

THE HURWITZ THEOREM ON SUMS OF SQUARES

KEITH CONRAD

1. INTRODUCTION

From commutativity of multiplication (for numbers), a product of two squares is a square: $x^2y^2 = (xy)^2$. A more interesting identity is the following one, which expresses a sum of two squares times a sum of two squares as another sum of two squares:

$$(1.1) \quad (x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

There is also an identity like this for a sum of four squares:

$$(1.2) \quad (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + \\ (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + \\ (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2.$$

This was discovered by Euler in the 18th century, forgotten, and then rediscovered in the 19th century by Hamilton in his work on quaternions. Shortly after Hamilton's rediscovery of (1.2) Cayley discovered a similar 8-square identity.

In all of these sum-of-squares identities, the terms being squared on the right side are all bilinear expressions in the x 's and y 's: each such expression, like $x_1y_2 + x_2y_1$ for sums of two squares, is a linear combination of the x 's when the y 's are fixed and a linear combination of the y 's when the x 's are fixed.

It was natural for mathematicians to search for a similar 16-square identity next, but they were unsuccessful. At the end of the 19th century Hurwitz [4] proved his famous "1,2,4,8 theorem," which says that further identities of this kind are *impossible*.

Theorem 1.1 (Hurwitz, 1898). *Let F be a field of characteristic not equal to 2. If there is an identity*

$$(1.3) \quad (x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2$$

for $x_1, \dots, x_n, y_1, \dots, y_n$ in F , where each z_k is an F -bilinear function of the x 's and the y 's, then $n = 1, 2, 4$ or 8 .

Hurwitz's original proof was stated for $F = \mathbf{C}$, but the field of scalars only needs to be of characteristic not equal to 2 for his proof to work. Nothing would be lost if you take $F = \mathbf{C}$ in the rest of this discussion. (What if the field F has characteristic 2? Then there *is* an identity as in (1.3) for all n because a sum of squares in characteristic 2 is again a square.)

To prove Theorem 1.1, we first show in Section 2 that the existence of a bilinear formula like (1.3) leads to a set of equations in $n \times n$ matrices over F . Then we show by representation

theory in Section 3 that the matrix equations can be solved only when $n = 1, 2, 4$, or 8 . This method is due to Eckmann [2], although our account is based on [3, pp. 141-144].

While Hurwitz proved only the dimension constraints $n = 1, 2, 4$, and 8 , it is also the case that, up to a linear change of variables, the only sum of squares identities in these dimensions are the ones associated to multiplication in the four classical real division algebras of dimensions $1, 2, 4$, and 8 : the real numbers, complex numbers, quaternions, and octonions. For a proof of this more precise result, see [1], [5, §7.6], or [7, Appendix, Chap. 1].

2. THE HURWITZ MATRIX EQUATIONS

Lemma 2.1. *Let V be a finite-dimensional vector space over F , where F does not have characteristic 2. If there is a pair of invertible anti-commuting linear operators on V , then $\dim V$ is even.*

Proof. Suppose $L, L': V \rightarrow V$ are linear, invertible, and $LL' = -L'L$. Taking the determinant of both sides, $(\det L)(\det L') = (-1)^{\dim V}(\det L')(\det L)$. Since L and L' have non-zero determinants, $1 = (-1)^{\dim V}$ in F , so $\dim V$ is even since the characteristic of F is not 2. \square

We return to (1.3). That z_k is a bilinear functions of the x 's and y 's means

$$(2.1) \quad z_k = \sum_{i,j=1}^n a_{ijk} x_i y_j$$

for some $a_{ijk} \in F$. For example, in the case $n = 2$ we see by (1.1) that we can use

$$(2.2) \quad z_1 = x_1 y_1 - x_2 y_2, \quad z_2 = x_1 y_2 + x_2 y_1.$$

We can collect the two equations in (2.2) as components of the equation

$$\begin{aligned} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} &= \begin{pmatrix} x_1 y_1 - x_2 y_2 \\ x_1 y_2 + x_2 y_1 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= \left(x_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}. \end{aligned}$$

From (1.2), in the $n = 4$ case we can use

$$\begin{aligned} z_1 &= x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4, \\ z_2 &= x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3, \\ z_3 &= x_1 y_3 + x_3 y_1 - x_2 y_4 + x_4 y_2, \\ z_4 &= x_1 y_4 + x_4 y_1 + x_2 y_3 - x_3 y_2, \end{aligned}$$

so

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = (x_1 A_1 + x_2 A_2 + x_3 A_3 + x_4 A_4) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix},$$

where A_1, A_2, A_3 , and A_4 are 4×4 matrices with entries 0, 1, and -1 . For example,

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The reader can work out A_3 and A_4 .

