Parallelogram-Law Type Identities

Ömer Eğecioğlu
Department of Computer Science
University of California Santa Barbara, CA 93106

Abstract

Identities generalizing the well-known formula relating the lengths of the sides and the diagonals of a parallelogram in the plane are given. These generalizations all have the flavor of the parallelogram-law, and specialize to formulas involving sums of roots of unity, trigonometric functions, binomial coefficients, and permutations over the symmetric and the alternating groups.

Keywords: Parallelogram-law, primitive root, doubly transitive group, Vandermonde convolution.

The parallelogram-law in the complex plane is

$$2\,(|z_1|^2 + |z_2|^2) = |z_1 + z_2|^2 + |z_1 - z_2|^2 \tag{1}$$

where $z_1 = x_1 + i\,y_1$, $z_2 = x_2 + i\,y_2$, and x_1, y_1, x_2, y_2 are real numbers. The parallelogram-law relates the lengths of the diagonals of a parallelogram with vertices $(0,0)$, (x_1, y_1), (x_2, y_2), and $(x_1 + x_2, y_1 + y_2)$ to the lengths of its sides.

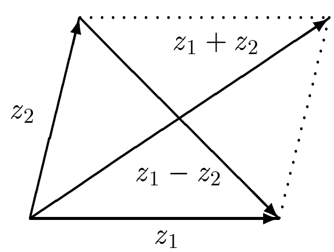

Figure 1: The Parallelogram law in the plane.

In general, a Hilbert space is a Banach space whose norm $\|x\|$ satisfies the parallelogram property

$$2\,(\|x\|^2 + \|y\|^2) = \|x + y\|^2 + \|x - y\|^2 \ .$$

Consider the binomial identity

$$(n+1)\,(m+1)^n \binom{2m}{m} \;=\; \sum_{0 \le i_0, i_1, \ldots, i_n \le m} \left[(-1)^{i_0} \binom{m}{i_0} + (-1)^{i_1} \binom{m}{i_1} + \cdots + (-1)^{i_n} \binom{m}{i_n} \right]^2 , \tag{2}$$

and the identity

$$\frac{(n-2)!}{2}\, n^3 \;=\; \sum_{\sigma\in\mathcal{A}_n} |\,\omega^{1+\sigma_1}+\omega^{2+\sigma_2}+\cdots+\omega^{n+\sigma_n}|^2 \,, \tag{3}$$

where $\mathcal{A}_n$ is the alternating group of degree n and ω is a primitive n-th root of unity. It is not immediately clear why (2) or (3) should have any relation to the parallelogram-law. However if we first write (1) in an equivalent form as

$$4\sum_{i=1}^{2}|z_i|^2 \;=\; \sum_{\alpha_{i_1},\alpha_{i_2}\in A} |\alpha_{i_1}z_1+\alpha_{i_2}z_2|^2 \,. \tag{4}$$

where $A=\{-1,1\}$, then the right hand sides of (2), (3), and (4) become sums of squares of norms of certain vectors. Generalizations of complex number identities of this type based on length-preserving properties of unitary transformations were considered by Klamkin and Murty [6]. In this paper, we take the formulation (4) for the parallelogram-law as the starting point, and give elementary proofs as well as a number of specializations of the following theorems of similar flavor.

Theorem 1 *Assume $A=\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ is a set of complex numbers with $\alpha_1+\alpha_2+\cdots+\alpha_m=0$. Then for any n complex numbers $z_1,z_2,\ldots,z_n$,*

$$m^{n-1}\left(\sum_{\alpha\in A}|\alpha|^2\right)\left(\sum_{i=1}^{n}|z_i|^2\right) \;=\; \sum_{\alpha_{i_1},\alpha_{i_2},\ldots,\alpha_{i_n}\in A} |\alpha_{i_1}z_1+\alpha_{i_2}z_2+\cdots+\alpha_{i_n}z_n|^2 \,. \tag{5}$$

