ such that $p(z) = a + cz$ and $q(z) = b + dz$ for some $a, b, c, d \in F$. Not all choices of a, b, c , and d produce unitary matrices. Note that $I \in \text{Factors}(F)$.

Proposition 3 (Parameterization of $\text{Factors}(F)$). *The map*

$$\rho: S^1(F) \cap \{(u, v) | u \in \mathbf{R}\} \rightarrow \text{Factors}(F)$$

is a bijection of sets such that $\rho(1, 0) = I$. *For* $(u, v) \in S^1(F)$ *and* $u \in \mathbf{R} \cap F$, *let*

$$\begin{aligned} a &= (u + 1)/2 \quad (\text{note } a \in \mathbf{R} \cap F), \\ b &= v/2, \quad c = 1 - a, \quad d = -b, \quad \text{all in } F, \\ p(z) &= a + cz, \quad q(z) = b + dz \quad \text{all in } F[z, 1/z]. \end{aligned}$$

Then defining

$$\rho(u, v) = \begin{pmatrix} p(z) & q(z) \\ -\overline{q(z)} & \overline{p(z)} \end{pmatrix},$$

we have the homeomorphism

$$\rho: S^1(F) \cap \{(u, v) | u \in \mathbf{R}\} \xrightarrow{\sim} \text{Factors}(F).$$

Proof. The condition that a factor be I at 1 implies $a + c = 1$ and $b + d = 0$. Using unitarity (and some algebra) all the other conditions can eventually be written as equivalent to the single condition $a\bar{a} + b\bar{b} = a$. Note this condition implies a is real.

By adding the equation to its conjugate and dividing by two we get

$$\begin{aligned} a\bar{a} - \frac{a}{2} - \frac{\bar{a}}{2} + b\bar{b} &= 0, \\ |a - \frac{1}{2}|^2 + |b|^2 &= \frac{1}{4}, \\ |2a - 1|^2 + |2b|^2 &= 1. \end{aligned}$$

Remarks. Topologically, $\text{Factors}(\mathbf{R})$ is a circle, $\text{Factors}(\mathbf{C})$ is a 2-sphere, and $\text{Factors}(\mathbf{Q})$ is the set of rational points on the unit circle, i.e., the relatively prime Pythagorean triples.

Remarks. $\text{Factors}(F)$ is a set. It is not closed under multiplication or inversion! $\text{Factors}(F)$ contains the identity matrix, which has degree equal to zero. All its other elements are of degree one. However, as we will demonstrate, $\text{Factors}(F)$ does not contain all the elements of $SU_I(2, F[z, 1/z])$ of degree 1.

We now investigate the form of the inverse of the elements in the set $\text{Factors}(F)$. Let $X \in \text{Factors}(F)$. Then

$$X = \begin{pmatrix} a + cz & b + dz \\ -\bar{d}/z - \bar{b} & \bar{c}/z + \bar{a} \end{pmatrix}.$$

So

$$X^\dagger = \begin{pmatrix} \bar{c}/z + \bar{a} & -b - dz \\ \bar{d}/z + \bar{b} & a + cz \end{pmatrix}.$$

Note $(\text{Factors}(F))^\dagger$ is a set of degree 1 or 0 elements. Moreover,

$$\{I\} = \text{Factors}(F) \cap (\text{Factors}(F))^\dagger.$$

Consider the map $\text{Factors}(F) \times \text{Factors}(F) \rightarrow SU_I(2, F[z, 1/z])$:

$$q: (A, B) \mapsto A^\dagger B.$$

By basic properties of the degree of an inverse and of products, one can see that the degree of the image must always be 0, 1, or 2.

It is easily verified that the degree of the image cannot be 2 because of the special form of the factor elements.

The degree of an element of $SU_I(2, F[z, 1/z])$ is zero iff the element is the identity matrix. So the degree of the image of (A, B) is I iff $A = B$.

Let $Q = \{\text{elements of degree } \leq 1 \text{ in } SU_I(2, F[z, 1/z])\}$. Let

$$W = \text{Factors}(F) \times \text{Factors}(F).$$

Let Δ be the diagonal in W , of all elements in the form (A, A) .