Such matrix equations can be developed in the $n \times n$ case too. The scalar equation (2.1) for $k = 1, \dots, n$ is the same as the single equation

$$(2.3) \quad \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} \sum_{i,j} a_{ij1} x_i y_j \\ \vdots \\ \sum_{i,j} a_{ijn} x_i y_j \end{pmatrix} \\ = \begin{pmatrix} \sum_j (\sum_i a_{ij1} x_i) y_j \\ \vdots \\ \sum_j (\sum_i a_{ijn} x_i) y_j \end{pmatrix} \\ = \begin{pmatrix} \sum_i a_{i11} x_i & \cdots & \sum_i a_{in1} x_i \\ \vdots & \ddots & \vdots \\ \sum_i a_{i1n} x_i & \cdots & \sum_i a_{inn} x_i \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

The $n \times n$ matrix in the last expression can be expressed as a sum of n matrices, each one containing only one x_i which can then be pulled out as a coefficient:

$$x_1 \begin{pmatrix} a_{111} & \cdots & a_{1n1} \\ \vdots & \ddots & \vdots \\ a_{11n} & \cdots & a_{1nn} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{n11} & \cdots & a_{nn1} \\ \vdots & \ddots & \vdots \\ a_{n1n} & \cdots & a_{nnn} \end{pmatrix}.$$

This sum can be written as $x_1 A_1 + \cdots + x_n A_n$, where A_i is an $n \times n$ matrix with (j, k) -entry a_{ikj} . (Why the index reversal on the subscripts? That is in the nature of how matrix-vector multiplication works: look at the $n = 2$ case to convince yourself in a concrete case that this index reversal is not an error.) Now (2.3) reads as

$$\mathbf{z} = (x_1 A_1 + \cdots + x_n A_n) \mathbf{y} = A_{\mathbf{x}} \mathbf{y},$$

where we set $A_{\mathbf{x}} = x_1 A_1 + \cdots + x_n A_n$.

With this notation, the right side of (1.3) is

$$\begin{aligned} z_1^2 + \cdots + z_n^2 &= \mathbf{z} \cdot \mathbf{z} \\ &= A_{\mathbf{x}} \mathbf{y} \cdot A_{\mathbf{x}} \mathbf{y} \\ &= (A_{\mathbf{x}}^\top A_{\mathbf{x}} \mathbf{y}) \cdot \mathbf{y}, \end{aligned}$$

where the last equation is a special instance of the general identity $\mathbf{v} \cdot A \mathbf{w} = A^\top \mathbf{v} \cdot \mathbf{w}$ for any $n \times n$ matrix A over F and vectors \mathbf{v} and \mathbf{w} in F^n .¹

¹The identity $\mathbf{v} \cdot A \mathbf{w} = A^\top \mathbf{v} \cdot \mathbf{w}$ holds for rectangular A , say $m \times n$, as long as the products make sense: \mathbf{v} is in F^m , \mathbf{w} is in F^n , the dot product on the left is in F^m , and the dot product on the right is in F^n .

The left side of (1.3) is

$$\left(\sum x_i^2\right) \mathbf{y} \cdot \mathbf{y} = \left(\left(\sum x_i^2\right) \mathbf{y}\right) \cdot \mathbf{y}.$$

Therefore

$$\left(A_{\mathbf{x}}^{\top} A_{\mathbf{x}} \mathbf{y}\right) \cdot \mathbf{y} = \left(\left(\sum x_i^2\right) \mathbf{y}\right) \cdot \mathbf{y}.$$

Comparing the two sides as \mathbf{y} varies shows (since F has more than 2 elements)

$$(2.4) \quad A_{\mathbf{x}}^{\top} A_{\mathbf{x}} = \left(\sum x_i^2\right) I_n.$$

