PACIFIC JOURNAL OF MATHEMATICS
Vol. 149, No. 1, 1991

GENERALIZED CLIFFORD-LITTLEWOOD-ECKMANN GROUPS

TARA L. SMITH

This paper investigates the structure of "generalized Clifford-Littlewood-Eckmann groups", which arise in a number of physical applications. They are a direct generalization of Clifford-Littlewood-Eckmann groups, which have many connections to quadratic forms and classical Clifford algebras. Here we show that any such group decomposes into a central product of factor groups of relatively small order, and that the number of isomorphism types of these factor groups is also small. The determination of the decomposition of these groups allows an easy calculation of many of the properties of the groups as well as of their associated generalized Clifford algebras. These applications will be carried out in subsequent papers.

Introduction. In [LS] we analyzed the structure of those 2-groups which can be presented as $\mathbf{G} = \langle \varepsilon, a_1, \dots, a_r | \varepsilon^2 = 1, a_i^2 = \varepsilon^{k(i)} \ \forall i, a_i a_j = \varepsilon a_j a_i \ \forall i < j, \varepsilon a_i = a_i \varepsilon \ \forall i \rangle$. Any group of this type can be parametrized in terms of the values $s := |\{i: k(i) \equiv 1 \pmod 2\}|$ and $t := |\{i: k(i) \equiv 0 \pmod 2\}|$, and can then be designated by $\mathbf{G} = \mathbf{G}_{s,t}$.

Examples of such groups (or closely related algebraic structures) have appeared in the mathematics and physics literature from the 19th century to the present day. For example, the so-called Dirac group is in fact $\mathbf{G}_{0,4}$, and more generally the groups $\mathbf{G}_{0,2n}$ arise naturally in quantum field theory (see, e.g., [We] and [Lo]). On the other hand, the groups $\mathbf{G}_{r,0}$ are exactly those used by Eckmann [E] in his elegant group-theoretic proof of the theorem of Hurwitz-Radon on the composition of sums of squares ([H1], [H2], [R]). Littlewood [Li] considered the general groups $\mathbf{G}_{s,t}$ in studying sets of anticommuting matrices.

These groups are implicit in Clifford's work on "geometric algebras" [Cl]. In fact, the group $\mathbf{G}_{s,t}$ appears naturally as a subgroup of the group of units of the Clifford algebra $C^{s,t}$ of the quadratic form $s\langle -1\rangle \perp t\langle 1\rangle$. These groups exhibit a "mod 8 periodicity" depending on s and t which parallels the well-known periodicity of the Clifford algebras; moreover, we can derive the Clifford algebra periodicity from that of the groups. Also the decomposition of the Clifford algebras $C^{s,t}$ into tensor products of low-dimensional Clifford algebras has an analogue in the decomposition of the groups $\mathbf{G}_{s,t}$ into central products of such groups of small order. Explicitly, these groups decompose into a product of quaternion and dihedral groups of order 8, cyclic groups of order 4, and Klein-4 groups. The decomposition theory for the groups $\mathbf{G}_{s,t}$ in turn makes it relatively easy to deduce almost all facts about these groups, their representations, and their abelian subgroup structures.

Because of the historical connections, the groups $\mathbf{G}_{s,t}$ are referred to as Clifford-Littlewood-Eckmann groups. In this paper we undertake the analysis of a generalized version of the groups $\mathbf{G}_{s,t}$, where we replace "2" by "n". Specifically, we consider those groups $\mathbf{G}$ which are generated by elements ω, a_i $(1 \leq i \leq r)$ subject to the relations $a_i^n = \omega^{e(i)}$ and $a_i a_j = \omega a_j a_i$ whenever $i < j$, where ω is a (fixed) central element such that $\omega^n = 1$.

If $\mathbf{F}$ is any field which contains a primitive nth root of unity ω', we can consider the finite-dimensional $\mathbf{F}$-algebra $[\mathbf{FG}] := \mathbf{FG}/(\omega - \omega')$. These algebras are so-called "generalized Clifford algebras", which seem to be of considerable interest to physicists. Indeed, collections of papers on generalized Clifford algebras and their connections to problems in physics have appeared in books by Ramakrishnan [**Ra**] and Chisholm and Common [**CC**], and have also been studied by Yamazaki [**Ya**], Morris [**Mo1**, **Mo2**], Popovici-Ghéorghe [**PG**], and Caenepeel and Van Oystaeyen [**CVO**]. The connections to generalized Clifford algebras provide much of the motivation for considering these generalized groups. In [**Sm3**] we use the results obtained here to see how the study of these algebras can often be simplified and clarified by working with the groups. Other applications are considered in [**Sm1**], [**Sm2**].

This paper is devoted to achieving a decomposition theory for these more general groups. We show that any such group decomposes (in an explicitly determined way) into a central product of groups of order n^3 and, if r is odd, one factor of order n^2. This is a direct generalization of the results obtained when $n = 2$. However, the methods required are considerably more technical, and greater care must be taken to be sure things work. The decomposition depends on the (easily determined) center of $\mathbf{G}$ if r is odd, and on $d := \text{g.c.d.}(e(1), \ldots, e(r), n)$, the parity of n, and if n is even, also on $r \pmod 8$ and on the number of i such that $e(i)/d$ is even or odd. These last dependencies are the generalizations of the parametrization of the 2-groups in terms of s and t, and the "mod 8 periodicity" observed there.

1. Building block groups. Our goal is to develop a decomposition theory for the generalized CLE-groups, showing how they can be constructed in a canonical way from certain small "building block groups", just as the CLE-groups discussed in [LS] were. The groups we are investigating here are those which can be presented as

$$\mathbf{G} = \langle \omega, a_1, \ldots, a_r | \omega^n = 1, \ a_i^n = \omega^{e(i)} \ \forall i, \\ a_i a_j = \omega a_j a_i \ \forall i < j, \ \omega a_i = a_i \omega \ \forall i \rangle.$$

As in the $n = 2$ case, we have a central element ω of order n in $\mathbf{G}$, which we intuitively think of as a primitive nth root of 1, and we may refer to the relations $a_i a_j = \omega a_j a_i$ $\forall i < j$ by saying the generators "ω-commute". (Of course, this depends on the particular presentation of $\mathbf{G}$ given, since the ω-commuting relations depend on the order and choice of the generators.) We record several other useful facts about such groups.

PROPOSITION 1.1. *For a group* $\mathbf{G}$ *as above the following hold true*:

(1) $|\mathbf{G}| = n^{r+1}$.

(2) *Let* $z := a_1 a_2^{-1} \cdots a_r^{(-1)^{r-1}}$. *Then* $\mathbf{Z}(\mathbf{G}) = \langle \omega, z \rangle$ *if* $r \equiv 1 \pmod 2$, *and* $\mathbf{Z}(\mathbf{G}) = \langle \omega \rangle$ *if* $r \equiv 0 \pmod 2$.