Proposition 4 (Form of degree one elements of $SU_I(2, F[z, 1/z])$). $q: W \rightarrow Q$ and $q: W - \Delta \rightarrow Q - \{I\}$ are well defined.

Remark. This last map is in fact a bijection as will follow by specializing the Unique Factorization Theorem to the case of degree 1 elements. But we point this fact out now as to allow the reader a full understanding of the structure of degree one elements of $SU_I(2, F[z, 1/z])$.

Lemma 1. Let $\begin{pmatrix} x \\ y \end{pmatrix}$ be a nonzero vector in the vector space $F \times F$ over F . Also consider the set in $F \times F$ described by

$$(*) \quad c\bar{c} + d\bar{d} = c \quad \text{for } (c, d) \in F \times F.$$

(Hence, c is real.)

If $x \neq 0$, then

$$\lambda = \frac{x}{x\bar{x} + y\bar{y}}$$

is the unique nonzero element of F such that $c = \lambda\bar{x}$, $d = \lambda\bar{y}$ is a solution to $(*)$. If $x = 0$, then $c = \lambda\bar{x}$, $d = \lambda\bar{y}$ is a solution to $(*)$ is equivalent to $\lambda = 0$.

Proof. Let $\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} \lambda\bar{x} \\ \lambda\bar{y} \end{pmatrix}$ in $(*)$. Then

$$\lambda\bar{\lambda}(x\bar{x} + y\bar{y}) = \lambda\bar{x}.$$

So

$$\lambda = 0 \quad \text{or} \quad \lambda = \frac{x}{x\bar{x} + y\bar{y}}.$$

Ignoring the $\lambda = 0$ solution, we note $x\bar{x} + y\bar{y} \neq 0$ by hypothesis and since F is a field $\lambda = x/(x\bar{x} + y\bar{y})$ is indeed in F . Recall F must be closed under complex conjugation.

Note, $c = \lambda\bar{x}$ must be real.

We will later see that factorization will fail for F not a field because λ needs a division to be computed!

Definition. Denote by $M(2, F)$, the ring of all two-by-two matrices over F .

Define $\omega: M(2, F) \rightarrow M(2, F)$ by

$$\omega(N) = \omega \begin{pmatrix} N_{00} & N_{01} \\ N_{10} & N_{11} \end{pmatrix} = \begin{pmatrix} \bar{N}_{11} & -\bar{N}_{10} \\ -\bar{N}_{01} & \bar{N}_{00} \end{pmatrix} = J^{-1}\bar{N}J,$$

where $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The map ω is well defined since by hypothesis F is closed under conjugation.

Proposition 5. (1) ω is a ring automorphism of $M(2, F)$; i.e., $\omega(N + P) = \omega(N) + \omega(P)$ and $\omega(NP) = \omega(N)\omega(P)$.

(2) ω^2 is the identity automorphism.

Proposition 6. Let $M \in SU_I(2, F[z, 1/z])$ of degree m . Express M as

$$M = \sum_{k=-m}^m M_k z^k \text{ for } M_k \in M(2, F).$$

Then $M_k = \omega(M_{-k})$ or equivalently $M_{-k} = \omega(M_k)$. We call the M_k 's the coefficient matrices of M .

Proof. Follows from fact $M = \begin{pmatrix} p & q \\ -q & p \end{pmatrix}$ for some $p, q \in F[z, 1/z]$.

Lemma 2. Let $M \in SU_I(2, F[z, 1/z])$ of nonzero degree m . Express M as $\sum_{k=-m}^m M_k z^k$ for $M_k \in M(2, F)$. Then

$$M_{-m} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ yet } \det(M_{-m}) = 0.$$

Hence writing

$$M_{-m} = \begin{pmatrix} (M_{-m})_{00} & (M_{-m})_{01} \\ (M_{-m})_{10} & (M_{-m})_{11} \end{pmatrix},$$

at least one choice of

$$\begin{pmatrix} (M_{-m})_{00} \\ (M_{-m})_{10} \end{pmatrix} \text{ or } \begin{pmatrix} (M_{-m})_{01} \\ (M_{-m})_{11} \end{pmatrix}$$

must not be $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ and if both columns are nontrivial then they are parallel.