Theorem 2 *Assume $A=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ is a set of complex numbers with $\alpha_1+\alpha_2+\cdots+\alpha_n=0$, and let $\mathcal{S}_n$ denote the symmetric group of degree n. Then for any n complex numbers $z_1,z_2,\ldots,z_n$,*

$$(n-2)!\left(\sum_{\alpha\in A}|\alpha|^2\right)\left[n\sum_{i=1}^{n}|z_i|^2-|z_1+z_2+\cdots+z_n|^2\right] \;=\; \sum_{\sigma\in\mathcal{S}_n} |\alpha_{\sigma_1}z_1+\alpha_{\sigma_2}z_2+\cdots+\alpha_{\sigma_n}z_n|^2 \,. \tag{6}$$

More generally

Theorem 3 *Assume $A=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ is a set of complex numbers with $\alpha_1+\alpha_2+\cdots+\alpha_n=0$, and let $\mathcal{G}$ be a doubly transitive group of permutations of degree n. Let g_2 denote the size of a stabilizer subgroup of a pair and let g_1 denote the size of the stabilizer subgroup of a single point. Then for any n complex numbers $z_1,z_2,\ldots,z_n$,*

$$g_2\left(\sum_{\alpha\in A}|\alpha|^2\right)\left[\frac{|\mathcal{G}|}{g_1}\sum_{i=1}^{n}|z_i|^2-\;|z_1+z_2+\cdots+z_n|^2\right] \;=\; \sum_{\sigma\in\mathcal{G}} |\alpha_{\sigma_1}z_1+\alpha_{\sigma_2}z_2+\cdots+\alpha_{\sigma_n}z_n|^2 \,. \tag{7}$$

Before giving the proofs, we look at some special cases. First, some consequences of Theorem 1:

Example 1.1: Take $A = \{-1, 1\}$ and $n = 2$. Then (5) reads

$$2 \cdot (2)\,(|z_1|^2 + |z_2|^2) \;=\; |z_1 + z_2|^2 + |z_1 - z_2|^2 + |-z_1 - z_2|^2 + |-z_1 + z_2|^2 \;=\; 2\,|z_1 + z_2|^2 + 2\,|z_1 - z_2|^2 ,$$

which simplifies to

$$2\,(|z_1|^2 + |z_2|^2) = |z_1 + z_2|^2 + |z_1 - z_2|^2 .$$

Example 1.2: Take $A = \{-1, 1\}$ and $n = 3$. Then

$$\begin{aligned} 8\,(|z_1|^2 + |z_2|^2 + |z_3|^2) \;&=\; |z_1 + z_2 + z_3|^2 + |z_1 + z_2 - z_3|^2 + |z_1 - z_2 + z_3|^2 + |z_1 - z_2 - z_3|^2 \\ &+\; |-z_1 - z_2 - z_3|^2 + |-z_1 - z_2 + z_3|^2 + |-z_1 + z_2 - z_3|^2 + |-z_1 + z_2 + z_3|^2 \end{aligned}$$

and therefore

$$4\,(|z_1|^2 + |z_2|^2 + |z_3|^2) = |z_1 + z_2 + z_3|^2 + |z_1 + z_2 - z_3|^2 + |z_1 - z_2 + z_3|^2 + |z_1 - z_2 - z_3|^2 .$$

Example 1.3: Let ω be a primitive cube root of unity and $A = \{1, \omega, \omega^2\}$. For $n = 2$ we have

$$\begin{aligned} 3\,(1 + |\omega|^2 + |\omega^2|^2)(|z_1|^2 + |z_2|^2) \;&=\; |z_1 + z_2|^2 + |z_1 + \omega z_2|^2 + |\omega z_1 + z_2|^2 + |\omega z_1 + \omega z_2|^2 + |\omega z_1 + \omega^2 z_2|^2 \\ &+\; |\omega^2 z_1 + \omega z_2|^2 + |\omega^2 z_1 + \omega^2 z_2|^2 + |\omega^2 z_1 + z_2|^2 + |z_1 + \omega^2 z_2|^2 . \end{aligned}$$