(3) $\mathbf{Z}(\mathbf{G}) \supseteq \mathbf{G}' = \langle \omega \rangle \cong \mathbb{Z}/n\mathbb{Z}$ *if* $r \geq 2$. *If* $r = 1$, *then* $\mathbf{G}$ *is abelian.*

(4) *Let* $g = \omega^{k_0} a_1^{k_1} \cdots a_r^{k_r} \in \mathbf{G}$. *Then*
$$g^m = \omega^{mk_0} a_1^{mk_1} \cdots a_r^{mk_r} \omega^{[m(m-1)/2] \sum_{i<j} -k_i k_j}.$$

(5) *If* $z \notin \mathbf{Z}(\mathbf{G})$, *i.e. if* $r \equiv 0 \pmod 2$, *then* $z a_i = \omega a_i z$ $\forall i$.

Proof. (1) follows because any element can be uniquely written as $\omega^{k_0} a_1^{k_1} \cdots a_r^{k_r}$, $0 \leq k_i \leq n-1$. (2) is done by calculating the "cost" in factors of ω of commuting each generator a_i across an arbitrary element $g \in \mathbf{G}$. If g is written as in (4) above, e.g., (and assuming $k_0 = 0$), the cost is $\sum_{j<i}(-k_j) + \sum_{j>i}(k_j)$. Setting each "cost" to be 0 (mod n), we get $k_i \equiv -k_{i+1} \pmod n$, $1 \leq i \leq r-1$, and $k_1 \equiv k_r \pmod n$. The only way such equations can be satisfied is if r is odd, and $k_i \equiv -k_{i+1} \pmod n$, $1 \leq i \leq r-1$. By (4) this will be the set of elements generated by ω and z. (4) is an elementary computation done by observing that $(a_1^{k_1} \cdots a_r^{k_r})(a_1^{ck_1} \cdots a_r^{ck_r}) = \omega^{c \sum_{i<j} -k_i k_j}(a_1^{(c+1)k_1} \cdots a_r^{(c+1)k_r})$. That $\langle \omega \rangle = \mathbf{G}'$ is obvious from the

presentation of $\mathbf{G}$, and with (2) the remainder of (3) is clear. Finally, (5) is again seen by an easy computation. □

COROLLARY 1.2. *Let z be as defined above. Then $z^n = \omega^{(-\sum(-1)^i e(i))}$ if $r \equiv 0$ or $1 \pmod 4$, and $z^n = \omega^{-(\sum(-1)^i e(i) + n(n-1)/2)}$ if $r \equiv 2$ or $3 \pmod 4$*

Proof. By (4) above, we see that for g as given,

$$g^n = \omega^{(\sum k_i e(i) - (\sum_{i<j} k_i k_j)(n-1)n/2)}.$$

Now for z, $k_i = (-1)^{i-1}$, and we see that $\sum k_i k_j \equiv 1 \pmod 2$ if $r \equiv 2$ or $3 \pmod 4$, while if $r \equiv 0$ or $1 \pmod 4$, then $\sum k_i k_j \equiv 0 \pmod 2$. The corollary then follows. □

We should remark that if $r \geq 2$, then ω is not essential as a generator, i.e. ω is in the Frattini subgroup $\mathbf{\Phi}$ of $\mathbf{G}$. The key to understanding these groups lies in the fact that any such group decomposes as a central product of groups of this type with two generators $\langle a_1, a_2 \rangle$ or $\langle \omega, a \rangle$, with at most one factor of the latter type occurring. This is proved in Lemma (1.4) below. To simplify notation we will write $\mathbf{G}$ as $\langle \omega, a_1, \dots, a_r \rangle$, and drop the relations. Let $\mathbf{H} = \langle \omega, b_1, \dots, b_s \rangle$, so $\mathbf{G}$ and $\mathbf{H}$ are two groups in the category whose objects are finite groups with a distinguished central element ω of order n and whose morphisms are ω-preserving homomorphisms. Define $\mathbf{G}\dot{\times}\mathbf{H} = \mathbf{GH} := (\mathbf{G}\times\mathbf{H})/(\langle \omega, \omega^{-1} \rangle)$, a central product of two such groups, which again has a distinguished central element $\omega = (\omega, 1) = (1, \omega)$ of order n. (This is exactly analogous to the $n = 2$ case.)

LEMMA 1.3. *Let $\mathbf{G}$ and $\mathbf{H}$ be as given above, and suppose $r \equiv 0 \pmod 2$. Let $z = a_1 a_2^{-1} \cdots a_r^{-1}$. Then $\mathbf{GH}$ can be written in "standard form" as $\langle \omega, zb_1, \dots, zb_s, a_1, \dots, a_r \rangle$, i.e. the generators $zb_1, \dots, zb_s, a_1, \dots, a_r$ "ω-commute".*

Proof. This follows from (5) of Proposition 1.1 above. □

LEMMA 1.4. *Any group $\mathbf{G}$ which can be presented as*

$$\mathbf{G} = \langle \omega, a_1, \dots, a_r | \omega^n = 1,\ a_i^n = \omega^{e(i)}\ \forall i,$$
$$a_i a_j = \omega a_j a_i\ \forall i < j,\ \omega a_i = a_i \omega\ \forall i \rangle$$

decomposes as a central product of groups of this type with two ω-commuting generators and at most one commutative factor generated by ω, z. This factor appears if and only if $r \equiv 1 \pmod 2$.

Proof. We prove the lemma via an induction "by 2" on r. Certainly it is true for $r = 1, 2$.

Claim. If it is true for any $\mathbf{G}$ with r ω-commuting generators $a_1, \dots, a_r$, then it holds true for any $\mathbf{H}$ with $r+2$ ω-commuting generators $b_1, \dots, b_{r+2}$: $\mathbf{H}$ is generated as well by $\{x^{-1}b_1, \dots, x^{-1}b_r, b_{r+1}, b_{r+2}\}$ where $x := b_{r+1}b_{r+2}^{-1}$. Let $a_i := x^{-1}b_i$, $1 \le i \le r$. It is directly seen that $a_ia_j = x^{-1}b_ix^{-1}b_j = \omega x^{-1}b_jx^{-1}b_i = \omega a_ja_i$, $1 \le i < j \le r$, and $a_ib_{r+k} = b_{r+k}a_i$, $k = 1, 2$. Hence $\mathbf{H} = \langle \omega, a_1, \dots, a_r\rangle\langle \omega, b_{r+1}, b_{r+2}\rangle$, and we are done by induction. □

We can now break down our problem of determining canonical decompositions for such groups into a series of steps:

(1) Analyze all two-generator groups.

(2) Determine how the two-generator groups combine under the central product defined above.

(3) Find a set of products of two-generator groups which provides a complete set of irredundant canonical forms for *all* such groups.

(4) Given a "standard" presentation of any such group (i.e. in terms of a set of ω-commuting generators), determine its associated canonical form.

