Canad. Math. Bull. Vol. 59 (1), 2016 pp. 123–135
http://dx.doi.org/10.4153/CMB-2015-066-4

Discrete Space-time and Lorentz Transformations

Gerd Jensen and Christian Pommerenke

Abstract. Alfred Schild established conditions where Lorentz transformations map world-vectors (ct, x, y, z) with integer coordinates onto vectors of the same kind. The problem was dealt with in the context of tensor and spinor calculus. Due to Schild's number-theoretic arguments, the subject is also interesting when isolated from its physical background.

Schild's paper is not easy to understand. Therefore, we first present a streamlined version of his proof which is based on the use of null vectors. Then we present a purely algebraic proof that is somewhat shorter. Both proofs rely on the properties of Gaussian integers.

1 Introduction

The points of the Minkowski space-time and the Lorentz transformations are usually written in the form $\vec{X} = (t, x, y, z)^\intercal \in \mathbb{R}^4$ and $\vec{X}' = L\vec{X}$, where L is a real 4×4 matrix and $t'^2 - x'^2 - y'^2 - z'^2 = t^2 - x^2 - y^2 - z^2$. The speed of light is here assumed to be 1.

An equivalent representation is obtained by the vector space

$$\mathbb{M} := \left\{ X = \begin{pmatrix} t+z & x+\mathrm{i}y \\ x-\mathrm{i}y & t-z \end{pmatrix} : t, x, y, z \in \mathbb{R} \right\} \tag{1.1}$$

of Hermitian matrices X. They satisfy $\det X = t^2 - x^2 - y^2 - z^2$. Given such a Hermitian matrix X, write $\vec{X}$ for the associated Lorentz vector $(t, x, y, z)^\intercal$. If

$$\Gamma := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{C}, \ |\det A| = 1 \right\} \tag{1.2}$$

and $A \in \Gamma$, then $X' := AXA^*$ is again Hermitian and has a form analogous to X in (1.1) with uniquely determined t', x', y', z'. Because $\det X' = \det X$, the linear mapping

$$X' = AXA^* \tag{1.3}$$

is a Lorentz transformation. It uniquely determines a real 4×4 matrix L_A such that

$$\vec{X}' = L_A \vec{X}. \tag{1.4}$$

In [7], A. Schild found conditions that all components of L_A are integers; an equivalent formulation is that L_A maps the lattice $\mathbb{Z}^4$ onto itself. His main result is the following theorem.

Received by the editors January 19, 2014.
Published electronically October 21, 2015.
AMS subject classification: **22E43**, 20H99, 83A05.
Keywords: Lorentz transformation, integer lattice, Gaussian integers.

Theorem 1.1 (Schild) (i) *Let $A \in \Gamma$, $\det A \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$, and either*

(a) *$a, b, c, d \in \mathbb{Z} + \mathrm{i}\mathbb{Z}$ and $|a|^2 + |b|^2 + |c|^2 + |d|^2$ even or*
(b) *$a, b, c, d \in \mathbb{Z} + \mathrm{i}\mathbb{Z} + \frac{1}{2}(1 + \mathrm{i})$.*

Then L_A defined by (1.4) has integer components.

(ii) *For every $B \in \Gamma$ such that the components of L_B are integers, there is $u \in \mathbb{C}$, $|u| = 1$ such that $A := uB$ fulfills the conditions in (i).*

If $\eta \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$, and A satisfies the conditions in (i), then so does ηA. Because $\det(\eta A) = \eta^2 \det A = \pm \det A$, one can assume that $\det(\eta A) = 1$ or $\det(\eta A) = \mathrm{i}$. Therefore the conclusion $\det A \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$ in (ii) can be replaced with $\det A \in \{1, \mathrm{i}\}$. This is no loss of generality for multiplication with a suitable power of $(1 + \mathrm{i})/\sqrt{2}$ converts $A \in \Gamma$ into an element of $\mathrm{SL}(2, \mathbb{C})$.

For Schild the physical aspects were essential, so the problem was dealt with in the context of tensor and spinor calculus. However, mainly because of Schild's number theoretic arguments, the subject is also interesting when isolated from its physical background. Therefore, a streamlined presentation, which is reduced to the quintessential mathematical features, might be useful.

In the following, Schild's proof is presented using only simple matrix calculus. His method is geometrical in nature; the problem is translated to mapping properties of the spin transformations A. Additionally, a more direct, algebraic proof is given. It must be emphasized, however, that Schild's method points to aspects and problems that could hardly be found in the course of a different reasoning. Some of these, *e.g.*, the question of the equivalence of timelike vectors with integer components under Lorentz transformations with integer components, are dealt with in [7]; further, there are outlined unpublished results of H. S. M. Coxeter concerning the generators of the discrete group; see also [4].

Both proofs rest upon the unique factorization in the ring of Gaussian integers. The crucial step in revealing the structure of the transformation matrices is in each case the comparison of the factorizations of a number that is both a square and a product of two different numbers (in the proofs of Theorem 3.4 and Lemma 4.3).

At the outset, integral Lorentz matrices are defined as those elements of $\mathbb{Z}^{4\times4}$ that satisfy the 10 orthogonality conditions for the columns. Theorem 1.1 disentangles the complexity significantly and brings it down to 8 integer parameters and 2 constraints; what is more, the smaller set of parameters allows deeper insight into the group structure. Another interesting and explicit method was presented by J. D. Louck in [5], based on the biquaternionic parametrization of $\mathrm{SL}(2, \mathbb{C})$.

2 Preliminaries

2.1 Four-vectors

The connection between (1.3) and (1.4) can be made explicit by means of the Kronecker product and the vectorization of matrices ([3, Chap. 4]). For 2×2 matrices $A = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ and B, the Kronecker product $A \otimes B$ is the 4×4 block matrix $\left(\begin{smallmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{smallmatrix}\right)$, and $\operatorname{vec} A$ is the vector $(a_{11}, a_{21}, a_{12}, a_{22})^{\intercal}$ obtained by stacking the columns of A on

https://doi.org/10.4153/CMB-2015-066-4 Published online by Cambridge University Press

top of one another. If C, D, X are also 2×2 matrices, then

$$\operatorname{vec}(AXB^{\mathsf{T}}) = (B \otimes A) \operatorname{vec} X, \tag{2.1}$$

$$(A \otimes B)(C \otimes D) = AC \otimes BD, \tag{2.2}$$

$$\det(A \otimes B) = (\det A)^2 (\det B)^2. \tag{2.3}$$

The points of space-time have the equivalent representations X, $\vec{X}$, and $\operatorname{vec} X = (t+z, x-\mathrm{i}y, x+\mathrm{i}y, t-z)^{\mathsf{T}}$. The vectors $\vec{X}$ and $\operatorname{vec} X$ are connected by a unitary matrix T:

$$\frac{\operatorname{vec} X}{\sqrt{2}} = T\vec{X} \quad \text{with} \quad T := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -\mathrm{i} & 0 \\ 0 & 1 & \mathrm{i} & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}. \tag{2.4}$$

Using (2.1), relation (1.3) becomes

$$\operatorname{vec} X' = (\overline{A} \otimes A) \operatorname{vec} X,$$

and with (2.4), it follows that the matrix L_A in (1.4) has the representation

$$L_A = T^* (\overline{A} \otimes A) T. \tag{2.5}$$

From (2.5), (2.3), and (1.2) one obtains

$$\det L_A = 1 \text{ for } A \in \Gamma. \tag{2.6}$$

With (2.2) it follows from (2.5) that

$$L_{BA} = L_B L_A, \quad L_A^{-1} = L_{A^{-1}}.$$

By substituting special matrices X in (1.3), one easily shows the following lemma.