Thus

$$3\,(|z_1|^2 + |z_2|^2) = |z_1 + z_2|^2 + |z_1 + \omega z_2|^2 + |\omega z_1 + z_2|^2 .$$

Example 1.4: Take A as in Example 1.3 and $n = 3$. Then

$$\begin{aligned} 9\,(|z_1|^2 + |z_2|^2 + |z_3|^2) \;&=\; |z_1 + z_2 + z_3|^2 + |z_1 + z_2 + \omega z_3|^2 + |z_1 + \omega z_2 + z_3|^2 + |\omega z_1 - z_2 - z_3|^2 + \\ &+\; |z_1 + z_2 + \omega^2 z_3|^2 + |z_1 + \omega^2 z_2 + z_3|^2 + |\omega^2 z_1 + z_2 + z_3|^2 + |z_1 + \omega z_2 + \omega^2 z_3|^2 + |z_1 + \omega^2 z_2 + \omega z_3|^2 \end{aligned}$$

Example 1.5: Let $A = \{(-1)^i \binom{m}{i} \mid i = 0, 1, \ldots, m\}$, m odd. Then

$$\sum_{\alpha \in A} |\alpha|^2 \;=\; \sum_{i=0}^{m} \binom{m}{i}^2 \;=\; \binom{2m}{m}$$

by the Vandermonde identity [2], [7]. Thus

$$(m+1)^n \binom{2m}{m} \sum_{i=0}^{n} |z_i|^2 \;=\; \sum_{0 \le i_0, i_1, \ldots, i_n \le m} \left| (-1)^{i_0} \binom{m}{i_0} z_0 + (-1)^{i_1} \binom{m}{i_1} z_1 + \cdots + (-1)^{i_n} \binom{m}{i_n} z_n \right|^2$$

In particular, taking $z_0 = z_1 = \cdots = z_n = 1$,

$$(n+1)\ (m+1)^n \binom{2m}{m} = \sum_{0 \le i_0, i_1, \ldots, i_n \le m} \left[(-1)^{i_0} \binom{m}{i_0} + (-1)^{i_1} \binom{m}{i_1} + \cdots + (-1)^{i_n} \binom{m}{i_n} \right]^2 ,$$

which is the identity (2), and taking $n = m$ with

$$z_i = \binom{m}{i} \ ; \quad i = 0, 1, \ldots, m \ ,$$

one has

$$(n+1)^n \binom{2n}{n}^2 = \sum_{0 \le i_0, i_1, \ldots, i_n \le n} \left[(-1)^{i_0} \binom{n}{i_0}\binom{n}{0} + (-1)^{i_1} \binom{n}{i_1}\binom{n}{1} + \cdots + (-1)^{i_n} \binom{n}{i_n}\binom{n}{n} \right]^2 .$$

Next we consider a number of special cases of Theorem 2:

Example 2.1: Take $A = \{-1, 1\}$. Then (6) reads

$$4\ (|z_1|^2 + |z_2|^2) - 2\ |z_1 + z_2|^2 = |z_1 - z_2|^2 + |-z_1 + z_2|^2 \ .$$

Consequently

$$2\ (|z_1|^2 + |z_2|^2) = |z_1 + z_2|^2 + |z_1 - z_2|^2 \ ,$$

which is again the parallelogram law for the plane.