We work on the first two steps in this section, and finish the last two in the next. Before beginning our analysis of the two-generator groups, we record the following useful fact.

LEMMA 1.5. *Let $\mathbf{G}_1 = \langle \omega, a_1, \dots, a_r\rangle$, $\mathbf{G}_2 = \langle \omega', b_1, \dots, b_r\rangle$, and $\mathbf{H} = \langle \omega'', c_1, \dots, c_s\rangle$ be three of our groups in "standard form", with distinguished central nth roots of 1 given by ω, ω', ω'' respectively. Suppose that $\Theta\colon \mathbf{G}_1 \to \mathbf{G}_2$ is an isomorphism of groups with $\Theta(\omega) = \omega'$. Then the two groups $\mathbf{G}_1\dot{\times}\mathbf{H}$ and $\mathbf{G}_2\dot{\times}\mathbf{H}$ are also isomorphic.*

Proof. $(\Theta, 1)\colon \mathbf{G}_1 \times \mathbf{H} \to \mathbf{G}_2 \times \mathbf{H}$ is an isomorphism which sends (ω, ω''^{-1}) to (ω', ω''^{-1}). Hence

$$\mathbf{G}_1\dot{\times}\mathbf{H} := \frac{\mathbf{G}_1 \times \mathbf{H}}{\langle(\omega, \omega''^{-1})\rangle} \quad \text{and} \quad \mathbf{G}_2\dot{\times}\mathbf{H} := \frac{\mathbf{G}_2 \times \mathbf{H}}{\langle(\omega', \omega''^{-1})\rangle}$$

are isomorphic. □

This lemma is important, because we will be working with various "standard forms" for the same group $\mathbf{G}$, and we need to know that we do not have to worry overly much about the choice of distinguished central nth root of 1. We can now determine the isomorphism types of groups for which $r = 1$.

PROPOSITION 1.6. *Let* $\mathbf{G} = \langle \omega, a | \omega^n = 1,\ a^n = \omega^e,\ \omega a = a\omega \rangle$, *and let* $d := \text{g.c.d.}(e, n)$. *Then* $\mathbf{G} \cong \mathbb{Z}/(n^2/d)\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$.

Proof. Write $e = k_1 d$ $\text{g.c.d.}(k_1, n) = 1$. Let k be such that $kk_1 \equiv 1 \pmod{n}$. Then $\mathbf{G} = \langle \omega, a^k | \omega^n = 1,\ a^{kn} = \omega^d,\ \omega a^k = a^k \omega \rangle$. Thus any such group with $r = 1$ can be written as $\mathbf{G} = \langle \omega, b | \omega^n = 1,\ b^n = \omega^d,\ \omega b = b\omega \rangle$ for some divisor d of n. Then $\mathbf{G}$, which is of order n^2, is generated by commuting elements b of order n^2/d and $b^{n/d}\omega^{-1}$ of order d. In particular, we see that $\mathbf{G} \cong \mathbb{Z}/(n^2/d)\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ as claimed. □

COROLLARY 1.7. *Let* $v(n)$ *denote the number of positive divisors of* n. *Then there are precisely* $v(n)$ *isomorphism types of our groups for which* $r = 1$. □

We can now proceed to analyze those groups for which $r = 2$. This becomes considerably more complicated. We must first set up some simplified notation. Let $\mathbf{G}$ be generated by r ω-commuting generators $a_1, \ldots, a_r$ satisfying $a_i^n = \omega^{e_i}$. We will denote this group by $\mathbf{G}(e_1, \ldots, e_r)$ when we are concerned with the way the nth powers of the generators behave, and by $\langle a_1, \ldots, a_r \rangle$ or $\langle \omega, a_1, \ldots, a_r \rangle$ when we are concerned with the generators themselves.

LEMMA 1.8. $\mathbf{G}(e_1, e_2) \cong \mathbf{G}(e_2, e_1)$.

Proof. Let $\mathbf{G}(e_1, e_2) = \langle \omega, a, b \rangle$. By choosing ω^{-1} as the distinguished nth root of 1, instead of ω, we will have $\{b^{-1}, a^{-1}\}$ as a set of ω^{-1}-commuting generators. This gives $\mathbf{G}(e_1, e_2) \cong \mathbf{G}(e_2, e_1)$ as desired. □

LEMMA 1.9. $\mathbf{G}(e_1, e_2) \cong \mathbf{G}(d_1, d_2)$ *where* $d_i := \text{g.c.d.}(e_i, n)$, $i = 1, 2$.

Proof. Let $\mathbf{G} = \mathbf{G}(e_1, e_2) = \langle a_1, a_2 \rangle$. Then $\exists c_i$ such that $c_i e_i \equiv d_i \pmod{n}$, and $\text{g.c.d.}(c_i, n) = 1$, $i = 1, 2$. Taking all exponents to be in $\mathbb{Z}/n\mathbb{Z}$ and choosing $\omega' = \omega^{(c_1 c_2)^{-1}}$ instead of ω as the distinguished

nth root of 1, and $a'_1 = (a_1)^{c_2^{-1}}$ and $a'_2 = (a_2)^{c_1^{-1}}$ as ω'-commuting generators, we see that $(a'_1)^n = \omega^{c_2^{-1}e_1} = \omega'^{c_1 e_1} = \omega'^{d_1}$, and similarly $(a'_2)^n = \omega'^{d_2}$. Thus $\mathbf{G}(e_1, e_2) \cong \mathbf{G}(d_1, d_2)$ as claimed. □

LEMMA 1.10. *Let n be a positive even integer, and let d be a divisor of n. Let $\mathbf{G} = \mathbf{G}(d + \lambda(n/2), d) = \langle \omega, a, b \rangle$. Then the isomorphism type of $\mathbf{G}$ depends on the class of n/d* (mod 4) *and the parity of λ, and is given by the following table.*

$\frac{n}{d}$ (mod 4)	λ (mod 2)	isomorphism-type of $\mathbf{G}$
1, 3	0 or 1	$\mathbf{G}(d, d) \cong \mathbf{G}\left(d + \frac{n}{2}, d\right) \cong \mathbf{G}(n, d) \cong \mathbf{G}(n, \frac{d}{2})$
2	1	$\mathbf{G}\left(d + \frac{n}{2}, d\right) \cong \mathbf{G}(n, d) \cong \mathbf{G}(2d, 2d) \cong \mathbf{G}(n, 2d)$
2	0	$\mathbf{G}(d, d) \left(\not\cong \mathbf{G}\left(d + \frac{n}{2}, d\right)\right)$
0	0 or 1	$\mathbf{G}(d, d) \cong \mathbf{G}\left(d + \frac{n}{2}, d\right) \cong \mathbf{G}(n, d)$