Lemma 2.1 *$L_A = L_B$ holds if and only if $B = uA$ with $u \in \mathbb{C}$, $|u| = 1$.*

From (2.5) (in its expanded form (4.3)) and (2.6) it is seen that L_A belongs to the group $\mathrm{SO}^+(1,3)$ of restricted Lorentz transformations. Actually the mapping $A \to L_A$ produces a double cover of $\mathrm{SO}^+(1,3)$ by $\mathrm{SL}(2,\mathbb{C})$ (see, for instance, [1, Sec. 6.3]), so Theorem 1.1 characterizes all members of $\mathrm{SO}^+(1,3)$ with integer components. For technical reasons, following Schild, we deal with Γ instead of $\mathrm{SL}(2,\mathbb{C})$, because this allows for a smaller number of case distinctions. Moreover, multiplication with a suitable power of $(1+\mathrm{i})/\sqrt{2}$ converts $A \in \Gamma$ into an element of $\mathrm{SL}(2,\mathbb{C})$.

2.2 Gaussian Integers

Let $\mathbb{Z}[\mathrm{i}] = \mathbb{Z} + \mathrm{i}\mathbb{Z}$ denote the ring of *Gaussian integers* and $\mathbb{E} = \{1, \mathrm{i}, -1, -\mathrm{i}\}$ its group of units. The *associates* of $x \in \mathbb{Z}[\mathrm{i}]$ are x, $\mathrm{i}x$, $-x$, and $-\mathrm{i}x$.

The prime elements of $\mathbb{Z}[\mathrm{i}]$ are called *Gaussian primes*. The Gaussian integers form a unique factorization domain ([2, Sec. 12.8]), which will be simply referred to by UFD; two factorizations of an integer are associates of each other. A natural number that is prime in $\mathbb{Z}$ is a Gaussian prime if and only if it is congruent to $-1 \pmod 4$ (see [2, Sec. 15.1]); otherwise, it is the product of two complex conjugate Gaussian primes. If the greatest common divisor of real integers $r, s, \dots$ is determined in $\mathbb{Z}$ and in $\mathbb{Z}[\mathrm{i}]$, the results are associates; the positive value will be denoted by $\gcd(r, s, \dots)$. For X as in (1.1) with $t, x, y, z \in \mathbb{Z}$, let

$$\delta(X) := \gcd(t, x, y, z). \tag{2.7}$$

Because $2 = (1+i)(1-i)$, all real Gaussian primes are odd. For $w \in \mathbb{Z}[i]$ the product $\rho(w)$ of its positive Gaussian prime factors is odd and has a factorization

$$\rho(w) = \sigma(w) r(w)^2 \tag{2.8}$$

with square-free $\sigma(w)$. All factors of $\rho(w)$ are congruent to $-1 \pmod 4$.

For $a \in \mathbb{Z}[i]$ the *parity* $\pi(a) \in \{0, 1\}$ is defined by

$$\pi(a) \equiv \operatorname{Re} a + \operatorname{Im} a \pmod 2.$$

If $\pi(a) = 0$, then a is called *even*; if $\pi(a) = 1$, then a is called *odd*. That extends the terminology for $\mathbb{Z}$, for $\operatorname{Im} a = 0$ if $a \in \mathbb{Z}$, hence $\pi(a) = 0$ for even and $\pi(a) = 1$ for odd a. Furthermore, π is a ring homomorphism $\mathbb{Z}[i] \to \mathbb{Z}_2$. The set

$$\mathbb{Z}[i]_0^2 := \{(\xi_0, \xi_1)^\intercal : \pi(\xi_0) = \pi(\xi_1)\} \tag{2.9}$$

is a submodule of the $\mathbb{Z}[i]$-module $\mathbb{Z}[i]^2$. It contains the vectors

$$e_0 := \begin{pmatrix} 1+i \\ 0 \end{pmatrix}, \quad e_1 := \begin{pmatrix} 0 \\ 1+i \end{pmatrix}, \quad e_2 := \begin{pmatrix} 1 \\ 1 \end{pmatrix}; \tag{2.10}$$

$\{e_0, e_2\}$ is a basis of $\mathbb{Z}[i]_0^2$. Each $w \in \mathbb{Z}[i]$ has a representation $w = (1+i)\widehat{w} + \varepsilon$ with uniquely determined $\widehat{w} \in \mathbb{Z}[i]$ and $\varepsilon \in \{0, 1\}$. Then $\varepsilon = \pi(w)$, hence $\pi(w) = 0$ if and only if $(1+i) \mid w$. Moreover,

$$(\xi_0, \xi_1)^\intercal \in \mathbb{Z}[i]_0^2 \iff \xi_0 = (1+i)\widehat{\xi_0} + \varepsilon, \quad \xi_1 = (1+i)\widehat{\xi_1} + \varepsilon. \tag{2.11}$$

In Theorem 1.1, the parity requirement in (a) is automatically fulfilled in (b).

Lemma 2.2 *Let $a, b, c, d \in \mathbb{Z}[i] + \frac{1}{2}(1+i)$ and $ad - bc \in \mathbb{E}$. Then $\pi(a+b+c+d) = 0$.*

Proof Write $a = a' + \frac{1}{2}(1+i)$ with $a' \in \mathbb{Z}[i]$ and likewise for b, c, d. Then

$$\begin{aligned} ad - bc &= a'd' - b'c' + \tfrac{1}{2}(1+i)(a' + d' - b' - c'), \\ a + b + c + d &= a' + b' + c' + d' + 2(1+i) \\ &= (1-i)\big(ad - bc - (a'd' - b'c')\big) + 2(b' + c') + 2(1+i). \end{aligned}$$

Since $ad - bc \in \mathbb{E}$, this is in $\mathbb{Z}[i]$ and is divisible by $1+i$, hence $\pi(a+b+c+d) = 0$. ∎

2.3 Integrity

If $X \in \mathbb{M}$ has integer components, then the components of $\vec{X}$ are integers if and only if the diagonal elements of X are both even or both odd. Let

$$\mathbb{M}_0 := \{X \in \mathbb{M} : \vec{X} \in \mathbb{Z}^4\}, \tag{2.12}$$

$$\Gamma_0 : = \{A \in \Gamma : L_A(\mathbb{Z}^4) \subset \mathbb{Z}^4\}. \tag{2.13}$$

The next lemma follows immediately from the definition (2.13).