Proof. If $M_{-m} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ by Proposition 6, $M_m = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ in which case $\deg(M) \neq m$ yielding a contradiction.

Since $M \in SU_I(2, F[z, 1/z])$, $\det(M) = 1$ as a Laurent polynomial in z . In the expression for $\det(M)$, $\det(M_{-m})$ is the coefficient of the z^{-2m} term, which must be zero since $m \neq 0$.

Lemma 3 (First Factor Lemma). Let $X \in \text{Factors}(F)$ and $M \in SU_I(2, F[z, 1/z])$ be of nonzero degree m . (Note $\deg(X) \leq 1$.)

We almost always have equality in $\deg(XM) \leq \deg(X) + \deg(M) = m + 1$. The cases of inequality concern us here. We want to know when multiplication by a factor element does not increase the degree by one.

Given M , let $x, y \in F$ be a nonzero column of M_{-m} . Then

$$\begin{pmatrix} x \\ y \end{pmatrix} \text{ is parallel to } \begin{pmatrix} (M_{-m})_{00} \\ (M_{-m})_{10} \end{pmatrix} \text{ is parallel to } \begin{pmatrix} (M_{-m})_{01} \\ (M_{-m})_{11} \end{pmatrix}.$$

Recall at least one of the latter two vectors is nonzero by Lemma 2. Let $\lambda = x/(x\bar{x} + y\bar{y})$. Note $\lambda \in F$.

Let

$$c = \lambda\bar{x}, \quad d = \lambda\bar{y}, \quad a = 1 - c, \quad b = -d.$$

Let $p = a + cz$, $q = b + dz$ and let $A = \begin{pmatrix} p & q \\ -\bar{q} & \bar{p} \end{pmatrix}$. We will show $A \in \text{Factors}(F)$.

A may indeed be the identity matrix. This occurs iff for all elements X of $\text{Factors}(F) - \{I\}$ we have $\deg(XM) = \deg(M) + 1$. This happens exactly when M has the following form:

$$(**) \quad M_{-m} = \begin{pmatrix} 0 & 0 \\ ? & ? \end{pmatrix} \quad \text{and} \quad \omega(M_{-m}) = M_m = \begin{pmatrix} ? & ? \\ 0 & 0 \end{pmatrix}.$$

If A is not I , then A is the unique element of $\text{Factors}(F)$ (other than I) such that

$$m - 1 \leq \deg(AM) \leq \deg(M) = m.$$

Still in the case where $A \neq I$, AM has the form $(**)$ meaning that its leftmost nontrivial coefficient matrix has upper row zero and its rightmost nontrivial coefficient matrix has lower row zero.

Since in all cases for A

$$M = (A^\dagger A)M = A^\dagger(AM),$$

we have factored M into A^\dagger and AM .

For A produced above, we call A the first factor of M and AM the remainder. We always have

$$(AM)_{-m} = \begin{pmatrix} 0 & 0 \\ ? & ? \end{pmatrix} \quad \text{and} \quad (AM)_m = \begin{pmatrix} ? & ? \\ 0 & 0 \end{pmatrix}.$$

It is perfectly acceptable for I to occur as the first factor A .

Proof. Let

$$X = \begin{pmatrix} 0 & 0 \\ -\bar{d} & \bar{c} \end{pmatrix} 1/z + \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} z.$$

Express

$$M = M_{-m}z^{-m} + \dots + M_mz^m.$$

If $\deg(XM) \leq \deg(M) = m$,

$$\begin{pmatrix} 0 & 0 \\ -\bar{d} & \bar{c} \end{pmatrix} M_{-m} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} M_m = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Using ω , these two conditions are equivalent. So let us only examine the first.

$$\begin{pmatrix} 0 & 0 \\ -\bar{d} & \bar{c} \end{pmatrix} M_{-m} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

By Lemma 2, choose $\begin{pmatrix} x \\ y \end{pmatrix}$ a nonzero vector generating the exactly one-dimensional image of M_{-m} from the columns of M_{-m} . We want

$$\begin{pmatrix} -\bar{d} & \bar{c} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0;$$

i.e., we want $\begin{pmatrix} c \\ d \end{pmatrix} = \lambda \begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix}$ for some $\lambda \in F$. So that $X \in \text{Factors}(F)$, we must have $a\bar{a} + b\bar{b} = a$ from Proposition 3. This condition is equivalent to $c\bar{c} + d\bar{d} = c$ since $a + c = 1$ and $b + d = 0$.