Expanding the left side of (2.4) using $A_{\mathbf{x}} = x_1 A_1 + \cdots + x_n A_n$, we have

$$A_{\mathbf{x}}^{\top} A_{\mathbf{x}} = \sum_{i=1}^n \left(A_i^{\top} A_i\right) x_i^2 + \sum_{1 \leq i < j \leq n} \left(A_i^{\top} A_j + A_j^{\top} A_i\right) x_i x_j,$$

so (2.4) is equivalent to the system of matrix equations

$$(2.5) \quad A_i^{\top} A_i = I_n, \quad A_i^{\top} A_j + A_j^{\top} A_i = O \text{ for } i < j.$$

These are the *Hurwitz matrix equations*. (The actual entries in the A_i 's won't matter anymore.) The rest of the proof of Theorem 1.1 is now devoted to showing these equations in $n \times n$ matrices can exist only if n is 1, 2, 4, or 8. Without loss of generality, $n > 2$.

We normalize the matrices A_i to make one of them the identity, as follows. By (2.5), A_i is an invertible matrix whose inverse is A_i^{\top} . Set

$$B_i = A_i A_n^{\top}.$$

The equations in (2.5) are easily seen to be equivalent to

$$(2.6) \quad B_n = I_n, \quad B_i^{\top} B_i = I_n, \quad B_i^{\top} B_j + B_j^{\top} B_i = O \text{ for } i \neq j.$$

(We write $i \neq j$ rather than $i < j$ to make things more symmetric; it doesn't change anything.) Taking $j = n$ in the third equation shows $B_i^{\top} = -B_i$ for $i \neq n$. Therefore the $n - 1$ matrices B_1, \dots, B_{n-1} satisfy

$$(2.7) \quad B_i^{\top} = -B_i, \quad B_i^2 = -I_n, \quad B_i B_j = -B_j B_i \text{ for } i \neq j.$$

Using (2.7), the group of matrices generated by the B_i 's. is the set of all matrix products

$$\pm B_1^{a_1} \cdots B_{n-1}^{a_{n-1}},$$

where $a_i = 0$ or 1. Note $-I_n \neq I_n$ since F doesn't have characteristic 2.

We see immediately from (2.7) and Lemma 2.1 that n is *even*. In the next section we will prove that if (2.7) holds for an even $n > 2$, then $n = 4$ or 8.

3. A 2-GROUP AND REPRESENTATION THEORY

For any integer $n \geq 2$, let G be a group generated by elements g_1, \dots, g_{n-1} such that

$$(3.1) \quad g_i^2 = \varepsilon \neq 1, \quad \varepsilon^2 = 1, \quad g_i g_j = \varepsilon g_j g_i \text{ for } i \neq j.$$

(Does such a group exist? For us, all that matters is that when n is even and the Hurwitz matrix equations (2.5) hold for some $n \times n$ matrices A_1, \dots, A_n , then by setting $B_i = A_i A_n^{\top}$ for $i = 1, \dots, n$, so $B_n = I_n$, the group $\langle B_1, \dots, B_{n-1} \rangle$ is an example of such G .) Since ε is a power of each g_i , ε commutes with each g_i , so $\varepsilon \in Z(G)$. In particular, the subgroup

$\langle \varepsilon \rangle = \{1, \varepsilon\}$ is normal in G and $G/\langle \varepsilon \rangle$ is abelian and generated by $n-1$ elements with order 1 or 2, so $|G/\langle \varepsilon \rangle|$ divides 2^{n-1} . Thus $|G| \mid 2^n$ and each $x \in G$ can be written as

$$(3.2) \quad \varepsilon^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}},$$

where the exponents a_i are each 0 or 1.

It is natural to expect that $|G| = 2^n$, so each element of G has a unique expression in the form (3.2). Indeed, Herstein [3, p. 142] writes in his treatment of Hurwitz's theorem that G "clearly" has order 2^n . However, this is wrong: the group Q_8 occurs as G using $n = 4$ with g_1, g_2 , and g_3 being i, j , and k , and $|Q_8|$ is $8 = 2^{n-1}$ rather than $16 = 2^n$. When Eckmann [2, pp. 359-360] proved Hurwitz's theorem using representation theory, he didn't define G merely as a group generated by elements satisfying (3.1), but as the group having a *presentation* analogous to (3.1): his G is the free group on $\varepsilon, g_1, \dots, g_{n-1}$ satisfying the relations $\varepsilon^2 = 1, g_i^2 = \varepsilon$, and $g_i g_j = \varepsilon g_j g_i$ for $i \neq j$. The group defined this way has order 2^n for all $n \geq 2$ and it is the group $\mathbf{G}_{n-1,0}$ within the family of Clifford–Littlewood–Eckmann groups $\mathbf{G}_{s,t}$ of order 2^{s+t+1} studied by Lam and Smith [6]. We won't use group presentations here, and retain the meaning of G as being just some group with generators satisfying (3.1). Such a group has order 2^n or 2^{n-1} , as we'll see below.