Lemma 2.3 *L_A has integer components if and only if $A \in \Gamma_0$.*

Clearly Γ_0 is a semigroup. Because $L_{A^{-1}} = L_A^{-1}$ and (2.6), we have $A^{-1} \in \Gamma_0$ if $A \in \Gamma_0$. Hence, Γ_0 is a group.

3 Schild's Proof

The fundamental entities in this proof are null vectors (see [6, Chap. I]). They span the Minkowski space-time and can be represented by vectors in $\mathbb{C}^2$. Lorentz transformations are already determined by their action on the null vectors and correspond to linear homogeneous transformations of $\mathbb{C}^2$ (spin transformations).

3.1 Null Vectors

$X \in \mathbb{M}$ is called a *null vector* if $t^2 - x^2 - y^2 - z^2 = 0$. From $\det(AXA^*) = \det X$ for $A \in \Gamma$, we have the following lemma.

Lemma 3.1 *For $A \in \Gamma$ and X a null vector, $X' = AXA^*$ is a null vector.*

For $\xi \in \mathbb{C}^2$,

$$\xi\xi^* = \begin{pmatrix} \xi_0 \\ \xi_1 \end{pmatrix} \begin{pmatrix} \overline{\xi}_0 & \overline{\xi}_1 \end{pmatrix} = \begin{pmatrix} \xi_0\overline{\xi}_0 & \xi_0\overline{\xi}_1 \\ \xi_1\overline{\xi}_0 & \xi_1\overline{\xi}_1 \end{pmatrix} \tag{3.1}$$

is a null vector. If X is *future-pointing* ($t \geq 0$), the converse also holds.

Lemma 3.2 *A future-pointing null vector X has the form (3.1), and $\widehat{\xi}\widehat{\xi}^* = \xi\xi^*$ holds if and only if there is $u \in \mathbb{C}$ with $|u| = 1$ and $\widehat{\xi} = u\xi$.*

Proof If $t > |z|$, then $X = \xi\xi^*$ with $\xi_0 = \sqrt{t+z}$ and $\xi_1 = (x - \mathrm{i}y)/\sqrt{t+z}$; if $t^2 = z^2$, then $x = y = 0$ and $X = \xi\xi^*$ with $\xi_0 = \sqrt{t+z}$ and $\xi_1 = \sqrt{t-z}$. The simple proof of the second assertion is omitted. ∎

Definition 3.3 Let $\mathbb{V}_0$ be the set of future-pointing null vectors in $\mathbb{M}_0$ (see (2.12)), *i.e.*,

$$\mathbb{V}_0 := \{X \in \mathbb{M}_0 : t^2 - x^2 - y^2 - z^2 = 0,\ t \geq 0\}.$$

If $\xi \in \mathbb{Z}[\mathrm{i}]^2$, then

$$\xi\xi^* \in \mathbb{M}_0 \iff \xi \in \mathbb{Z}[\mathrm{i}]_0^2.$$

Theorem 3.4 (i) *If $\xi \in \mathbb{Z}[\mathrm{i}]_0^2$ and $r \in \mathbb{N}$, then $r\xi\xi^* \in \mathbb{V}_0$.*
(ii) *Conversely, for each $X \in \mathbb{V}_0$ there is $\xi \in \mathbb{Z}[\mathrm{i}]_0^2$ such that*

$$X = s\xi\xi^* \tag{3.2}$$

and s is a square-free product of positive Gaussian primes. Then ξ is uniquely determined up to a factor $u \in \mathbb{C}$ with $|u| = 1$. Further, $s = \sigma(\delta(X))$ (with δ and σ as defined in (2.7) and (2.8)).

https://doi.org/10.4153/CMB-2015-066-4 Published online by Cambridge University Press

Proof (i) is trivial. (ii) is proved in three steps.

1. We suppose at first that $\delta(X) = 1$. Let $\rho(t+z) = \sigma r^2$ and $\rho(t-z) = \sigma' r'^2$ be the factorizations according to (2.8). Then

$$\rho\big((t+z)(t-z)\big) = \sigma\sigma' r^2 r'^2.$$

From UFD, it follows that $\rho(x+\mathrm{i}y) = \rho(x-\mathrm{i}y)$, and because

$$(t+z)(t-z) = (x+\mathrm{i}y)(x-\mathrm{i}y), \tag{3.3}$$

we must have

$$\sigma\sigma' r^2 r'^2 = \rho\big((t+z)(t-z)\big) = \rho(x+\mathrm{i}y)^2.$$

As a consequence of UFD it follows that $\sigma' = \sigma$ and $\sigma r r' \mid (x+\mathrm{i}y)$. Furthermore, $\sigma r r' \mid (x-\mathrm{i}y)$, so $\sigma r r' \mid 2x$ and $\sigma r r' \mid 2y$. Now σ is odd, so $\sigma \mid x$ and $\sigma \mid y$. From $\sigma \mid t+z$ and $\sigma \mid t-z$ it follows that $\sigma \mid 2t$ and $\sigma \mid 2z$, hence $\sigma \mid t$ and $\sigma \mid z$. But then $\sigma = 1$, since $\delta(X) = 1$.

The non-real prime factors of $t+z$ and of $t-z$ form pairs $(\zeta_j, \overline{\zeta}_j)$ and $(\zeta'_k, \overline{\zeta}'_k)$ of complex conjugate numbers. With $\zeta = \prod_j \zeta_j$ and $\zeta' = \prod_k \zeta'_k$ then

$$t+z = r^2\zeta\overline{\zeta} = (r\zeta)\overline{(r\zeta)} \quad \text{and} \quad t-z = r'^2\zeta'\overline{\zeta'} = (r'\zeta')\overline{(r'\zeta')}.$$

From (3.3) and UFD, we may suppose that $\zeta_j \mid (x+\mathrm{i}y)$, $\zeta'_k \mid (x+\mathrm{i}y)$ and $\overline{\zeta}_j \mid (x-\mathrm{i}y)$, $\overline{\zeta}'_k \mid (x-\mathrm{i}y)$. From (3.3) follows further that $\rho(x+\mathrm{i}y) = \rho(x-\mathrm{i}y) = rr'$. Then $x+\mathrm{i}y = u(r\zeta)(r'\zeta')$ and $x-\mathrm{i}y = \overline{u(r\zeta)(r'\zeta')}$, where u is a unit of $\mathbb{Z}[\mathrm{i}]$. Since $\delta(X) = 1$ and therefore $s = \sigma(\delta(X)) = 1$, (3.2) holds with $\xi := (ru\zeta, r'\zeta')^\intercal$. From $\pi(ru\zeta) = \pi(r^2\zeta\overline{\zeta}) = \pi(t+z) = \pi(t-z) = \pi(r'^2\zeta'\overline{\zeta'}) = \pi(r'\zeta')$, it follows that $\xi \in \mathbb{Z}[\mathrm{i}]_0^2$.