Example 2.2: Let ω be a primitive n-th root of unity and $A = \{1, \omega, \ldots, \omega^{n-1}\}$. Then Theorem 2 gives

$$(n-2)!\, n^2 \sum_{i=1}^{n} |z_i|^2 \ = \ (n-2)!\, n\, |z_1 + z_2 + \cdots + z_n|^2 + \sum_{\sigma \in \mathcal{S}_n} |\omega^{\sigma_1} z_1 + \omega^{\sigma_2} z_2 + \cdots + \omega^{\sigma_n} z_n|^2$$

Example 2.3: Let ω be a primitive n-th root of unity and take $z_i = \omega^i$ for $i = 1, 2, \ldots, n$. Then

$$(n-2)!\, n^2 \sum_{\alpha \in A} |\alpha|^2 = \sum_{\sigma \in \mathcal{S}_n} |\alpha_{\sigma_1}\omega + \alpha_{\sigma_2}\omega^2 + \cdots + \alpha_{\sigma_n}\omega^n|^2 \tag{8}$$

for any set of complex numbers $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ whose sum is zero. In particular

$$(n-2)!\, n^3 \ = \ \sum_{\sigma \in \mathcal{S}_n} |\, \omega^{1+\sigma_1} + \omega^{2+\sigma_2} + \cdots + \omega^{n+\sigma_n}|^2 \ .$$

Example 2.4: Let $\alpha_k = z_k = \cos\frac{2\pi k}{n}$ for $k = 1, 2, \ldots, n$. Then

$$\sum_{k=1}^{n} \alpha_k = \sum_{k=1}^{n} z_k \;=\; 0 \quad .$$

Since

$$\sum_{k=1}^{n} \cos^2 kx \;=\; \frac{n}{2} + \frac{\cos(n+1)x \sin nx}{2\ \sin x}$$

(see [5], for example), we have

$$\sum_{k=1}^{n} |\alpha_k|^2 \;=\; \sum_{k=1}^{n} |z_k|^2 \;=\; \frac{n}{2} \quad .$$

This gives the identity

$$(n-2)!\ \frac{n^3}{4} \;=\; \sum_{\sigma\in\mathcal{S}_n} \left[\cos\frac{2\pi\sigma_1}{n}\cos\frac{2\pi}{n} + \cos\frac{2\pi\sigma_2}{n}\cos\frac{4\pi}{n} + \cdots + \cos\frac{2\pi\sigma_n}{n}\cos\frac{2n\pi}{n}\right]^2 \quad .$$

Similarly, since

$$\sum_{k=1}^{n} \sin^2 kx \;=\; \frac{n}{2} - \frac{\cos(n+1)x \sin nx}{2\ \sin x} \quad ,$$

by taking $\alpha_k = \cos\frac{2\pi k}{n}$, $z_k = \sin\frac{2\pi k}{n}$ we obtain the trigonometric identity

$$(n-2)!\ \frac{n^3}{4} \;=\; \sum_{\sigma\in\mathcal{S}_n} \left[\sin\frac{2\pi\sigma_1}{n}\cos\frac{2\pi}{n} + \sin\frac{2\pi\sigma_2}{n}\cos\frac{4\pi}{n} + \cdots + \sin\frac{2\pi\sigma_n}{n}\cos\frac{2n\pi}{n}\right]^2 \quad ,$$

and by taking $\alpha_k = \sin\frac{2\pi k}{n}$, $z_k = \sin\frac{2\pi k}{n}$ for $k = 1, 2, \ldots, n$, we obtain the identity

$$(n-2)!\ \frac{n^3}{4} \;=\; \sum_{\sigma\in\mathcal{S}_n} \left[\sin\frac{2\pi\sigma_1}{n}\sin\frac{2\pi}{n} + \sin\frac{2\pi\sigma_2}{n}\sin\frac{4\pi}{n} + \cdots + \sin\frac{2\pi\sigma_n}{n}\sin\frac{2n\pi}{n}\right]^2 \quad .$$