We now prove the following facts about G :²

- (a) $Z(G) = \{1, \varepsilon\}$ for odd n and $Z(G) = \{1, \varepsilon, g_1 \cdots g_{n-1}, \varepsilon g_1 \cdots g_{n-1}\}$ for even n (the 4 elements in the even case might not be different, as indicated in (b)),
- (b) if n is odd, then $|G| = 2^n$ and $|Z(G)| = 2$, while if n is even, then (i) $|G| = 2^{n-1}$ and $|Z(G)| = 2$, or (ii) $|G| = 2^n$ and $|Z(G)| = 4$.
- (c) if $n \geq 3$, then $[G, G] = \{1, \varepsilon\}$,
- (d) If $x \notin Z(G)$, then the conjugacy class of x is $\{x, \varepsilon x\}$.

Fact (a): Let's see how each g_i conjugates elements in G . For $x \in G$, written as in (3.2),

$$(3.3) \quad g_i x g_i^{-1} = (g_i \varepsilon g_i^{-1})^{a_0} (g_i g_1 g_i^{-1})^{a_1} \cdots (g_i g_{n-1} g_i^{-1})^{a_{n-1}},$$

with $g_i \varepsilon g_i^{-1} = \varepsilon$, $g_i g_i g_i^{-1} = g_i$, and $g_i g_j g_i^{-1} = \varepsilon g_j$ if $j \neq i$. Since $\varepsilon \in Z(G)$, by setting $S = a_1 + \cdots + a_{n-1}$, (3.3) simplifies to

$$(3.4) \quad g_i x g_i^{-1} = \varepsilon^{a_0 + \sum_{j \neq i, j \geq 1} a_j} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}} = \varepsilon^{S-a_i} x$$

for each $i \geq 1$. Thus

$$x \in Z(G) \iff g_i x g_i^{-1} = x \text{ for all } i \geq 1 \iff \varepsilon^{S-a_i} = 1 \text{ for all } i \geq 1,$$

which is equivalent to $S \equiv a_i \pmod{2}$ for all i , so all a_i 's for $i \geq 1$ are equal (each is 0 or 1). Let a be that common value, so $S = a_1 + \cdots + a_{n-1} \equiv (n-1)a \pmod{2}$. Hence $(n-1)a \equiv a \pmod{2}$, which is equivalent to $na \equiv 0 \pmod{2}$. Thus $x \in Z(G)$ if and only if $x = \varepsilon^{a_0} g_1^a \cdots g_{n-1}^a$ where the common exponent a in $\{0, 1\}$ satisfies $na \equiv 0 \pmod{2}$.

For odd n , necessarily $a = 0$, so $x = \varepsilon^{a_0}$. We already know $\varepsilon \in Z(G)$, so $Z(G) = \{1, \varepsilon\}$.

For even n , a is 0 or 1: $x = \varepsilon^{a_0}$ if $a = 0$ and $x = \varepsilon^{a_0} g_1 \cdots g_{n-1}$ if $a = 1$, so $Z(G) = \{1, \varepsilon, g_1 \cdots g_{n-1}, \varepsilon g_1 \cdots g_{n-1}\}$. (**Note**: this $Z(G)$ has order 2 or 4, not necessarily 4.)

Fact (b): If $n = 2$ then $G = \langle g_1 \rangle$ is cyclic with $g_1^2 = \varepsilon \neq 1$ and $\varepsilon^2 = 1$, so G is cyclic of order 4, which fits condition (ii) in Fact (b). Now take $n \geq 3$.

²I thank M. Mazur for fixing some gaps in the reasoning I used in (a) and (b) in an earlier version.