2. Now let $X \in \mathbb{V}_0$ be arbitrary and $d = \delta(X)$, hence $\delta(X/d) = 1$. Therefore, $X/d = \xi\xi^*$ for suitable $\xi = (\xi_0, \xi_1)^\intercal \in \mathbb{Z}[\mathrm{i}]_0^2$. If $\rho(d) = \sigma(d) r^2$ then $X = \sigma(d) r\xi(r\xi)^*$.

3. Suppose also that $X = s_1\xi_1\xi_1^*$ with a square-free product s_1 of positive Gaussian primes. Since the highest power of a positive Gaussian prime that divides all components of $\xi\xi^*$ or all components of $\xi_1\xi_1^*$ is even, it must be $s_1 = s$. Now the uniqueness assertion follows from Lemma 3.2. ∎

Theorem 3.5 *$A \in \Gamma_0$ if and only if $L_A(\vec{\mathbb{V}}_0) \subset \vec{\mathbb{V}}_0$ and $L_A^{-1}(\vec{\mathbb{V}}_0) \subset \vec{\mathbb{V}}_0$.*

Proof If $A \in \Gamma_0$, then $L_A(\vec{\mathbb{V}}_0) \subset \vec{\mathbb{V}}_0$ and $L_A^{-1}(\vec{\mathbb{V}}_0) \subset \vec{\mathbb{V}}_0$ by (2.13) and Lemma 3.1. For the converse we show that L_A maps a basis of $\mathbb{Z}^4$ into $\mathbb{Z}^4$.

Now $\vec{X}_0 := (1,-1,0,0)^\intercal$, $\vec{X}_1 := (1,1,0,0)^\intercal$, $\vec{X}_2 := (1,0,1,0)^\intercal$, and $\vec{X}_3 := (1,0,0,1)^\intercal$ belong to $\mathbb{V}_0$. For $i = 0,1,2,3$ at least one component of $(t_i, x_i, y_i, z_i)^\intercal := L_A(\vec{X}_i)$ must be odd, for otherwise $\vec{X}_i = 2L_A^{-1}(L_A(\vec{X}_i)/2) \in 2\mathbb{Z}^4$ by hypothesis, which is wrong. Since the square of a real integer leaves a remainder of 1 or 0 on division by 4, it follows from $t_i^2 = x_i^2 + y_i^2 + z_i^2$ that t_i and exactly one of x_i, y_i, z_i are odd.

Because of the invariance of the bilinear form associated with $t^2 - x^2 - y^2 - z^2$, it follows that $t_0t_1 - x_0x_1 - y_0y_1 - z_0z_1 = 2$. Since t_0t_1 is odd, at least one of x_0x_1, y_0y_1, z_0z_1, say x_0x_1, is odd. Then t_0, t_1, x_0, x_1 are odd and y_0, y_1, z_0, z_1 must be even. Hence, $t_0 + t_1$, $x_0 + x_1$, $y_0 + y_1$ and $z_0 + z_1$ are all even, and

$$L_A(1,0,0,0) = L_A\Big(\frac{1}{2}(\vec{X}_0 + \vec{X}_1)\Big) = \frac{1}{2}\Big(L_A(\vec{X}_0) + L_A(\vec{X}_1)\Big) \in \mathbb{Z}^4.$$

Then

$$L_A(0,1,0,0) = L_A(\vec{X}_1) - L_A(1,0,0,0),$$
$$L_A(0,0,1,0) = L_A(\vec{X}_2) - L_A(1,0,0,0),$$
$$L_A(0,0,0,1) = L_A(\vec{X}_3) - L_A(1,0,0,0)$$

are also in $\mathbb{Z}^4$. ∎

3.2 Reformulation of the Problem

Definition 3.6 Let $\Delta_0 := \{ A \in \Gamma : A(\mathbb{Z}[\mathrm{i}]_0^2) \subset \mathbb{Z}[\mathrm{i}]_0^2,\ A^{-1}(\mathbb{Z}[\mathrm{i}]_0^2) \subset \mathbb{Z}[\mathrm{i}]_0^2 \}$, where $\mathbb{Z}[\mathrm{i}]_0^2$ is defined in (2.9).

Theorem 3.7 *$\Delta_0 \subset \Gamma_0$. Conversely, for $B \in \Gamma_0$ there is $u \in \mathbb{C}$ with $|u| = 1$ and $uB \in \Delta_0$.*

Proof Let $A \in \Delta_0$ and $X \in \mathbb{V}_0$. By Theorem 3.4(ii) there exists $\xi \in \mathbb{Z}[\mathrm{i}]_0^2$ such that $X = \sigma(\delta(X))\xi\xi^*$ and

$$X' = AXA^* = \sigma(\delta(X))A(\xi\xi^*)A^* = \sigma(\delta(X))(A\xi)(A\xi)^*.$$

Since $A\xi \in \mathbb{Z}[\mathrm{i}]_0^2$ by hypothesis, this implies by Theorem 3.4(i) that $AXA^* \in \mathbb{V}_0$. Similarly, $A^{-1}X(A^{-1})^* \in \mathbb{V}_0$. Hence, $A \in \Gamma_0$ by Theorem 3.5.

The converse is proved in three steps.

1. At first it is shown that for each $\xi \in \mathbb{Z}[\mathrm{i}]_0^2$ there is $u \in \mathbb{C}$ with $|u| = 1$ and

$$uB\xi \in \mathbb{Z}[\mathrm{i}]_0^2. \tag{3.4}$$

Let $X := \xi\xi^*$. Then $X \in \mathbb{V}_0$, so $X' := L_B(X) \in \mathbb{V}_0$ by Theorem 3.5. From

$$X' = B(\xi\xi^*)B^* = (B\xi)(B\xi)^* \tag{3.5}$$

and Theorem 3.4(ii), it follows that $\sigma(\delta(X)) = 1$ and that there is $\eta \in \mathbb{Z}[\mathrm{i}]_0^2$ such that

$$X' = \sigma(\delta(X'))\eta\eta^*. \tag{3.6}$$

Since L_B and L_B^{-1} have integer components, we see that $\delta(X') = \delta(X)$, and therefore $\sigma(\delta(X')) = \sigma(\delta(X)) = 1$. Now (3.4) follows from (3.5), (3.6), and Lemma 3.2.