Now apply Lemma 1.

Let $\lambda = x/(x\bar{x} + y\bar{y})$. This is the *only choice*. λ will be zero only if $x = 0$.

We have constructed $A \in \text{Factors}(F)$. We want to understand the $-m$ th coefficient matrix of AM .

$$(AM)_{-m} = A_{-1}M_{-m+1} + A_0M_{-m}.$$

Now

$$A_{-1} = \begin{pmatrix} 0 & 0 \\ -\bar{d} & \bar{c} \end{pmatrix}, \quad A_0 = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}.$$

So

$$(AM)_{-m} = \begin{pmatrix} 0 & 0 \\ ? & ? \end{pmatrix} + \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} M_{-m}.$$

But this sum has the form $\begin{pmatrix} 0 & 0 \\ ? & ? \end{pmatrix}$ as we shall now show. Surprisingly enough

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} (M_{-m})_{00} \\ (M_{-m})_{10} \end{pmatrix} = 0 \quad \text{and} \quad \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} (M_{-m})_{01} \\ (M_{-m})_{11} \end{pmatrix} = 0.$$

Indeed $\begin{pmatrix} a \\ b \end{pmatrix}$ is parallel to $\begin{pmatrix} \bar{d} \\ -\bar{c} \end{pmatrix}$ for A to be in $\text{Factors}(F)$ (see Proposition 3).

But $\begin{pmatrix} \bar{d} \\ -\bar{c} \end{pmatrix}$ is perpendicular to $\begin{pmatrix} \bar{c} \\ \bar{d} \end{pmatrix}$ which is parallel to both

$$\begin{pmatrix} (M_{-m})_{00} \\ (M_{-m})_{10} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} (M_{-m})_{01} \\ (M_{-m})_{11} \end{pmatrix}$$

by construction.

The rest of the lemma follows easily.

Lemma 4 (Second Factor Lemma). *Let $X \in \text{Factors}(F)$, which is necessarily of degree 0 or 1. Let $R \in SU_1(2, F[z, 1/z])$ be of nonzero degree m such that $R_{-m} = \begin{pmatrix} 0 & 0 \\ r & s \end{pmatrix}$.*

It is easy to verify that we never have $\deg(X^\dagger R) = m + 1$. We almost always have equality in the expression $\deg(X^\dagger R) = m$.

We will show that there always exists a unique $X \neq I$ with the property that $\deg(X^\dagger R) = m - 1$. This unique X , denoted B , will be called the second factor. For R will have been factored into $R = B(B^\dagger R)$. $B^\dagger R$ is called the remainder and is necessarily of degree $m - 1$. A formula for computing B is given below.

Proof. Denote X^\dagger as

$$X^\dagger = \begin{pmatrix} \bar{c} & 0 \\ \bar{d} & 0 \end{pmatrix} 1/z + \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} + \begin{pmatrix} 0 & -d \\ 0 & c \end{pmatrix} z.$$

Denote $R_{-m+1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$. If $\deg(X^\dagger R) \neq m + 1$, then (using ω and coefficient matrices) $(X^\dagger)_{-1}R_{-m}$ must be the zero matrix. This circumstance always occurs as stated above.