Example 2.5: Let $A \;=\; \{(-1)^i \binom{n}{i} \mid i = 0, 1, \ldots, n\}$, n odd. If we take

$$z_i \;=\; (-1)^i \binom{n}{i} \quad ; \qquad i = 0, 1, \ldots, n \ ,$$

and use the Vandermonde convolution identity, we find that

$$\frac{(n+1)!}{n}\binom{2n}{n}^2 \;=\; \sum_{\sigma\in\mathcal{S}_{\{0,1,\ldots,n\}}} \left[(-1)^{\sigma_0}\binom{n}{\sigma_0}\binom{n}{0} + (-1)^{1+\sigma_1}\binom{n}{\sigma_1}\binom{n}{1} + \cdots + (-1)^{n+\sigma_n}\binom{n}{\sigma_n}\binom{n}{n}\right]^2 ,$$

where $\mathcal{S}_{\{0,1,\ldots,n\}}$ denotes the permutation group on $\{0, 1, \ldots, n\}$. Taking

$$z_i \;=\; \binom{n}{i} \quad ; \qquad i = 0, 1, \ldots, n \ ,$$

we obtain

$$\frac{(n+1)!}{n}\binom{2n}{n}\left[\binom{2n}{n}-4^n\right] = \sum_{\sigma\in\mathcal{S}_{\{0,1,\ldots,n\}}}\left[(-1)^{\sigma_0}\binom{n}{\sigma_0}\binom{n}{0}+(-1)^{\sigma_1}\binom{n}{\sigma_1}\binom{n}{1}+\cdots+(-1)^{\sigma_n}\binom{n}{\sigma_n}\binom{n}{n}\right]^2 .$$

Finally we consider some special cases of Theorem 3:

Example 3.1: Let $\mathcal{G}=\mathcal{S}_n$. Then $g_2=(n-2)!$, $g_1=(n-1)!$ and Theorem 3 specializes to Theorem 2.

Example 3.2: Take $\alpha_i=z_i=\omega^i$ for $i=1,2,\ldots,n$, where ω is a primitive n-th root of unity. Then

$$n^2\,(g_1+g_2) = \sum_{\sigma\in\mathcal{G}}|\,\omega^{1+\sigma_1}+\omega^{2+\sigma_2}+\cdots+\omega^{n+\sigma_n}|^2 ,$$

for any doubly transitive group of permutations $\mathcal{G}$ of degree n.

Example 3.3: Let $\mathcal{G}=\mathcal{A}_n$ be the alternating group of degree n. Then $g_2=(n-2)!/2$, $g_1=(n-1)!/2$ and (7) becomes

$$\frac{(n-2)!}{2}\left(\sum_{\alpha\in A}|\alpha|^2\right)\left[n\sum_{i=1}^{n}|z_i|^2-|z_1+z_2+\cdots+z_n|^2\right] = \sum_{\sigma\in\mathcal{A}_n}|\alpha_{\sigma_1}z_1+\alpha_{\sigma_2}z_2+\cdots+\alpha_{\sigma_n}z_n|^2 .$$

Taking $z_i=\omega^i$ for $i=1,2,\ldots,n$, where ω is a primitive n-th root of unity, analogous to (8) we obtain

$$\frac{(n-2)!}{2}\,n^2\sum_{\alpha\in A}|\alpha|^2=\sum_{\sigma\in\mathcal{A}_n}|\alpha_{\sigma_1}\omega+\alpha_{\sigma_2}\omega^2+\cdots+\alpha_{\sigma_n}\omega^n|^2$$

for any set of complex numbers $A=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ whose sum is zero. In particular

$$\frac{(n-2)!}{2}\,n^3 = \sum_{\sigma\in\mathcal{A}_n}|\omega^{1+\sigma_1}+\omega^{2+\sigma_2}+\cdots+\omega^{n+\sigma_n}|^2 ,$$

which is the identity given in (3).

Now we give proofs of Theorems 1–3. These proofs are essentially based on the fact that unitary transformations are length-preserving.