2. Next we show that u can be chosen independent of ξ, *i.e.*, $uB(\mathbb{Z}[\mathrm{i}]_0^2) \subset \mathbb{Z}[\mathrm{i}]_0^2$. For the vectors e_0 and e_2 (see (2.10)) there exist, by step 1, $u_0, u_1 \in \mathbb{C}$ such that

$$u_0Be_0 = e_0' \in \mathbb{Z}[\mathrm{i}]_0^2, \qquad u_1Be_2 = e_2' \in \mathbb{Z}[\mathrm{i}]_0^2 \tag{3.7}$$

and $|u_0| = |u_1| = 1$. Then

$$u_0e_0 + u_1e_2 = B^{-1}(e_0' + e_2').$$

Since $B^{-1} \in \Gamma_0$, there is, by step 1, $u \in \mathbb{C}$ with $|u| = 1$ and $\overline{u}(u_0e_0 + u_1e_2) \in \mathbb{Z}[\mathrm{i}]_0^2$. Hence, there are $p, q \in \mathbb{Z}[\mathrm{i}]$ with $\pi(p) = \pi(q)$ and

$$(1+\mathrm{i})\overline{u}u_0 + \overline{u}u_1 = p, \quad \overline{u}u_1 = q.$$

So $\overline{u}u_1 \in \mathbb{Z}[\mathrm{i}]$ and $\overline{u}u_0 = \frac{1}{2}(1-\mathrm{i})(p-q) \in \mathbb{Z}[\mathrm{i}]$, the latter because of $\pi(p-q) = 0$. This is only possible if $\overline{u}u_0, \overline{u}u_1 \in \mathbb{E}$. From (3.7) it now follows that $uBe_0 = u\overline{u}_0e_0' \in \mathbb{Z}[\mathrm{i}]_0^2$

https://doi.org/10.4153/CMB-2015-066-4 Published online by Cambridge University Press

and $uBe_2 = u\overline{u}_1 e_2' \in \mathbb{Z}[\mathrm{i}]_0^2$. Since e_0 and e_2 are a basis of $\mathbb{Z}[\mathrm{i}]_0^2$, we have $uB(\mathbb{Z}[\mathrm{i}]_0^2) \subset \mathbb{Z}[\mathrm{i}]_0^2$.

3. Likewise there is $v \in \mathbb{C}$ with $|v| = 1$ and $vB^{-1}(\mathbb{Z}[\mathrm{i}]_0^2) \subset \mathbb{Z}[\mathrm{i}]_0^2$. From

$$uv(\mathbb{Z}[\mathrm{i}]_0^2) = uB(vB^{-1}(\mathbb{Z}[\mathrm{i}]_0^2)) \subset uB(\mathbb{Z}[\mathrm{i}]_0^2) \subset \mathbb{Z}[\mathrm{i}]_0^2$$

it follows that $uve_2 \in \mathbb{Z}[\mathrm{i}]_0^2$, hence $uv \in \mathbb{E}$ and

$$u^{-1}B^{-1}(\mathbb{Z}[\mathrm{i}]_0^2) = (uv)^{-1}vB^{-1}(\mathbb{Z}[\mathrm{i}]_0^2) \subset \mathbb{Z}[\mathrm{i}]_0^2. \qquad \blacksquare$$

Theorem 3.7 shows that Δ_0 is big enough to substantially represent all elements of Γ_0. The matrices L_A with integer components can therefore be characterized by mapping properties of the matrices $A \in \Delta_0$. It follows immediately from the definition that Δ_0 is a group. Further properties are given in the following lemma.

Lemma 3.8 *If $A \in \Delta_0$, then*

(i) $\det A \in \mathbb{E}$,

(ii) $uA \in \Delta_0$ *if and only if* $u \in \mathbb{E}$.

Proof (i) The columns of $M := A\begin{pmatrix} 1+\mathrm{i} & 1 \\ 0 & 1 \end{pmatrix}$ are in $\mathbb{Z}[\mathrm{i}]_0^2$, hence $(1+\mathrm{i})\det A = \det M \in \mathbb{Z}[\mathrm{i}]$. From $|\det M|^2 = 2$, it follows that $\det M \in (1+\mathrm{i})\mathbb{E}$, so $(1+\mathrm{i})\det A \in (1+\mathrm{i})\mathbb{E}$.

(ii) If $u \in \mathbb{E}$, then clearly $uA \in \Delta_0$. Conversely, let $uA \in \Delta_0$. Then $A^{-1}e_2 \in \mathbb{Z}[\mathrm{i}]_0^2$, hence $ue_2 = uA(A^{-1}e_2) \in \mathbb{Z}[\mathrm{i}]_0^2$ and therefore $u \in \mathbb{E}$. $\blacksquare$

The lemma shows that each L_B, $B \in \Gamma_0$, can be represented by exactly four matrices in Δ_0: $A = uB$, $\mathrm{i}A$, $-A$, and $-\mathrm{i}A$; then $L_B = L_A = L_{\mathrm{i}A} = L_{-A} = L_{-\mathrm{i}A}$.

3.3 Proof of Theorem 1.1(i)

In case (a) both components of Ae_0 are even (see Section 2.2). Because $\det A \in \mathbb{E}$, the same holds for $A^{-1}e_0$. Therefore, $Ae_0, A^{-1}e_0 \in \mathbb{Z}[\mathrm{i}]_0^2$.

In case (b) both components of Ae_0 and of $A^{-1}e_0$ are odd. Therefore $Ae_0, A^{-1}e_0 \in \mathbb{Z}[\mathrm{i}]_0^2$ in this case , too.

In both cases the sum of the components of Ae_2 is $a+b+c+d$, and $\pi(a+b+c+d) = 0$ (see Lemma 2.2 in case (b)), so both components of Ae_2 have the same parity, hence $Ae_2 \in \mathbb{Z}[\mathrm{i}]_0^2$. The sum of the components of $A^{-1}e_2$ is in both cases $(d-b-c+a)/\det A = (a+b+c+d)/\det A - 2(b+c)/\det A$; since in both cases $b+c \in \mathbb{Z}[\mathrm{i}]$ and $\det A \in \mathbb{E}$, this expression is in $\mathbb{Z}[\mathrm{i}]$ and has parity 0. Therefore, $A^{-1}e_2 \in \mathbb{Z}[\mathrm{i}]_0^2$. Since $\{e_0, e_2\}$ is a basis of $\mathbb{Z}[\mathrm{i}]_0^2$, it follows that $A \in \Delta_0$. The assertion now follows from the first statement in Theorem 3.7. $\blacksquare$