If $\deg(X^\dagger R) < m$, then we must have $(X^\dagger)_{-1}R_{-m+1} + (X^\dagger)_0R_{-m}$ equal to the zero matrix. Writing out this matrix and then factoring it, we want (recall

$a, c \in \mathbf{R}$)

$$\begin{pmatrix} -b & c \\ \bar{a} & \bar{d} \end{pmatrix} \begin{pmatrix} r & s \\ e & f \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

It is easily seen that the two left-hand matrices have determinant zero, but that neither one can be the zero matrix. $X \in \text{Factors}(F) \Rightarrow a\bar{c} + b\bar{d} = 0$. That $rf - es = 0$ follows from fact that $\det(R) = 1$ as a Laurent polynomial and that $rf - es$ appears as the coefficients of z^{-2m+1} . For $X \in \text{Factors}(F)$, not all a, b, c , and d can be zero. By hypothesis, $\deg(R) = m$, so $r \neq 0$ or $s \neq 0$.

Choose $\begin{pmatrix} x \\ y \end{pmatrix}$ to be a nonzero column of $\begin{pmatrix} r & s \\ e & f \end{pmatrix}$. Note $x, y \in F$. Note $x \neq 0$ since $r \neq 0$ or $s \neq 0$.

Let $\lambda = \bar{x}/(x\bar{x} + y\bar{y})$. Since $x \neq 0$, $\lambda \neq 0$. Note $\lambda \in F$.

It is easy to verify that the only valid choice for a, b, c , and d is given by the below equations since we must have $c\bar{c} + b\bar{b} = c$.

$$\begin{pmatrix} b \\ c \end{pmatrix} = \lambda \begin{pmatrix} y \\ x \end{pmatrix} \quad (\text{note } c \in \mathbf{R}),$$

$$a = 1 - c \quad (\text{note } a \in \mathbf{R}), \quad d = -b.$$

Note a, b, c , and $d \in F$. Let $p = a + cz$, $q = b + dz$. And $B = \begin{pmatrix} p & q \\ -\bar{q} & \bar{p} \end{pmatrix}$. Then $B \in \text{Factors}(F) - I$. Note since $x \neq 0$ and $\lambda \neq 0$, then $c \neq 0$. So B can never be I .

Theorem 2 (The Unique Factorization Theorem for $SU_1(2, F[z, 1/z])$). *Let $M \in SU_1(2, F[z, 1/z])$ with $\deg(M) > 0$.*

(1) *There exist $A_i, B_i \in \text{Factors}(F)$ such that $M = A_1^\dagger B_1 \cdots A_m^\dagger B_m$. This expression is the factorization of M as a product of $2m$ factor inverse and factor elements. Furthermore, this factorization is unique. If $M = J_1^\dagger K_1 \cdots J_m^\dagger K_m$ for $J_i, K_i \in \text{Factors}(F)$, then for all i , $A_i = J_i$ and $B_i = K_i$.*

I may occur in the factorization expression, but I cannot occur adjacent to other I 's because a contradiction would be evident upon taking degrees.

(2) *Note this theorem has a slightly weaker form. Let $C_i = A_i^\dagger B_i$. By Proposition 4, the C_i 's are of degree 1 and in this case $M = C_1 \cdots C_m$ is a factorization of M into m degree 1 elements (but not necessarily factor elements). Note none of these C_i 's can be I by a degree argument. This degree one factorization is also unique. For if $M = D_1 \cdots D_m$ for D_i degree 1 elements, then for all i , $C_i = D_i$.*

Proof of existence. Proof by induction on m .

Use the First Factor Lemma on M to get $A_1 \in \text{Factors}(F)$. Let $R = A_1 M$. Either $\deg(R) = m$ or $\deg(R) = m - 1$.

If $\deg(R) = m - 1$, let $B_1 = I$, and find the remaining factors of M by factoring R , which is of degree $m - 1$.

If $\deg(R) = m$, use the Second Factor Lemma on R to find $B_1 \in \text{Factors}(F)$ such that $B_1^\dagger R$ has degree $m - 1$. Now find the remaining factors of M by factoring $B_1^\dagger R$, which must be of degree $m - 1$.

Proof of uniqueness. Degree one factorization uniqueness (2) of the hypothesis follows from uniqueness of factorization (1).

Proof by induction on m .

Say $M = A_1^\dagger B_1 \cdots A_m^\dagger B_m = J_1^\dagger K_1 \cdots J_m^\dagger K_m$ for J_i and K_i in $\text{Factors}(F)$. We want to show for all i that $A_i = J_i$ and $B_i = K_i$. Here the A_i 's and B_i 's have come from the factorization procedure above. Much of this proof will depend on heavy usage of elementary properties of the degree.