Proof. Notice first that $\mathbf{G} \cong \mathbf{G}(d, d)$ or $\mathbf{G} \cong \mathbf{G}(d + n/2, d)$, accordingly as $\lambda \equiv 0 \pmod 2$ or $\lambda \equiv 1 \pmod 2$. Moreover, $\mathbf{G}(d + n/2, d) = \langle a^*, b^* \rangle = \langle a^* b^{*n-1}, b^* \rangle \cong \mathbf{G}(n, d)$. First suppose that $\frac{n}{d}$ is odd, and let $\mathbf{G}(d, d) \cong \langle a, b \rangle$. Set $a' = ab^{-1+n/d}$. Then a' and b are ω-commuting generators, and $\langle a', b \rangle \cong \mathbf{G}(d + n/2, d)$. Thus we see that in this case, the parity of λ is irrelevant. But we could also choose as ω-commuting generators the elements a' and $a'b$ to give $\mathbf{G} \cong \mathbf{G}(n, d + \frac{n}{2})$. Since g.c.d.$(d + \frac{n}{2}, n) = \frac{d}{2}$, we see by (1.9) that $\mathbf{G} \cong \mathbf{G}(n, \frac{d}{2})$ as well.

Next let us consider the case when $\frac{n}{d} \equiv 2 \pmod 4$. Here the parity of λ comes into play. First assume λ to be odd. Then $\mathbf{G} \cong \mathbf{G}(d + n/2, d) \cong \mathbf{G}(n, d)$. Let $d^* = 2d$, so n/d^* is odd, and $\mathbf{G}(2d, 2d) = \mathbf{G}(d^*, d^*) \cong \mathbf{G}(n, d^*/2) = \mathbf{G}(n, d)$ as well. (Here we are making use of the preceding case.) If instead λ is even, we have $\mathbf{G} \cong \mathbf{G}(d, d)$. We claim that for this case ($\frac{n}{d} = 2 \pmod 4$) $\mathbf{G}_1 := \mathbf{G}(d, d)$ is not isomorphic to $\mathbf{G}_2 := \mathbf{G}(n, d)$. For suppose there were an isomorphism $\Theta\colon \mathbf{G}_1 \to \mathbf{G}_2$. Let $\mathbf{G}_1 = \langle \omega, a, b \rangle$ and $\mathbf{G}_2 = \langle \omega', a', b' \rangle$, and suppose $\Theta(a) = \omega'^e a'^p b'^q$, $\Theta(b) = \omega'^f a'^s b'^t$. Then $\Theta(a)$ and $\Theta(b)$ must generate $\mathbf{G}_2$. Now $\Theta(a)^n = \Theta(a^n) = \Theta(\omega^d) = \Theta(b^n) = \Theta(b)^n$, so $\Theta(a)^n$ and $\Theta(b)^n$ must both be primitive $\frac{n}{d}$th roots of 1. Also, $\Theta(a)^n = \omega'^{ne} a'^{np} b'^{nq} \omega'^{-pqn(n-1)/2} = \omega'^{dq-pqn/2}$. Similarly, $\Theta(b)^n = \omega'^{dt-stn/2}$. Since $\frac{n}{d} \equiv 2 \pmod 4$, we can write $n = 2du$, where u is odd. We must have $dq - pqn/2 = dq - pqdu \equiv md \pmod n$, where g.c.d.$(m, n/d) = 1$, in order for $\Theta(a)^n$ to be a primitive $\frac{n}{d}$th root of unity. Thus we need $q(1-pu)$ to be a unit in $\mathbb{Z}/(n/d)\mathbb{Z}$. In particular, if a prime π divides $\frac{n}{d}$, it cannot divide $1-pu$. If $\pi \neq 2$, then $\pi | \frac{n}{d} \Rightarrow \pi | u \Rightarrow \pi \nmid 1-pu$. If $\pi = 2$, $\pi | \frac{n}{d}$, but $\pi \nmid u$, so if $1-pu$ is to be odd, we must have p even. By the same analysis, s must be even. But then $\langle \Theta(a), \Theta(b) \rangle$ is a subgroup of $\langle \omega', a'^2, b' \rangle$, which is a proper subgroup of $\mathbf{G}_2$, giving a contradiction.

Finally we suppose $\frac{n}{d} \equiv 0 \pmod 4$. We know $\mathbf{G}(d+n/2, d) \cong \mathbf{G}(n, d)$, so we need to show $\mathbf{G}(n, d) \cong \mathbf{G}(d, d)$. Let $\mathbf{G}(n, d) = \langle a^*, b^* \rangle$. Choosing instead $\langle a^* b^{*k}, b^* \rangle$ for some choice of k gives $\mathbf{G}(n, d) \cong \mathbf{G}(k(d-\frac{n}{2}), d)$. Thus $\mathbf{G}(n, d)$ will be seen to be isomorphic to $\mathbf{G}(d, d)$ if we can find a k such that $k(d-\frac{n}{2}) \equiv d \pmod n$. Write $\frac{n}{d} = 4u$, so $\frac{n}{2} = 2ud$. Then $\exists k$ such that $k(d-2ud) \equiv d \pmod n \Leftrightarrow \exists k$ such that $k(1-2u) \equiv 1 \pmod{\frac{n}{d}} \Leftrightarrow (1-2u)$ is a unit in $\mathbb{Z}/(n/d)\mathbb{Z}$. It is a unit, because $\frac{n}{d} = 4u$, so for any prime p, $p | \frac{n}{d} \Rightarrow p | 2u$, and thus $p \nmid (1-2u)$. This gives $\mathbf{G} \cong \mathbf{G}(d, d) \cong \mathbf{G}(n, d)$, and we are done. □

THEOREM 1.11. *There are precisely $v(n)$ distinct isomorphism types of groups $\mathbf{G}(e_1, e_2)$ having order n^3. They are represented by $\mathbf{G}(d^*, d^*)$ where d^* is a divisor of n. The particular value d^* for which $\mathbf{G}(e_1, e_2) \cong \mathbf{G}(d^*, d^*)$ is determined by $d :=$ g.c.d.(e_1, e_2, n), the class of n/d* (mod 4)*, and the parity of e_1e_2/d^2, as given in the following table*:

$\frac{n}{d}$ (mod 4)	$\frac{e_1e_2}{d^2}$ (mod 2)	isomorphism-type of $\mathbf{G}$
0, 1, 3	0 or 1	$\mathbf{G}(d, d)$ ($\cong \mathbf{G}(n, d)$)
2	0	$\mathbf{G}(2d, 2d)$ ($\cong \mathbf{G}(n, d)$)
2	1	$\mathbf{G}(d, d)$ ($\not\cong \mathbf{G}(n, d)$)