We saw in (3.4) that when x is written as in (3.2), $g_i x g_i^{-1} = \varepsilon^{S-a_i} x$ for all $i \geq 1$. Write x in a second way as $\varepsilon^{b_0} g_1^{b_1} \cdots g_{n-1}^{b_{n-1}}$ where the exponents are again 0 or 1, so $g_i x g_i^{-1} = \varepsilon^{T-b_i} x$ for $i \geq 1$ where $T = b_1 + \cdots + b_{n-1}$. Thus

$$\varepsilon^{S-a_i} = \varepsilon^{T-b_i}$$

for $i \geq 1$. Since ε has order 2,

$$(3.5) \quad S - a_i \equiv T - b_i \pmod{2}$$

for $i \geq 1$.

Case 1: $S \equiv T \pmod{2}$. By (3.5), $a_i \equiv b_i \pmod{2}$ for $i \geq 1$, so $a_i = b_i$ for $i \geq 1$. Equating the two formulas for x having exponents a_0, \dots, a_{n-1} and b_0, \dots, b_{n-1} now gives us

$$\varepsilon^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}} = \varepsilon^{b_0} g_1^{b_1} \cdots g_{n-1}^{b_{n-1}} = \varepsilon^{b_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}},$$

so $\varepsilon^{a_0} = \varepsilon^{b_0}$. Thus $a_0 = b_0$ since ε has order 2, so $a_i = b_i$ for $i \geq 0$.

Case 2: $S \not\equiv T \pmod{2}$. By (3.5), $a_i \equiv b_i + 1 \pmod{2}$ for $i \geq 1$, so $S = a_1 + \cdots + a_{n-1} \equiv (b_1 + \cdots + b_{n-1}) + n - 1 \equiv T + n - 1 \pmod{2}$. Thus $n - 1 \equiv S - T \equiv 1 \pmod{2}$, so n is even.

If n is odd, then Case 2 can't occur, so by Case 1,

$$\varepsilon^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}} = \varepsilon^{b_0} g_1^{b_1} \cdots g_{n-1}^{b_{n-1}} \implies a_i = b_i \text{ in } \{0, 1\} \text{ for } i \geq 0,$$

which implies $|G| = 2^n$. By Fact (a), $Z(G) = \{1, \varepsilon\}$ and this has order 2 since $\varepsilon \neq 1$.

Now suppose n is even, so $n \geq 4$. The subgroup $H = \langle g_1, \dots, g_{n-2} \rangle$ has $n - 1$ in place of n since $n - 2 = (n - 1) - 1$, and H has the same defining properties as G except the odd number $n - 1$ replaces the even number n and $n - 1 \geq 3$. By what we already did in the odd case, $|H| = 2^{n-1}$. Since $|G| \mid 2^n$, $|G|$ is either 2^{n-1} or 2^n . If $|G| = 2^{n-1}$ then $G = H$, so $Z(G) = Z(H)$, which has order 2. This is part (i) in Fact (b). If instead $|G| = 2^n$, then since the elements of G all have the form (3.2) with exponents 0 and 1 and this gives us at most 2^n elements, different sets of n exponents must belong to different elements of G . Thus in Fact (a), the 4 products in $Z(G)$ are distinct.

Fact (c): Since $G/\{1, \varepsilon\}$ is abelian, $[G, G] \subset \{1, \varepsilon\}$. When $n \geq 3$, $g_1 g_2 g_1^{-1} g_2^{-1} = \varepsilon$, so $[G, G] = \{1, \varepsilon\}$. (When $n = 2$, G is cyclic of order 4, and thus is abelian, so $[G, G]$ is trivial.)

Fact (d): By (3.4), $g_i x g_i^{-1}$ is x or εx . The set $\{x, \varepsilon x\}$ is closed under conjugation by G since the g_i 's generate G . Thus the conjugacy class of x is contained in $\{x, \varepsilon x\}$. When $x \notin Z(G)$, the conjugacy class of x has to contain more than x , so it must be $\{x, \varepsilon x\}$.

We now bring in representation theory. The original Hurwitz problem when $n \geq 3$ gives us an n -dimensional (faithful) representation of G over F where n is even. View this as a representation of G over the algebraic closure \overline{F} . Which irreducible representations of G over \overline{F} can occur in this n -dimensional representation? Since $|G|$ is a power of 2 and \overline{F} doesn't have characteristic 2, the characteristic of \overline{F} doesn't divide $|G|$, so classical representation theory applies.

By Fact (b) for even n , $|G|$ is 2^n or 2^{n-1} .