Note $\deg(J_1 M) \leq m$ since $J_1 M = K_1 \cdots J_m^\dagger K_m$, and we can group, for all $i > 1$, the $J_i^\dagger K_i$ into a degree 1 elements by Proposition 4. By the First Factor Lemma, since $\deg(J_1 M) \leq m$ either $J_1 = I$ or J_1 is the first factor of M which must be A_1 . If $J_1 \neq A_1$, then we would have to have $J_1 = I$ and $A_1 \neq I$. If $J_1 = I$, then $M = K_1 \cdots J_m^\dagger K_m$. Note $K_1 \neq I$ since $\deg(M) = m$. But then M would have to have exactly the form in the First Factor Lemma to require that M 's first factor A_1 be I . This contradiction means that we *must* have $A_1 = J_1$.

Let $R = A_1 M = J_1 M$. R must have degree m or degree $m - 1$.

If $\deg(R) = m$, note $\deg(B_1^\dagger R) = \deg(K_1^\dagger R) = m - 1$ by degree arguments. By the Second Factor Lemma, we must thus have $B_1 = K_1$.

If $\deg(R) = m - 1$, then $B_1 = I$ because it was *chosen that way* in the existence part of the proof. Let $Q = J_2^\dagger K_2 \cdots J_m^\dagger K_m$. Note $\deg(Q) = m - 1$ exactly. Since $R = K_1 Q$ and $\deg(R) = m - 1$. Then $\deg(K_1 Q) \leq \deg(Q)$. So by the First Factor Lemma applied to Q , either $K_1 = I$, in which case we are done with the argument in this paragraph, or K_1 is the first factor of Q , which is of degree $m - 1$ by uniqueness of factorization for Q . The first factor of Q *must be* J_2 . Hence, $K_1 = J_2$. This cannot be, for then we would have cancellation in $\deg(M) = \deg(J_1^\dagger K_1 J_2^\dagger K_2 \cdots J_m^\dagger K_m)$, yielding the contradiction that $m = m - 1$. Hence, K_1 actually had to be I . So $B_1 = K_1$ always.

The uniqueness of the remaining factors follows by induction on m .

DISCUSSION AND IMPLICATIONS

Not all products of the form $A_1^\dagger B_1 \cdots A_m^\dagger B_m$ for $A_i, B_i \in \text{Factors}(F)$ are of degree m . Examples of this phenomenon are the adjacency of elements and their inverses or adjacent identity elements in the expression. Such nonminimal degree products cannot appear as the factorization of any element since their product has a simpler factorization in terms of fewer factors.

Note that implicit in this paper is a *Factorization Algorithm* for computing all the factors of an element of $SU_1(2, F[z, 1/z])$. It can easily be verified that the factors can be computed from the coefficients of the polynomial matrix entries *using only field operations on F and complex conjugation*. This remarkable property of $SU_1(2, F[z, 1/z])$ is in contrast to the situation in $\mathbb{C}[x]$, which has a somewhat similar Unique Factorization Theorem, the Fundamental Theorem of Algebra. In $\mathbb{C}[x]$, computation of the factors of polynomials from their coefficients often requires radical operations. And, as Galois theory tells us,

even the radical operations will not suffice for general polynomial factorization in $\mathbb{C}[x]$ for polynomials of degree five or greater.

Example. Let $M \in SU_I(2, \mathbb{Q}[z, 1/z])$, where

$$M = \frac{1}{55250} \begin{pmatrix} p & q \\ -\tilde{q} & \tilde{p} \end{pmatrix},$$

where

$$p = p(z) = -12/z^2 - 4173/z + 52435 + 6982z + 18z^2,$$

$$q = q(z) = -9/z^2 - 3311/z + 12170 - 8826z - 24z^2.$$

Note $\deg(M) = 2$.