3.4 Proof of Theorem 1.1(ii)

By Lemma 2.3 the hypothesis stands for $B \in \Gamma_0$. By Theorem 3.7 there is u such that $A := uB \in \Delta_0$. Let e_0, e_1, e_2 be the $\mathbb{Z}[\mathrm{i}]_0^2$-vectors from (2.10). Then we have $Ae_0, Ae_1, Ae_2 \in \mathbb{Z}[\mathrm{i}]_0^2$, since $A \in \Delta_0$. According to (2.11), $Ae_0 \in \mathbb{Z}[\mathrm{i}]_0^2$ and $Ae_1 \in \mathbb{Z}[\mathrm{i}]_0^2$

mean that

$$(1+\mathrm{i})a = (1+\mathrm{i})\widehat{a} + \varepsilon, \quad (1+\mathrm{i})c = (1+\mathrm{i})\widehat{c} + \varepsilon, \tag{3.8a}$$

$$(1+\mathrm{i})b = (1+\mathrm{i})\widehat{b} + \varepsilon', \quad (1+\mathrm{i})d = (1+\mathrm{i})\widehat{d} + \varepsilon' \tag{3.8b}$$

with $\widehat{a}, \widehat{c}, \widehat{b}, \widehat{d} \in \mathbb{Z}[\mathrm{i}]$ and $\varepsilon, \varepsilon' \in \{0,1\}$. Further, $Ae_2 \in \mathbb{Z}[\mathrm{i}]_0^2$ means that

$$a + b = (1+\mathrm{i})g_1 + \varepsilon'', \tag{3.9}$$

$$c + d = (1+\mathrm{i})g_2 + \varepsilon'' \tag{3.10}$$

with $g_1, g_2 \in \mathbb{Z}[\mathrm{i}]$ and $\varepsilon'' \in \{0,1\}$. From (3.9) and (3.8a), it follows that

$$(1+\mathrm{i})b = (1+\mathrm{i})\big((1+\mathrm{i})g_1 + \varepsilon'' - \widehat{a} - (1-\mathrm{i})\varepsilon\big) + \varepsilon,$$

and comparing that with (3.8b), one obtains $\varepsilon = \varepsilon'$. Furthermore, addition of (3.9) and (3.10) shows that $\pi(a+b+c+d) = 0$. Finally, we note that $\det A \in \mathbb{E}$ by Lemma 3.8(i).

If $\varepsilon = 0$, then $a, b, c, d \in \mathbb{Z}[\mathrm{i}]$ and all requirements in (a) hold. If $\varepsilon = 1$, then (3.8a) means that $a = \widehat{a} + \frac{1}{1+\mathrm{i}} = (\widehat{a} - \mathrm{i}) + \frac{1+\mathrm{i}}{2}$, and likewise for the other relations (3.8). Hence, all requirements of (b) are satisfied. ∎

4 Alternative Proof

4.1 Reformulation of the Problem

At the outset, the condition that the components of L_A are integers is expressed through the components of A.

Lemma 4.1 *Let $A \in \Gamma$. Then $A \in \Gamma_0$ if and only if*

$$a_1\overline{a}_2 \pm a_3\overline{a}_4 \in \mathbb{Z}[\mathrm{i}] \tag{4.1}$$

for all permutations (a_1, a_2, a_3, a_4) of (a, b, c, d), and

$$\pm|a|^2 \pm |b|^2 \pm |c|^2 \pm |d|^2 \in 2\mathbb{Z} \tag{4.2}$$

whenever the number of plus signs is even.

Proof It is $A \in \Gamma_0$ if and only if the components of L_A are integers. We need (2.5) to be expanded at full length:

$$L_A = \begin{pmatrix} \frac{1}{2}(|a|^2+|b|^2+|c|^2+|d|^2) & \mathrm{Re}(a\overline{b}+c\overline{d}) & -\mathrm{Im}(a\overline{b}+c\overline{d}) & \frac{1}{2}(|a|^2-|b|^2+|c|^2-|d|^2) \\ \mathrm{Re}(a\overline{c}+b\overline{d}) & \mathrm{Re}(a\overline{d}+b\overline{c}) & -\mathrm{Im}(a\overline{d}-b\overline{c}) & \mathrm{Re}(a\overline{c}-b\overline{d}) \\ \mathrm{Im}(a\overline{c}+b\overline{d}) & \mathrm{Im}(a\overline{d}+b\overline{c}) & \mathrm{Re}(a\overline{d}-b\overline{c}) & \mathrm{Im}(a\overline{c}-b\overline{d}) \\ \frac{1}{2}(|a|^2+|b|^2-|c|^2-|d|^2) & \mathrm{Re}(a\overline{b}-c\overline{d}) & -\mathrm{Im}(a\overline{b}-c\overline{d}) & \frac{1}{2}(|a|^2-|b|^2-|c|^2+|d|^2) \end{pmatrix}. \tag{4.3}$$

Obviously (4.1) and (4.2) are sufficient for $A \in \Gamma_0$. Conversely, if L_A has integer components, then from (4.3) one obtains (4.2) and $a\overline{b} \pm c\overline{d}$, $a\overline{c} \pm b\overline{d}$, $a\overline{d} \pm b\overline{c} \in \mathbb{Z}[\mathrm{i}]$. From $a\overline{b} + c\overline{d} = g$ and $a\overline{b} - c\overline{d} = p$ with $g, p \in \mathbb{Z}[\mathrm{i}]$ follows that $2c\overline{d} = g - p$ and $2c\overline{d} - 2d\overline{c} = g - p - (\overline{g} - \overline{p}) = 2\mathrm{i}\,\mathrm{Im}(g-p) \in 2\mathbb{Z}[\mathrm{i}]$, so $c\overline{d} - d\overline{c} \in \mathbb{Z}[\mathrm{i}]$, hence

https://doi.org/10.4153/CMB-2015-066-4 Published online by Cambridge University Press

$a\overline{b} \pm d\overline{c} \in \mathbb{Z}[\mathrm{i}]$. Similarly, $a\overline{c} \pm d\overline{b} \in \mathbb{Z}[\mathrm{i}]$ and $a\overline{d} \pm c\overline{b} \in \mathbb{Z}[\mathrm{i}]$. This proves (4.1) for all permutations with first term a. By forming complex conjugates and negatives, one obtains all other expressions (4.1). ∎

4.2 Proof of Theorem 1.1 (i)

If (a) holds, (4.1) and (4.2) are obvious. In case (b),

$$(1+\mathrm{i})a = (1+\mathrm{i})a' + 1 \qquad (a' \in \mathbb{Z}[\mathrm{i}]) \tag{4.4}$$

and likewise for b, c, d. It follows that

$$2\mathrm{i}[(ad-bc)-(a'd'-b'c')] = (1+\mathrm{i})(a'-c'-b'+d').$$

Because $\det A \in \mathbb{E}$, this implies that all expressions $(1+\mathrm{i})(\pm a' \pm b' \pm c' \pm d')$ are divisible by 2, the signs being arbitrary. From (4.4) and the analogs for b, c, d it follows that

$$a\overline{b} = \tfrac{1}{2}[(1+\mathrm{i})a'+1][(1-\mathrm{i})\overline{b}'+1] = a'\overline{b}' + \tfrac{1}{2}((1+\mathrm{i})a' + (1-\mathrm{i})\overline{b}'+1),$$
$$c\overline{d} = \tfrac{1}{2}[(1+\mathrm{i})c'+1][(1-\mathrm{i})\overline{d}'+1] = c'\overline{d}' + \tfrac{1}{2}((1+\mathrm{i})c' + (1-\mathrm{i})\overline{d}'+1),$$

$$\begin{aligned} a\overline{b} \pm c\overline{d} &= a'\overline{b}' \pm c'\overline{d}' + \tfrac{1}{2}(1+\mathrm{i})(a' \pm c') + \tfrac{1}{2}(1-\mathrm{i})(b' \pm d') + \tfrac{1}{2}(1\pm 1), \\ &= a'\overline{b}' \pm c'\overline{d}' + \tfrac{1}{2}(1+\mathrm{i})(a' \pm c' + b' \pm d') - \mathrm{i}(b' \pm d') + \tfrac{1}{2}(1\pm 1). \end{aligned}$$

All terms on the right are in $\mathbb{Z}[\mathrm{i}]$. Likewise, all other relations (4.1) are obtained.