Proof of Theorem 1: Consider the $m^n\times n$ matrix $\mathbf{M}$ whose rows consists of all distinct vectors $(\alpha_{i_1},\alpha_{i_2},\ldots,\alpha_{i_n})$ with $\alpha_{i_k}\in A$, $k=1,2,\ldots,n$. Let $\mathbf{z}=(z_1,z_2,\ldots,z_n)^T$. Then the right hand side of (5) is simply

$$\|\mathbf{M}\,\mathbf{z}\|^2 . \tag{9}$$

Let $\mathbf{u} = (u_1, u_2, \ldots, u_{m^n})^T$ and $\mathbf{v} = (v_1, v_2, \ldots, v_{m^n})^T$ denote two distinct columns of $\mathbf{M}$. Let $\chi(S)$ be the indicator of the statement S: $\chi(S) = 1$ if S is true and $\chi(S) = 0$ if S is false. Then for any $\alpha \in A$

$$\sum_{i=1}^{m^n} \chi(\alpha = u_i) \;=\; m^{n-1} \quad .$$

Similarly, given $\alpha, \beta \in A$,

$$\sum_{i=1}^{m^n} \chi(\alpha = u_i)\chi(\beta = v_i) \;=\; m^{n-2} \; .$$

Now

$$< \mathbf{u}, \mathbf{v} > \;=\; \sum_{i=1}^{m^n} u_i \, \overline{v_i} \;=\; \sum_{\alpha \in A} \sum_{\beta \in A} \sum_{i=1}^{m^n} \alpha \, \overline{\beta} \, \chi(\alpha = u_i) \; \chi(\beta = v_i) \; .$$

Thus

$$\begin{aligned} < \mathbf{u}, \mathbf{v} > \;&=\; \sum_{\alpha \in A} \sum_{\beta \in A} \alpha \, \overline{\beta} \sum_{i=1}^{m^n} \chi(\alpha = u_i) \; \chi(\beta = v_i) \;=\; \sum_{\alpha \in A} \sum_{\beta \in A} \alpha \, \overline{\beta} \, m^{n-2} = \\ &=\; m^{n-2} \, |\alpha_1 + \alpha_2 + \cdots + \alpha_m|^2 \;=\; 0 \; . \end{aligned} \tag{10}$$

On the other hand,

$$< \mathbf{u}, \mathbf{u} > \;=\; \sum_{\alpha \in A} \sum_{\beta \in A} \alpha \, \overline{\beta} \sum_{i=1}^{m^n} \chi(\alpha = \beta = u_i) \;=\; \sum_{\alpha \in A} |\alpha|^2 \sum_{i=1}^{m^n} \chi(\alpha = u_i) \;=\; m^{n-1} \sum_{\alpha \in A} |\alpha|^2 \; . \tag{11}$$

It follows that

$$\mathbf{M}^* \mathbf{M} \;=\; \left(m^{n-1} \sum_{\alpha \in A} |\alpha|^2 \right) \mathbf{I} \; ,$$

where $\mathbf{M}^*$ is the conjugate transpose of $\mathbf{M}$ and $\mathbf{I}$ is the $n \times n$ identity matrix. Since [3]

$$\|\mathbf{M}\,\mathbf{z}\|^2 \;=\; < \mathbf{M}\,\mathbf{z}, \mathbf{M}\,\mathbf{z} > \;=\; < \mathbf{M}^* \mathbf{M}\,\mathbf{z}, \mathbf{z} > \quad , \tag{12}$$

combining (10), (11) and (12) we have

$$\|\mathbf{M}\,\mathbf{z}\|^2 \;=\; m^{n-1} \left(\sum_{\alpha \in A} |\alpha|^2 \right) < \mathbf{z}, \mathbf{z} > \quad ,$$

which is the content of Theorem 1. □

Proof of Theorem 2: For this proof we take $\mathbf{M}$ to be the $n! \times n$ matrix with rows $(\alpha_{\sigma_1}, \alpha_{\sigma_2}, \ldots, \alpha_{\sigma_n})$, for $\sigma \in \mathcal{S}_n$. Let $\mathbf{z} = (z_1, z_2, \ldots, z_n)^T$. The right hand side of (6) is again given by (9). Let $\mathbf{u} = (u_1, u_2, \ldots, u_{n!})^T$ and $\mathbf{v} = (v_1, v_2, \ldots, v_{n!})^T$ denote two distinct columns of $\mathbf{M}$. Then for any $\alpha \in A$