First suppose $|G| = 2^n$. Then $G/[G, G]$ has size 2^{n-1} by Fact (c), so G has 2^{n-1} representations of degree 1. The number of representations of G over \overline{F} is the number of conjugacy classes of G . Fact (d) tells us conjugacy classes of G outside $Z(G)$ have size 2,

and $|Z(G)| = 4$ by Fact (b), so the number of conjugacy classes in G is

$$|Z(G)| + \frac{1}{2}(|G| - |Z(G)|) = 4 + \frac{1}{2}(2^n - 4) = 2^{n-1} + 2.$$

Thus, G has two irreducible representations of degree greater than 1. Let f_i be the degrees of the irreducible representations of G over \overline{F} . Since $|G| = \sum f_i^2$ and all f_i divide $|G|$ (hence all f_i are powers of 2), the uniqueness of base 2 expansions implies (since $n - 1 > 1$) that G has two irreducible representations of degree $2^{\frac{n}{2}-1} > 1$ since n is even.

The Hurwitz problem gives us an n -dimensional representation of G where ε is represented by $-I_n$, so ε acts by the negative of the identity map on each subspace. Since $\varepsilon \in [G, G]$, it is sent to 1 under all 1-dimensional representations. Therefore our n -dimensional representation of G has no irreducible subrepresentations of degree 1, which means its irreducible subrepresentations all have degree $2^{n/2-1}$. So for even $n > 2$ we must have

$$(3.6) \quad 2^{\frac{n}{2}-1} \mid n.$$

Letting $n = 2^r s$ for $r \geq 1$ and s odd, we get $\frac{n}{2} - 1 \leq r$ by (3.6), so

$$2^r \leq n \leq 2r + 2.$$

Since $2^r > 2r + 2$ when $r \geq 4$, we have $r = 1, 2$, or 3 , so $2 \leq n \leq 4$, $4 \leq n \leq 6$, or $8 \leq n \leq 8$. Thus n is 4, 6, or 8. The option $n = 6$ doesn't work since $2^{\frac{6}{2}-1} \nmid 6$, so n is 4 or 8.

Next suppose $|G| = 2^{n-1}$, so $Z(G)$ has size 2 by Fact (b) and $G/[G, G]$ has size 2^{n-2} by Fact (c). Thus G has 2^{n-2} representations of degree 1. By Fact (d), the number of conjugacy classes of G is

$$|Z(G)| + \frac{1}{2}(|G| - |Z(G)|) = 2 + \frac{1}{2}(2^{n-1} - 2) = 2^{n-2} + 1,$$

so G has just 1 irreducible representation of degree f greater than 1 and $2^{n-2} + f^2 = 2^{n-1}$, so $f = 2^{\frac{n}{2}-1}$. By the same reasoning as in the case $|G| = 2^n$, we get $2^{\frac{n}{2}-1} \mid n$, which implies n is 4 or 8 just like before.

Remark 3.1. When the group G is defined for odd $n \geq 3$, we have $|G| = 2^n$, $|[G, G]| = 2$, and $|Z(G)| = 2$, so G has 2^{n-1} irreducible representations of degree 1 and the number of conjugacy classes in G is $2 + \frac{1}{2}(2^n - 2) = 2^{n-1} + 1$. Thus G has just one irreducible representation of degree greater than 1, and that degree is $2^{\frac{n-1}{2}}$.

REFERENCES

- [1] M. L. Curtis, *Abstract Linear Algebra*, Springer-Verlag, New York, 1990.
- [2] B. Eckmann, "Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Composition quadratischen Formen," *Comment. Math. Helv.* **15** (1942), 358–366. URL <https://eudml.org/doc/138818>.
- [3] I. Herstein, *Noncommutative Rings*, Mathematical Association of America, 1968.
- [4] A. Hurwitz, "Über die Composition der quadratischen Formen von beliebig vielen Variablen," *Werke*, Band II, Basel 1932, 565–571. URL <https://eudml.org/doc/58420>.
- [5] N. Jacobson, *Basic Algebra I*, 2nd ed., W.H. Freeman and Co., New York, 1985.
- [6] T. Y. Lam and T. Smith, "On the Clifford–Littlewood–Eckmann Groups: a New Look at Periodicity mod 8," *Rocky Mountain J. Math.* **19** (1989), 749–786. URL <https://projecteuclid.org/journalArticle/Download?urlId=10.1216%2FRMJ-1989-19-3-749#page15>.
- [7] D. Shapiro, *Compositions of Quadratic Forms*, de Gruyter, New York, 2000.