Then $M = A_1^\dagger B_1 A_2^\dagger B_2$ for A_1, A_2, B_1, B_2 in Factors(Q):

$$A_1 = \frac{1}{5} \begin{pmatrix} 4 + z & 2 - 2z \\ -2/z - 2 & 1/z + 4 \end{pmatrix},$$

$$B_1 = \frac{1}{13} \begin{pmatrix} 9 + 4z & 6 - 6z \\ -6/z - 6 & 4/z + 9 \end{pmatrix},$$

$$A_2 = \frac{1}{34} \begin{pmatrix} 25 + 9z & 15 - 15z \\ -15/z - 15 & 9/z + 25 \end{pmatrix},$$

$$B_2 = \frac{1}{25} \begin{pmatrix} 16 + 9z & 12 - 12z \\ -12/z - 12 & 9/z + 16 \end{pmatrix}.$$

Discussion. Let $M, N \in SU_I(2, F[z, 1/z])$ be of nonzero degrees m and n respectively. We almost always have equality in $\deg(MN) \leq \deg(M) + \deg(N)$. We want to know exactly when we have equality.

Using the Unique Factorization Theorem, factorize

$$M = A_1(M)^\dagger B_1(M) \cdots A_m(M)^\dagger B_m(M)$$

and

$$N = A_1(N)^\dagger B_1(N) \cdots A_n(N)^\dagger B_n(N).$$

We will call $B_m(M)$ the *last factor* of M . Recall $A_1(N)$ is the *first factor* of N .

Lemma 5 (Maximal Degree of Product Lemma). *We will show $\deg(MN) < \deg(M) + \deg(N)$ iff the last factor of M equals the first factor of N .*

Proof. \Leftarrow is obvious by using basic properties of the degree and grouping the remaining factors after cancellation into $m + n - 1$ degree 1 elements using Proposition 4.

\Rightarrow Using Lemma 2, M_{-m} and N_{-n} each have determinant 0 but are not the zero matrix. Note we can assume $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma',$ and δ' are in F where

$$M_{-m} = \begin{pmatrix} \alpha\gamma & \alpha\delta \\ \beta\gamma & \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} (\gamma \ \delta)$$

and

$$N_{-n} = \begin{pmatrix} \alpha'\gamma' & \alpha'\delta' \\ \beta'\gamma' & \beta'\delta' \end{pmatrix} = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} (\gamma' \ \delta').$$

Now $\deg(MN) < \deg(M) + \deg(N)$ iff $(MN)_{-m-n} = M_{-m}N_{-n}$ is the zero matrix. But

$$\begin{aligned} M_{-m}N_{-n} &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} (\gamma \ \delta) \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} (\gamma' \ \delta') \\ &= (\gamma\alpha' + \delta\beta') \begin{pmatrix} \alpha \\ \beta \end{pmatrix} (\gamma' \ \delta'). \end{aligned}$$

Since M_{-m} and N_{-n} are each not the zero matrix, then none of $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $\begin{pmatrix} \gamma \\ \delta \end{pmatrix}$, $\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}$, and $\begin{pmatrix} \gamma' \\ \delta' \end{pmatrix}$ are the zero vector. So $\deg(MN)$ is not maximal iff $\begin{pmatrix} \delta \\ -\gamma \end{pmatrix}$ and $\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}$ are parallel.

We will come back to this condition later.

Note that since $\deg(M) = \deg(M^\dagger)$ the last factor of M must be the first factor of M^\dagger by the Unique Factorization Theorem. So we must only investigate $(M^\dagger)_{-m}$ to determine the last factor of M .

Using ω and M_{-m} , $(M^\dagger)_{-m} = \begin{pmatrix} \beta\delta & -\alpha\delta \\ -\beta\gamma & \alpha\gamma \end{pmatrix}$. So the first factor of $(M^\dagger)_{-m}$, which is the last factor of M , is determined in the First Factor Lemma by

$$\begin{pmatrix} x \\ y \end{pmatrix} \text{ is parallel to } \begin{pmatrix} \delta \\ -\gamma \end{pmatrix}.$$

The first factor of N is determined by

$$\begin{pmatrix} x \\ y \end{pmatrix} \text{ is parallel to } \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}.$$

So the last factor of M is the first factor of N iff $\begin{pmatrix} \delta \\ -\gamma \end{pmatrix}$ is parallel to $\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}$, which completes the proof since this is exactly the condition we found above for the degree not to be maximal.