Now let $\alpha, \beta, \gamma, \delta \in \mathbb{E}$ and $\alpha+\beta+\gamma+\delta$ divisible by 2. From (4.4) follows that

$$\begin{aligned} &(1+\mathrm{i})(\alpha a + \beta b + \gamma c + \delta d) \\ &\quad = (1+\mathrm{i})(\alpha a' + \beta b' + \gamma c' + \delta d') + \alpha+\beta+\gamma+\delta \\ &\quad = (1+\mathrm{i})\big((\alpha-1)a' + (\beta-1)b' + (\gamma-1)c' + (\delta-1)d' + (a'+b'+c'+d')\big) \\ &\qquad + \alpha+\beta+\gamma+\delta. \end{aligned}$$

Then

$$2 \mid (1+\mathrm{i})(\alpha a + \beta b + \gamma c + \delta d)$$

since $1+\mathrm{i} \mid \alpha-1, 1+\mathrm{i} \mid \beta-1, 1+\mathrm{i} \mid \gamma-1, 1+\mathrm{i} \mid \delta-1$ and $2 \mid (1+\mathrm{i})(a'+b'+c'+d')$. Hence,

$$\begin{aligned} &(\alpha a + \beta b + \gamma c + \delta d)(\alpha\overline{a} + \beta\overline{b} + \gamma\overline{c} + \delta\overline{d}) \\ &\quad = \alpha^2|a|^2 + \beta^2|b|^2 + \gamma^2|c|^2 + \delta^2|d|^2 + \big[\alpha\beta \operatorname{Re}(2a\overline{b}) + \gamma\delta \operatorname{Re}(2c\overline{d})\big] \\ &\qquad + \big[\alpha\gamma \operatorname{Re}(2a\overline{c}) + \beta\delta \operatorname{Re}(2b\overline{d})\big] + \big[\alpha\delta \operatorname{Re}(2a\overline{d}) + \beta\gamma \operatorname{Re}(2b\overline{c})\big] \end{aligned}$$

is divisible by 2. If $(\alpha, \beta, \gamma, \delta)$ is one of the four combinations $(1,1,1,1)$, $(1,1,\mathrm{i},\mathrm{i})$, $(1,\mathrm{i},1,\mathrm{i})$, or $(1,\mathrm{i},\mathrm{i},1)$, then $\alpha+\beta+\gamma+\delta$ is divisible by 2 and $\alpha\beta = \gamma\delta$ or $\alpha\beta = -\gamma\delta$, $\alpha\gamma = \beta\delta$ or $\alpha\gamma = -\beta\delta$ and $\alpha\delta = \beta\gamma$ or $\alpha\delta = -\beta\gamma$. Using (4.1), it is seen that the expressions in brackets are all divisible by 2. This proves (4.2). ∎

https://doi.org/10.4153/CMB-2015-066-4 Published online by Cambridge University Press

4.3 Proof of Theorem 1.1(ii)

Lemmas 4.2 and 4.3 are intermediate steps.

Lemma 4.2 *Let $A \in \Gamma_0$. Then $2v_1\overline{v}_2 \in \mathbb{Z}[\mathrm{i}]$ for all $v_1, v_2 \in \{a, b, c, d\}$. If in addition $\det A \in \mathbb{E}$, then $2v_1v_2 \in \mathbb{Z}[\mathrm{i}]$ for all $v_1, v_2 \in \{a, b, c, d\}$.*

Proof The first assertion follows from (4.1) and (4.2). For $t = 1$ and $x = y = z = 0$ we have $X = I$. The components of X' are integers by hypothesis. From (1.3), it follows that $X' = AA^*$ and $X'(A^*)^{-1}2v = 2Av$. By the first part of the lemma, for $v \in \{a, b, c, d\}$, all components on the left side of this equation, and hence all components of $2Av$, are in $\mathbb{Z}[\mathrm{i}]$. ∎

Because UFD, each $w \in \mathbb{Z}[\mathrm{i}]$ has a unique factorization

$$w = \varepsilon(1+\mathrm{i})^j g^2 \gamma \tag{4.5}$$

with the following properties: $\varepsilon \in \mathbb{E}$, $0 \le j \in \mathbb{Z}$, g and γ are odd and γ is square-free.

Lemma 4.3 *If $A \in \Gamma_0$ and $\det A \in \mathbb{E}$, then all components of A have the form*

$$v = \tfrac{1}{2}(1+\mathrm{i})^{k+1} h \tag{4.6}$$

or all have the form

$$v = \tfrac{1}{2}\sqrt{2}(1+\mathrm{i})^{k} h \tag{4.7}$$

with $0 \le k \in \mathbb{Z}$ and odd $h \in \mathbb{Z}[\mathrm{i}]$.

Proof Let $v_1, v_2 \in \{a, b, c, d, \overline{a}, \overline{b}, \overline{c}, \overline{d}\}$. Then $2v_1^2, 2v_2^2, 2v_1v_2 \in \mathbb{Z}[\mathrm{i}]$ by Lemma 4.2, and therefore according to (4.5),

$$2v_1^2 = \varepsilon_1(1+\mathrm{i})^{j_1} g_1^2 \gamma_1, \tag{4.8}$$

$$2v_2^2 = \varepsilon_2(1+\mathrm{i})^{j_2} g_2^2 \gamma_2, \tag{4.9}$$

$$2v_1v_2 = \varepsilon_3(1+\mathrm{i})^{j_3} g_3^2 \gamma_3. \tag{4.10}$$

Multiplication of (4.8) by (4.9) gives on the one hand

$$4v_1^2v_2^2 = \varepsilon_1\varepsilon_2(1+\mathrm{i})^{j_1+j_2}(g_1g_2)^2\gamma_1\gamma_2, \tag{4.11}$$

and squaring (4.10) on the other hand

$$4v_1^2v_2^2 = \varepsilon_3^2(1+\mathrm{i})^{2j_3}(g_3^2\gamma_3)^2. \tag{4.12}$$

From the uniqueness of the factorization (4.5) follows that $\gamma_1 = \gamma_2$, since comparison of (4.11) with (4.12) shows that $\gamma_1\gamma_2$ has solely double prime factors. One concludes that the factor γ in $2v^2 = \varepsilon(1+\mathrm{i})^j g^2\gamma$ is the same for all $v \in \{a, b, c, d, \overline{a}, \overline{b}, \overline{c}, \overline{d}\}$. From

$$2v^2 = \varepsilon(1+\mathrm{i})^j g^2 \gamma, \tag{4.13}$$

$$2\overline{v}^2 = \overline{\varepsilon}(1-\mathrm{i})^j \overline{g}^2 \overline{\gamma} = [\overline{\varepsilon}(-\mathrm{i})^j](1+\mathrm{i})^j \overline{g}^2 \overline{\gamma}, \tag{4.14}$$

it now follows that $\overline{\gamma} = \gamma$, so all prime factors of γ are real. Hence, $\gamma = 1$ or $\gamma \ge 3$.