Proof. We have seen (1.9) that we can write $\mathbf{G}(e_1, e_2) \cong \mathbf{G}(d_1, d_2)$ where $d_i =$ g.c.d.(e_i, n). Now let $d =$ g.c.d.(d_1, d_2), and write $d_i = k_i d$, $i = 1, 2$. Then k_i divides n, and g.c.d.$(k_1, k_2) = 1$. Notice that if $n/d \equiv 0 \pmod 2$, we must have $k_1 k_2 \equiv e_1 e_2/d^2 \pmod 2$, so for the purposes of our proof, there is no loss of generality in assuming $e_i = d_i$, $i = 1, 2$. Since g.c.d.$(k_1, k_2) = 1$, we can find integers m_1 and m_2 such that $m_1 k_1 + m_2 k_2 = 1$, and we may further assume that g.c.d.$(m_2, n) = 1$. (Write $n = ab$ where g.c.d.$(a, b) = 1$ and a, m_2 have exactly the same prime divisors. Then $k_1 | n \Rightarrow k_1 | b$ since

g. c. d.$(k_1, m_2) = 1$. Then g. c. d.$(m_2 + b, n) = 1$, for if a prime p divides n, then p divides either b or m_2, but not both.) Fix such m_1, m_2. We have $\mathbf{G} = \mathbf{G}(d_1, d_2) = \mathbf{G}(k_1 d, k_2 d) = \langle \omega_0, a_0, b_0 \rangle$. Now choose $\omega' = \omega_0^{m_2^{-1}}$, $a' = a_0^{m_2^{-1}}$, and $b' = a_0^{m_2^{-1} m_1} b_0$ as generators for $\mathbf{G}$, instead of ω_0, a_0, and b_0. Calculating the nth powers of the new generators (by (1.1.4)), we get $\mathbf{G} \cong \mathbf{G}(k_1 d, d - m_1 n(n-1)/2)$. By choosing $\omega'' = \omega'$, $a'' = a' b'^{(1-k_1)}$, and $b'' = b'$, we see finally $\mathbf{G} \cong \mathbf{G}(d + (m_1 + 1)(k_1 - 1)n(n-1)/2, d - m_1 n(n-1)/2)$.

We must now consider several cases, depending on the parities of n and m_1. First, if n is odd, then $n(n-1)/2 \equiv 0 \pmod{n}$, and we see that our result yields $\mathbf{G} \cong \mathbf{G}(d, d)$. Since if $\mathbf{G} = \mathbf{G}(d, d) = \langle a^*, b^* \rangle$, then $a^* b^{*n-1}$, b^* are also ω-commuting generators for $\mathbf{G}$, we see that $\mathbf{G} \cong \mathbf{G}(n, d)$ as well. If n is even, then m_2 must be odd, and we have two possibilities to consider, depending on the parity of m_1. If m_1 is odd, then $\mathbf{G} \cong \mathbf{G}(d, d + n/2)$, so $\mathbf{G} \cong \mathbf{G}(n, d)$ by (1.10). Since $m_1 k_1 + m_2 k_2 = 1$, if both m_1 and m_2 are odd, we must have $k_1 k_2$ even. If m_1 is even, then $\mathbf{G} \cong \mathbf{G}(d + (k_1 + 1)n/2, d)$. Moreover, in this case k_2 must be odd (because $m_1 k_1 + m_2 k_2 = 1$), so $k_1 \equiv k_1 k_2 \pmod{2}$. Then $\mathbf{G} \cong \mathbf{G}(d + n/2, d) \cong \mathbf{G}(n, d)$ if $k_1 k_2$ is even, and $\mathbf{G} \cong \mathbf{G}(d, d)$ if $k_1 k_2$ is odd. Now by a comparison with the chart in (1.10), we obtain the isomorphisms given in the statement of the theorem.

We have seen that any group $\mathbf{G}(e_1, e_2)$ is indeed isomorphic to some $\mathbf{G}(d, d)$, d a divisor of n. We must now show that no two of these groups are isomorphic. This is most easily done by calculating $\mathbf{G}^n = \{g^n | g \in \mathbf{G}\}$ for each $\mathbf{G} = \mathbf{G}(d, d)$. (We remark that by applying (1.1.4) with $m = n$, we can show that for a group $\mathbf{G}(e_1, \dots, e_r)$ of this type, $\mathbf{G}^n = \{g^n | g \in \mathbf{G}\} = \langle g^n | g \in \mathbf{G} \rangle$, i.e. the nth powers in $\mathbf{G}$ actually form a subgroup of $\mathbf{G}$. For by using the Euclidean algorithm and the fact that if $\omega^e = g^n$, then $\omega^{ke} = (g^k)^n$, we see that $\{g^n | g \in \mathbf{G}\} = \{\omega^k | k = e_1 k_1 + \cdots + e_r k_r + \sum_{i<j}(-k_i k_j) n(n-1)/2\} = \langle \omega^{k'} | k' = \text{g.c.d.}(e_1, \dots, e_r, n(n-1)/2) \rangle$.) First let n be odd. Then we see that for $\mathbf{G} = \mathbf{G}(d, d)$, $\mathbf{G}^n = \langle \omega^d \rangle \cong \mathbb{Z}/(n/d)\mathbb{Z}$. Thus if $d \neq d'$, $\mathbf{G}(d, d)$ is not isomorphic to $\mathbf{G}(d', d')$. For the remainder of this proof, we assume n is even. If $\frac{n}{d}$ is odd, we see that for $\mathbf{G} = \mathbf{G}(d, d)$ we have $\mathbf{G}^n = \langle \omega^{d/2} \rangle \cong \mathbb{Z}/(2n/d)\mathbb{Z}$. If $\frac{n}{d}$ is even and $\mathbf{G} = \mathbf{G}(d, d)$, we have $\mathbf{G}^n = \langle \omega^d \rangle \cong \mathbb{Z}/(n/d)\mathbb{Z}$. Thus if $d \neq d'$, the only possibility for $\mathbf{G}(d, d) \cong \mathbf{G}(d', d')$ is if $n/d \equiv 1 \pmod{2}$ and $d' = d/2$. However, in (1.10) we saw that $\mathbf{G}(d, d)$ is isomorphic to $\mathbf{G}(n, d/2)$ and not isomorphic to $\mathbf{G}(d/2, d/2)$ when n/d is odd. □

We are now ready to carry out the second stage of our program, which is to understand how any two of these small groups behave under the central product we defined earlier. We begin with the product of a group of order n^2 with one of order n^3.

LEMMA 1.12. *Let* $d = \text{g.c.d.}(f_1, f_2, f_3, n)$ *and* $\mathbf{G} = \mathbf{G}(f_1, f_2)\mathbf{G}(f_3)$.
(a) *If* $\frac{n}{d} \equiv 0, 1,$ *or* $3 \pmod 4$, *then* $\mathbf{G} \cong \mathbf{G}(d, d)\mathbf{G}(f_3)$.

(b) *If* $\frac{n}{d} \equiv 2 \pmod 4$, *there are two subcases*: *If* $\frac{f_1}{d}$ *and* $\frac{f_2}{d}$ *are odd, but* $\frac{f_3}{d}$ *is even, then* $\mathbf{G} \cong \mathbf{G}(d, d)\mathbf{G}(f_3)$. *In all other cases,* $\mathbf{G} \cong \mathbf{G}(2d, 2d)\mathbf{G}(f_3)$.