$$\sum_{i=1}^{n!} \chi(\alpha = u_i) \;=\; (n-1)! \quad ,$$

and for any distinct pair $\alpha, \beta \in A$,

$$\sum_{i=1}^{n!} \chi(\alpha = u_i)\chi(\beta = v_i) \;=\; (n-2)!\ .$$

Similar to the computation of (10) and (11), we find that

$$\begin{aligned} < \mathbf{u}, \mathbf{v} > \;&=\; (n-2)! \sum_{i \neq j} \alpha_i \overline{\alpha_j} \;=\; (n-2)! \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \overline{\alpha_j} \;-\; (n-2)! \sum_{i=1}^{n} \alpha_i \overline{\alpha_i} \\ &=\; (n-2)!\, |\alpha_1 + \alpha_2 + \cdots + \alpha_n|^2 \;-\; (n-2)! \sum_{\alpha \in A} |\alpha|^2 \;=\; -\,(n-2)! \sum_{\alpha \in A} |\alpha|^2 \end{aligned}$$

and

$$< \mathbf{u}, \mathbf{u} >= (n-1)! \sum_{\alpha \in A} |\alpha|^2\ .$$

Thus

$$\mathbf{M}^*\mathbf{M} = \left((n-2)! \sum_{\alpha \in A} |\alpha|^2 \right) (n\mathbf{I} - \mathbf{J})\ ,$$

where $\mathbf{I}$ is the $n \times n$ identity matrix and $\mathbf{J}$ is the $n \times n$ matrix of 1's. Since

$$< \mathbf{Jz}, \mathbf{z} > \;=\; |z_1 + z_2 + \cdots + z_n|^2\ ,$$

we have

$$\|\mathbf{M}\,\mathbf{z}\|^2 \;=\; < \mathbf{M}\,\mathbf{z}, \mathbf{M}\,\mathbf{z} > \;=\; < \mathbf{M}^*\mathbf{M}\,\mathbf{z}, \mathbf{z} > \;=\; \left((n-2)! \sum_{\alpha \in A} |\alpha|^2 \right) < (n\mathbf{I} - \mathbf{J})\mathbf{z}, \mathbf{z} >$$

Consequently

$$\|\mathbf{M}\,\mathbf{z}\|^2 \;=\; n \left((n-2)! \sum_{\alpha \in A} |\alpha|^2 \right) \sum_{i=1}^{n} |z_i|^2 - \left((n-2)! \sum_{\alpha \in A} |\alpha|^2 \right) |z_1 + z_2 + \cdots + z_n|^2\ ,$$

which proves Theorem 2. □

Proof of Theorem 3: If $\mathcal{G}$ is doubly transitive, then the stabilizers of pairs of points are all conjugate subgroups of $\mathcal{G}$. Similarly, the subgroups fixing a point are all conjugates. Thus it makes sense to talk about g_2 and g_1. Let $\mathbf{M}$ to be the $|\mathcal{G}| \times n$ matrix with rows $(\alpha_{\sigma_1}, \alpha_{\sigma_2}, \ldots, \alpha_{\sigma_n})$, for $\sigma \in \mathcal{G}$. Then for any two column vectors $\mathbf{u}, \mathbf{v}$ of $\mathbf{M}$ and $\alpha \in A$

$$\sum_{i=1}^{|\mathcal{G}|} \chi(\alpha = u_i) \;=\; g_1\ ,$$

and for any distinct pair $\alpha, \beta \in A$,

$$\sum_{i=1}^{|\mathcal{G}|} \chi(\alpha = u_i)\chi(\beta = v_i) \;=\; g_2\ .$$

In this case we compute that

$$< \mathbf{u}, \mathbf{v} >= -g_2 \sum_{\alpha \in A} |\alpha|^2 \ , \quad \text{and} \quad < \mathbf{u}, \mathbf{u} >= g_1 \sum_{\alpha \in A} |\alpha|^2 \ .$$