https://doi.org/10.4153/CMB-2015-066-4 Published online by Cambridge University Press

From the comparison of (4.11) with (4.12), it follows that $\varepsilon_1^2\varepsilon_2^2 = \varepsilon_3^4 = 1$, so

$$\varepsilon_1\varepsilon_2 = \pm 1, \tag{4.15}$$

and that $j_1 + j_2 = 2j_3$. Applied to (4.11), this gives $2v_1v_2 = \eta(1+\mathrm{i})^{j_3}g_1g_2\gamma$ with $\eta \in \mathbb{E}$. Therefore, $\gamma \mid 2v_1v_2$ for all v_1, v_2; in particular, $\gamma \mid 2(ad - bc)$. But this implies $\gamma \le 2$, so $\gamma = 1$. Therefore, all $v \in \{a, b, c, d, \overline{a}, \overline{b}, \overline{c}, \overline{d}\}$ have a representation

$$2v^2 = \varepsilon(1+\mathrm{i})^j g^2. \tag{4.16}$$

If (4.15) is applied to (4.13) and (4.14), it follows that $\varepsilon\overline{\varepsilon}(-\mathrm{i})^j = (-\mathrm{i})^j = \pm 1$, so all j are even, $j = 2k$. As another consequence of (4.15), the set of factors ε in the representations (4.16) of $\{a, b, c, d, \overline{a}, \overline{b}, \overline{c}, \overline{d}\}$ is either

$$\{-1, 1\} = \{\eta^2 : \eta \in \mathbb{E}\} \quad \text{or} \quad \{-\mathrm{i}, \mathrm{i}\} = \Big\{\big(\tfrac{1}{2}\eta\sqrt{2}\big)^2 : \eta \in \mathbb{E}\Big\}.$$

Having the factors ε written as squares we can extract square roots in (4.16) and obtain (4.7) or (4.6). In each case, $h = \eta g$ is odd. ■

After these preparations the proof can be carried out. Let $B \in \Gamma_0$. We choose $\widehat{u}$ with $|\widehat{u}| = 1$ such that $\det(\widehat{u}B) = 1$ and set $\widehat{A} := \widehat{u}B$. By Lemma 4.3 the components of $\widehat{A}$ have the form (4.6) or (4.7). In the first case let $A := \widehat{A}$ and $u := \widehat{u}$; then the components of A satisfy (4.6) and we have $\det A = 1$. In the second case let

$$A := \frac{1}{\sqrt{2}}(1+\mathrm{i})\widehat{A} \quad \text{and} \quad u := \frac{1}{\sqrt{2}}(1+\mathrm{i})\widehat{u};$$

then the components of A also satisfy (4.6) and it is $\det A = \mathrm{i}$. In both cases we have $A = uB$ with $|u| = 1$, $\det A \in \mathbb{E}$, and the components of A have the form $v_j = \frac{1}{2}(1+\mathrm{i})^{k_j+1}h_j$ ($j = 1, 2, 3, 4$).

If $k_j \ge 1$, then $v_j \in \mathbb{Z}[\mathrm{i}]$. If $k_j = 0$, then $v_j = \frac{1}{2}(1+\mathrm{i})h_j$ with odd $\mathrm{i}h_j = (1+\mathrm{i})h'_j + 1$ ($h'_j \in \mathbb{Z}[\mathrm{i}]$), hence $v_j = h'_j + \frac{1}{2}(1-\mathrm{i})$ and $|v_j|^2 = \frac{1}{2}|h_j|^2 = q_j + \frac{1}{2}$ with $q_j \in \mathbb{Z}$.

As a consequence of (4.2) we conclude that the number of indices j with $k_j = 0$ is even. Hence there are three cases to consider.

(i) $k_j \ge 1$ for all j. Then all components of A are in $\mathbb{Z}[\mathrm{i}]$. Since $\det A \in \mathbb{E}$ and $|a|^2 + |b|^2 + |c|^2 + |d|^2$ is even according to (4.2), case (a) is present.

(ii) $k_j = 0$ for exactly two indices j. Assume that $k_1 = k_2 = 0$. Then $k_3 \ge 1$, $k_4 \ge 1$, so $v_3, v_4 \in \mathbb{Z}[\mathrm{i}]$. Since $v_1\overline{v}_2 - v_3\overline{v}_4 \in \mathbb{Z}[\mathrm{i}]$ by Lemma 4.1, it follows that $v_1\overline{v}_2 \in \mathbb{Z}[\mathrm{i}]$. On the other hand, it was shown before that $v_1 = \frac{1}{2}(1+\mathrm{i})h_1$ and $v_2 = \frac{1}{2}(1+\mathrm{i})h_2$ with odd h_1 and h_2, hence $v_1\overline{v}_2 = \frac{1}{2}h_1\overline{h}_2$ where $h_1\overline{h}_2$ is odd. So this case is impossible.

(iii) $k_j = 0$ for all j. Then $v_j = h'_j - \mathrm{i} + \frac{1}{2}(1+\mathrm{i})$ with $h'_j \in \mathbb{Z}[\mathrm{i}]$ for $j = 1, 2, 3, 4$. So case (b) is present. ■

References

[1] A. Baker, *Matrix groups*. Springer, 2002.

[2] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*. Fifth ed., The Clarendon Press, Oxford University Press, New York, 1979.

[3] R. A. Horn and C. R. Johnson, *Topics in matrix analysis*. Cambridge University Press, Cambridge, 1991.

[4] M. Lorente and P. Kramer, *Representations of the discrete inhomogeneous Lorentz group and Dirac wave equation on the lattice.* J. Phys. A **32**(1999), no. 12, 2481–2497. http://dx.doi.org/10.1088/0305-4470/32/12/019
[5] J. D. Louck, *A new parametrization and all integral realizations of the Lorentz group.* J. Math. Phys. **43**(2002), 5108–5134. http://dx.doi.org/10.1063/1.1505124
[6] R. Penrose and W. Rindler, *Spinors and space-time.* Vol. I, Cambridge Monographs on Mathematical Physics Cambridge University Press, Cambridge, 1984. http://dx.doi.org/10.1017/CBO9780511564048
[7] A. Schild, *Discrete space-time and integral Lorentz transformations.* Canad. J. Math. **1**(1949), 29–47. http://dx.doi.org/10.4153/CJM-1949-003-4

Sensburger Allee 22 a, D–14055 Berlin
e-mail: cg.jensen@arcor.de

Institut für Mathematik, Technische Universität, D–10623 Berlin
e-mail: pommeren@math.tu-berlin.de