Proof. Let $\mathbf{G}_1 := \mathbf{G}(f_1, f_2) = \langle \omega, a, b\rangle$ and $\mathbf{G}_2 := \mathbf{G}(f_3) = \langle \omega, c\rangle$. By (1.3) we have

$$(1) \qquad \mathbf{G}_1\mathbf{G}_2 \cong \langle \omega, a, b, a^{-1}bc\rangle = \mathbf{G}(f_1, f_2, -f_1 + f_2 + f_3 + n(n-1)/2).$$

Working the other way and decomposing, let $\mathbf{H} = \langle \omega, a, b, c\rangle = \mathbf{G}(e_1, e_2, e_3)$. Then

$$(2)\ \mathbf{H} \cong \langle \omega, a, c\rangle\langle \omega, ab^{-1}c\rangle = \mathbf{G}(e_1, e_3)\mathbf{G}(e_1 - e_2 + e_3 + n(n-1)/2).$$

Now let $kd := \text{g.c.d.}(f_1, f_2, n)$, $q_ikd := \text{g.c.d.}(f_i, n)$, $i = 1, 2$, and $qd := \text{g.c.d.}(f_3, n)$, so that $\text{g.c.d.}(q_1, q_2) = 1$ and $\text{g.c.d.}(k, q) = 1$. Then by (1.6) and (1.9) we may write

$$\mathbf{G}(f_1, f_2)\mathbf{G}(f_3) \cong \mathbf{G}(q_1kd, q_2kd)\mathbf{G}(qd).$$

Again we must subdivide into several cases depending on congruence classes of our integers modulo 2 and 4. First let us assume n is odd. Then as we have seen in (1.11), $\mathbf{G}(f_1, f_2) \cong \mathbf{G}(kd, kd)$, and we have

$$\begin{aligned}\mathbf{G} &\cong \mathbf{G}(kd, kd)\mathbf{G}(qd) \cong \mathbf{G}(kd, kd, qd) && \text{by (1)}\\ &\cong \mathbf{G}(kd, qd)\mathbf{G}(qd) && \text{by (2)}\\ &\cong \mathbf{G}(d, d)\mathbf{G}(qd) && \text{by (1.11)}\\ &\cong \mathbf{G}(d, d)\mathbf{G}(f_3) && \text{by (1.6).}\end{aligned}$$

For the remainder of the proof we will assume n to be even. Initially let us also assume $\frac{n}{d}$ is odd, so we may write $\frac{n}{2} = \gamma\frac{d}{2}$ for some odd integer γ. In this case $\frac{n}{kd}$ will also be odd, so $\mathbf{G}(q_1kd, q_2kd) \cong \mathbf{G}(kd, kd)$ by (1.11). Then

$$\begin{aligned}\mathbf{G} &\cong \mathbf{G}(kd, kd)\mathbf{G}(qd) \cong \mathbf{G}(kd, kd, qd + \tfrac{n}{2}) && \text{by (1)}\\ &\cong \mathbf{G}(kd, qd + \tfrac{n}{2})\mathbf{G}(qd) && \text{by (2)}\\ &\cong \mathbf{G}(2k\tfrac{d}{2}, (2q + \gamma)\tfrac{d}{2})\mathbf{G}(qd) \cong \mathbf{G}(d, d)\mathbf{G}(qd) && \text{by (1.11).}\end{aligned}$$

(This last step holds because g. c. d.$(kd, qd + \frac{n}{2}, n) = \frac{d}{2}$, $\frac{n}{d/2} \equiv 2 \pmod 4$ and $2k$ is even.) Thus we see (using (1.6)) that $\mathbf{G} \cong \mathbf{G}(d, d)\mathbf{G}(f_3)$.

Next assume $\frac{n}{d} \equiv 0 \pmod 4$, and write $\frac{n}{2} = 2\gamma d$ for some integer γ. If $\frac{n}{kd} \equiv 0$, 1, or 3 $\pmod 4$, or if $q_1 q_2 \equiv 1 \pmod 2$, then

$$\begin{aligned} \mathbf{G} &\cong \mathbf{G}(kd, kd)\mathbf{G}(qd) && \text{by } (1.11) \\ &\cong \mathbf{G}(kd, kd, qd + \tfrac{n}{2}) && \text{by } (1), \\ &\cong \mathbf{G}(kd, qd + \tfrac{n}{2})\mathbf{G}(qd) && \text{by } (2) \\ &\cong \mathbf{G}(kd, (q + 2\gamma) d)\mathbf{G}(qd) \cong \mathbf{G}(d, d)\mathbf{G}(qd) && \text{by } (1.11). \end{aligned}$$

This last step follows from the fact that g. c. d.$(kd, (q+2\gamma)d, n) = d$. Thus $\mathbf{G} \cong \mathbf{G}(d, d)\mathbf{G}(f_3)$ as claimed. If $\frac{n}{kd} \equiv 2 \pmod 4$ and $q_1 q_2$ is even, then

$$\begin{aligned} \mathbf{G} &\cong \mathbf{G}(2kd, 2kd)\mathbf{G}(qd) && \text{by } (1.11) \\ &\cong \mathbf{G}(2kd, qd + \tfrac{n}{2})\mathbf{G}(qd) && \text{by } (1) \text{ and } (2) \\ &\cong \mathbf{G}(d, d)\mathbf{G}(f_3) && \text{by } (1.11) \text{ and } (1.6). \end{aligned}$$

Again this last step is justified because q is odd in this case (2 divides k), and hence g. c. d.$(2kd, qd + \frac{n}{2}, n) = d$.

Finally we must determine what happens when $\frac{n}{d} \equiv 2 \pmod 4$. Here we may write $\frac{n}{2} = \gamma d$, where γ is an odd integer. Suppose first that either $\frac{n}{kd} \equiv 1 \pmod 2$, or $q_1 q_2 \equiv 1 \pmod 2$ and $\frac{n}{kd} \equiv 2 \pmod 4$. In these cases we have

$$\begin{aligned} \mathbf{G} &\cong \mathbf{G}(kd, kd)\mathbf{G}(qd) && \text{by } (1.11) \\ &\cong \mathbf{G}(kd, qd + \tfrac{n}{2})\mathbf{G}(qd) && \text{by } (1) \text{ and } (2) \\ &\cong \mathbf{G}(kd, (q + \gamma) d)\mathbf{G}(qd). \end{aligned}$$

If k is even, then q is odd, and g. c. d.$(kd, (q + \gamma) d, n) = 2d$, so $\mathbf{G} \cong \mathbf{G}(2d, 2d)\mathbf{G}(qd)$ by (1.11). If both k and q are odd, then $q+\gamma$ is even, and again by (1.11) we see that $\mathbf{G} \cong \mathbf{G}(2d, 2d)\mathbf{G}(qd)$. If k is odd but q is even, then g. c. d.$(kd, (q + \gamma) d, n) = d$ and $k(q + \gamma)$ is odd, so (1.11) shows that in this case we have $\mathbf{G} \cong \mathbf{G}(d, d)\mathbf{G}(qd)$. Notice that in this case $q_1 q_2$ is odd by assumption (k odd $\Rightarrow \frac{n}{kd} \equiv 2 \pmod 4$), and so both f_1/d and f_2/d are odd, while f_3/d is even.