Thus

$$\mathbf{M}^* \mathbf{M} \ = \ \left(\sum_{\alpha \in A} |\alpha|^2 \right) \left((g_1 + g_2) \, \mathbf{I} - g_2 \, \mathbf{J} \right) \ .$$

Therefore

$$\| \mathbf{M} \, \mathbf{z} \|^2 \ = \ < \mathbf{M}^* \mathbf{M} \, \mathbf{z}, \mathbf{z} > \ = \ \left(\sum_{\alpha \in A} |\alpha|^2 \right) \left((g_1 + g_2) \sum_{i=1}^{n} |z_i|^2 - g_2 \, |z_1 + z_2 + \cdots + z_n|^2 \right) \ .$$

Now Theorem 3 follows from the relation

$$g_1 + g_2 = \frac{g_2}{g_1} \, |\mathcal{G}|$$

satisfied by every doubly transitive permutation group $\mathcal{G}$ [4]. □

Remarks

The identities derived here are of the same type as consequences of a general theorem of Brauer & Coxeter [1]:

Theorem 4 *Suppose $\mathcal{G}$ is an absolutely irreducible finite group of homogeneous linear transformations of an n-dimensional complex vector space U. Pick an h-dimensional subspace V_1 together with its complementary subspace W_1, and suppose the pairs $\{(V_1, W_1), (V_2, W_2), \ldots, (V_k, W_k)\}$ form an orbit under $\mathcal{G}$. If $\mathbf{p}_i$ denotes the vector of V_i obtained from a given vector $\mathbf{z} \in U$ by projection parallel to W_i, then*

$$\frac{h}{n} \, \mathbf{z} \ = \ \frac{1}{k} \left(\mathbf{p}_1 + \mathbf{p}_2 + \cdots + \mathbf{p}_k \right) \ . \tag{13}$$

As an example of a special case of this result, Brauer & Coxeter obtain Schönhardt's theorem [8] that if a vector $\mathbf{z}$ in the plane is projected orthogonally on the sides of a regular k-gon, then the arithmetic mean of these k projections is $\mathbf{z}/2$. If in Theorem 4 the group $\mathcal{G}$ and the subspace V_1 can be picked in such a way as to guarantee that the subspaces $V_1, V_2, \ldots, V_k$ are pairwise orthogonal, then $< \mathbf{p}_i, \mathbf{p}_j >= 0$ for $i \neq j$ and from (13) we obtain

$$\frac{h^2 k^2}{n^2} \, \|\mathbf{z}\|^2 \ = \ \sum_{i=1}^{k} \|\mathbf{p}_i\|^2 \ ,$$

which would furnish further identities of the type given here.

Acknowledgement: I would like to thank the referee who pointed out the relevance of the references [1] and [6].

References

[1] R. Brauer and H. S. M. Coxeter, A Generalization of Theorems of Schönhardt and Mehmke on Polytopes, Trans. Royal Society of Canada, 34 (1940), Sec III, pp. 29–34.

[2] D. I. A. Cohen, *Basic Techniques of Combinatorial Theory*, John Wiley & Sons, New York, 1978, p. 34.

[3] K. Hoffman and R. Kunze, *Linear Algebra*, Prentice Hall, Englewood Cliffs, 1961, pp. 237–238.

[4] D. Gorenstein, *Finite Groups*, 2nd edition, Chelsea Publishing Co., New York, 1980, p. 35.

[5] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, corrected and enlarged edition, Academic Press Inc., Orlando, 1980, pp. 30–31.

[6] M. S. Klamkin and V. N. Murty, Generalization of a Complex Number Identity, *College Math. Journal*, 20 (1989), pp. 415–416.

[7] J. Riordan, *An Introduction to Combinatorial Analysis*, Princeton University Press, Princeton, 1978, p. 9.

[8] E. Schönhardt, Deutsche Mathematik, 2 (1937), p. 446.