We now generalize Lemma 5.

Lemma 6 (Degree of Product Lemma). *Let $M, N \in SU_1(2, F[z, 1/z])$ be of nonzero degrees m and n respectively. We know $\deg(MN) \leq \deg(M) + \deg(N)$. Let $q = \deg(M) + \deg(N) - \deg(MN) \geq 0$ measure the deficiency.*

Use the Unique Factorization Theorem on M and N and amalgamate the expressions for their factorizations into

$$A_1(M)^\dagger B_1(M) \cdots A_m(M)^\dagger B_m(M) A_1(N)^\dagger B_1(N) \cdots A_n(N)^\dagger B_n(N).$$

It may be that equal adjacent factors in the middle cancel in the expression, i.e., that $B_m(M) = A_1(N)$ or even also $A_m(M) = B_1(N)$ or even also $B_{m-1}(M) = A_2(N)$, etc. Count the number of such cancellations. This number will be exactly q . Furthermore, the unique factorization of the product MN will be the resulting amalgamation of the factorizations of M and N after all the equal adjacent factors are cancelled.

Proof. The case of $q = 0$ is Lemma 5.

Case $q = 1$. If we have $B_m(M) = A_1(N)$ but $A_m(M) \neq B_1(N)$, note that then $A_2(N)^\dagger B_2(N) \cdots A_n(N)^\dagger B_n(N)$ has degree exactly $n - 1$. In addition, $A_m(M)^\dagger B_1(N)$ has degree exactly 1 and their product

$$A_m(M)^\dagger B_1(N) A_2(N)^\dagger B_2(N) \cdots A_n(N)$$

has degree exactly n by Lemma 5. $B_1(N) \neq A_2(N)$ since these two elements came from the unique factorization of N . Now $A_{m-1}(M)^\dagger B_{m-1}(M)$ has degree exactly 1 and $A_{m-1}(M)^\dagger B_{m-1}(M) A_m(M)^\dagger B_1(N) \cdots A_n(N)^\dagger B_n(N)$ has degree exactly $n + 1$ by Lemma 5. Continuing this process, $\deg(MN) = \deg(M) + \deg(N) - 1$. We have now proven Lemma 6 in the case where $q = 1$.

For any q using the same method above, we see that if exactly q adjacent factors cancel out then $\deg(MN) = \deg(M) + \deg(N) - q$ and that the amalgamation expression still equal to MN has the right degree and so by the Unique Factorization Theorem must be the unique factorization of MN .

Theorem 3. $SU_1(2, F[z, 1/z])$ is a (nonabelian) free group on $\text{Factors}(F) - \{I\}$.

Proof. This theorem follows from Lemma 6.

(Recall that $\text{Factors}(F) \cap (\text{Factors}(F))^\dagger = I$.)

ACKNOWLEDGMENTS

The author is deeply indebted to Wayne Lawton whose penetrating analysis of an earlier version of the Unique Factorization Theorem led to a great simplification of the proof and strengthening of the theorem.

In addition special thanks are given to Howard L. Resnikoff, Andy Latto, David Plummer, Ned Resnikoff, and Diana Lesser.

REFERENCES

- [D1] Ingrid Daubechies, *Orthonormal bases of compactly supported wavelets*, Comm. Pure Appl. Math. **41** (1989), 909–989.
- [D2] Ingrid Daubechies and Jeffrey Lagarias, *Two-scale difference equations*. Parts I and II, Preprint, AT&T Bell Labs., 1988.
- [PS] Andrew Pressley and Graeme Segal, *Loop groups*, corrected ed., Clarendon Press, Oxford, 1988.
- [V] P. P. Vaidyanathan, et al, *Improved technique for design of perfect reconstruction FIR QMF banks with lossless polyphase matrices*, IEEE Trans. Acoust. Speech Signal Process. **37** (1989).

AWARE INCORPORATED, 124 MOUNT AUBURN STREET, CAMBRIDGE, MASSACHUSETTS 02138