The remaining case is when $\frac{n}{kd} \equiv 2 \pmod 4$ and $q_1 q_2 \equiv 0 \pmod 2$. Now q_i is even $\Leftrightarrow$ f_i/d is even, but g. c. d.$(q_1, q_2) = 1$. Therefore 2 divides precisely one of f_1/d, f_2/d, and we have

$$\begin{aligned} \mathbf{G} &\cong \mathbf{G}(2kd, 2kd)\mathbf{G}(qd) && \text{by } (1.11) \\ &\cong \mathbf{G}(2kd, (q + \gamma) d)\mathbf{G}(qd) && \text{by } (1) \text{ and } (2), \\ &\cong \mathbf{G}(2d, 2d)\mathbf{G}(qd). \end{aligned}$$

The last isomorphism follows because either q is odd, in which case $\text{g.c.d.}(2kd(q+\gamma)\,d, n) = 2d$, or q is even, in which case $\text{g.c.d.}(2kd, (q+\gamma)\,d, n) = d$, but $2k$ is even and again (1.11) shows that $\mathbf{G} \cong \mathbf{G}(2d, 2d)\mathbf{G}(qd)$, and $\mathbf{G}(qd) \cong \mathbf{G}(f_3)$ by (1.6). □

Remarks 1.13. There are two easily seen isomorphisms which may prove useful later on. First, let r be odd. Then $\langle \omega, a_1, \dots, a_r\rangle \cong \langle \omega, a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_r\rangle\langle \omega, z\rangle$, for any i, where $z := a_1 a_2^{-1} \cdots a_r$ as before. Second, $\langle \omega, a, b\rangle\langle \omega, c\rangle \cong \langle \omega, ac, b\rangle\langle \omega, c\rangle$.

These results can be converted to give an analysis of the decomposition of a group of order n^4 into a product of a group of order n^3 and an abelian group of order n^2. We do this next, as it will help in the understanding of the general decomposition theory later on.

Corollary 1.14. *Let* $\mathbf{G} = \mathbf{G}(e, f, g) = \langle a, b, c\rangle$, *and let* $d := \text{g.c.d.}(e, f, g, n)$. *Set* $z = ab^{-1}c$.

(1) *If* $\frac{n}{d} \equiv 0, 1$, *or* $3 \pmod 4$, *then* $\mathbf{G} \cong \mathbf{G}(d, d)\langle \omega, z\rangle$.

(2) *If* $\frac{n}{d} \equiv 2 \pmod 4$, *then* $\mathbf{G} \cong \mathbf{G}(d, d)\langle \omega, z\rangle$ *if at least two of* e/d, f/d, g/d *are odd, and* $\mathbf{G} \cong \mathbf{G}(2d, 2d)\langle \omega, z\rangle$ *if at most two of* e/d, f/d, g/d *are odd.*

Proof. By (1.3), $\mathbf{G}(e, f, g) \cong \mathbf{G}(e, f)\mathbf{G}(e - f + g + n(n-1)/2)$. Let $\delta = \text{g.c.d.}(e, f, e - f + g + n(n-1)/2, n)$, and apply (1.12). Observe that if n is odd, then $\delta = d$, while if n is even, $\delta = d$ when $\frac{n}{d} \equiv 0 \pmod 2$, but $\delta = d/2$ when $\frac{n}{d} \equiv 1 \pmod 2$. Then if $\frac{n}{d}$ is odd and n is odd, we have $\frac{n}{\delta}$ is odd, and (1.12.a) gives $\mathbf{G} \cong \mathbf{G}(\delta, \delta)\langle \omega, z\rangle = \mathbf{G}(d, d)\langle \omega, z\rangle$. If $\frac{n}{d}$ is odd and n is even, we have $\frac{n}{\delta} \equiv 2 \pmod 4$, but e/δ and f/δ are even, so (1.12.b) gives $\mathbf{G} \cong \mathbf{G}(2\delta, 2\delta)\langle \omega, z\rangle = \mathbf{G}(d, d)\langle \omega, z\rangle$. If $\frac{n}{d} \equiv 0 \pmod 4$, then $\delta = d$, and $\mathbf{G} \cong \mathbf{G}(\delta, \delta)\langle \omega, z\rangle$ by (1.12.a). Thus $\mathbf{G} \cong \mathbf{G}(d, d)\langle \omega, z\rangle$ and we are done in this case. Finally we consider the situation when $\frac{n}{d} \equiv 2 \pmod 4$. Again $\delta = d$. By (1.12.b) we know that $\mathbf{G} \cong \mathbf{G}(2d, 2d)\langle \omega, z\rangle$ unless e/d and f/d are odd and

$$(e - f + g + n(n-1)/2)/d$$

is even, in which case g/d must be odd as well. Thus if at most two of e/d, f/d, g/d are odd, then $\mathbf{G} \cong \mathbf{G}(2d, 2d)\langle \omega, z\rangle$, while if all are odd then $\mathbf{G} \cong \mathbf{G}(d, d)\langle \omega, z\rangle$. However, if exactly one of e/d, f/d, g/d is even, then $(e - f + g + n(n-1)/2)/d$ is odd, and we may write $(e - f + g + n(n-1)/2)$ as γd, where γ is odd. Using the fact that $\langle \omega, a, b\rangle\langle \omega, z\rangle \cong \langle \omega, az, b\rangle\langle \omega, z\rangle$, we have that

$\mathbf{G}(d, d)\langle\omega, z\rangle \cong \mathbf{G}((1+\gamma)d, d)\langle\omega, z\rangle$, and since $1+\gamma$ is even, (1.11) shows this is isomorphic to $\mathbf{G}(2d, 2d)\langle\omega, z\rangle$. □

The analysis of the products of two groups of order n^3 is similar in flavor to what we have just done, but it is many times worse in tedious calculations. To simplify things we begin with two charts showing how the groups can be rearranged. The left-hand side gives the ω-commuting generators, and the right-hand side gives the corresponding ω-powers of the nth powers of the generators.

1.15.A

	$\langle a, b\rangle\langle c, d\rangle$	$\mathbf{G}(e, f)\mathbf{G}(g, h)$
(i)	$\langle a, b, a^{-1}bc, a^{-1}bd\rangle$	$\mathbf{G}(e, f, -e+f+g+n(n-1)/2, -e+f+h+n(n-1)/2)$
(ii)	$\langle a, abc, b, a^{-1}bd\rangle$	$\mathbf{G}(e, e+f+g+n(n-1)/2, f, -e+f+h+n(n-1)/2)$
(iii)	$\langle a, abc, abd, b\rangle$	$\mathbf{G}(e, e+f+g+n(n-1)/2, e+f+h+n(n-1)/2, f)$
(iv)	$\langle ab^{-1}c, a, b, a^{-1}bd\rangle$	$\mathbf{G}(e-f+g+n(n-1)/2, e, f, -e+f+h+n(n-1)/2)$
(v)	$\langle ab^{-1}c, a, abd, b\rangle$	$\mathbf{G}(e-f+g+n(n-1)/2, e, e+f+h+n(n-1)/2, f)$
(vi)	$\langle ab^{-1}c, ab^{-1}d, a, b\rangle$	$\mathbf{G}(e-f+g+n(n-1)/2, e-f+h+n(n-1)/2, e, f)$

1.15.B

	$\langle a, b, c, d\rangle$	$\mathbf{G}(e, f, g, h)$
(i)	$\langle a, b\rangle\langle ab^{-1}c, ab^{-1}d\rangle$	$\mathbf{G}(e, f)\mathbf{G}(e-f+g+n(n-1)/2, e-f+h+n(n-1)/2)$
(ii)	$\langle a, c\rangle\langle a^{-1}bc^{-1}, ac^{-1}d\rangle$	$\mathbf{G}(e, g)\mathbf{G}(-e+f-g+n(n-1)/2, e-g+h+n(n-1)/2)$
(iii)	$\langle a, d\rangle\langle a^{-1}bd^{-1}, a^{-1}cd^{-1}\rangle$	$\mathbf{G}(e, h)\mathbf{G}(-e+f-h+n(n-1)/2, -e+g-h+n(n-1)/2)$
(iv)	$\langle b, c\rangle\langle ab^{-1}c, bc^{-1}d\rangle$	$\mathbf{G}(f, g)\mathbf{G}(e-f+g+n(n-1)/2, f-g+h+n(n-1)/2)$
(v)	$\langle b, d\rangle\langle ab^{-1}d, b^{-1}cd^{-1}\rangle$	$\mathbf{G}(f, h)\mathbf{G}(e-f+h+n(n-1)/2, -f+g-h+n(n-1)/2)$
(vi)	$\langle c, d\rangle\langle ac^{-1}d, bc^{-1}d\rangle$	$\mathbf{G}(g, h)\mathbf{G}(e-g+h+n(n-1)/2, f-g+h+n(n-1)/2)$

Note that also $\langle a, b\rangle \cong \langle a^{-1}, b\rangle \cong \langle b, a\rangle \cong \langle b^{-1}, a^{-1}\rangle$, and that $\langle a, b\rangle\langle c, d\rangle \cong \langle c, d\rangle\langle a, b\rangle$. This yields a number of other variations on the isomorphisms given in the charts above. Furthermore, we will often be interested in just the parity of the ω-powers of the nth powers of the generators, which means we can ignore the signs on the right-hand side above, and then there is complete symmetry among $\{e, f, g, h\}$. With this information it is now not too difficult to write down what happens when we take the central product of two groups of order n^3.

LEMMA 1.16. *Let* $\mathbf{G}_1 = \mathbf{G}(e, e), \mathbf{G}_2 = \mathbf{G}(f, f)$, *where* e, f *are divisors of* n, *and let* $d := \text{g.c.d.}(e, f)$. *Set* $e = \alpha d$ *and* $f = \beta d$. *Then* $\mathbf{G}_1\mathbf{G}_2 \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$ *unless* $n/d \equiv 2 \pmod 4$ *and* $\alpha\beta \equiv 1 \pmod 2$, *in which case* $\mathbf{G}_1\mathbf{G}_2 \cong \mathbf{G}(n, n)\mathbf{G}(2d, 2d)$.

Proof. Let $\mathbf{G} := \mathbf{G}(e, e)\mathbf{G}(f, f)$. We consider all cases for $n/d \pmod 4$ and $\alpha\beta \pmod 2$.

(i) Let $n \equiv 1 \pmod 2$. Then

$$\begin{aligned}\mathbf{G} &\cong \mathbf{G}(e, e, f, f) \quad \text{by (1.15.A.i)}\\ &\cong \mathbf{G}(e, f)\mathbf{G}(f, e) \quad \text{by (1.15.B.iv)}\\ &\cong \mathbf{G}(d, d)\mathbf{G}(d, d) \cong \mathbf{G}(n, d)\mathbf{G}(d, n) \quad \text{by (1.11)}\\ &\cong \mathbf{G}(n, n, d, d) \quad \text{by (1.15.A.v)}\\ &\cong \mathbf{G}(n, n)\mathbf{G}(d, d) \quad \text{by (1.15.B.i), as desired.}\end{aligned}$$

(ii) Let $n \equiv 0 \pmod 2$ and $\frac{n}{d} = \gamma$, an odd integer.

$$\begin{aligned}\mathbf{G} &\cong \mathbf{G}(e, e, f + n/2, f + n/2)\\ &\cong \mathbf{G}(e, f + n/2)\mathbf{G}(f, e + n/2) \quad \text{by (1.15.A.i and B.iv)}\\ &\cong \mathbf{G}(2\alpha d/2, (2\beta + \gamma)d/2)\mathbf{G}(2\beta d/2, (2\alpha + \gamma)d/2)\\ &\cong \mathbf{G}(d, d)\mathbf{G}(d, d) \quad \text{by (1.11).}\end{aligned}$$

Now $\mathbf{G}(d, d) \cong \mathbf{G}(n/2, d) \cong \mathbf{G}(d + n/2, n)$, by considering g.c.d.'s and using the results of (1.10) and (1.11). Thus

$$\begin{aligned}\mathbf{G} &\cong \mathbf{G}(n/2, d)\mathbf{G}(d + n/2, n)\\ &\cong \mathbf{G}(n/2, n/2, d, d) \quad \text{by (1.15.a.iv)}\\ &\cong \mathbf{G}(d, d)\mathbf{G}(n, n) \quad \text{by (1.15.B.vi)}.\end{aligned}$$

(iii) Let $n \equiv 0 \pmod 2$ and $\frac{n}{2} = \gamma d$, where γ is an even integer.

$$\begin{aligned}\mathbf{G} &\cong \mathbf{G}(e, f + n/2)\mathbf{G}(f, e + n/2) \quad \text{as in the preceding case}\\ &\cong \mathbf{G}(\alpha d, (\beta + \gamma)d)\mathbf{G}(\beta d, (\alpha + \gamma)d)\\ &\cong \mathbf{G}(d, d)\mathbf{G}(d, d) \quad \text{by consideration of g.c.d.'s}\\ &\cong \mathbf{G}(n/2, d)\mathbf{G}(d + n/2, n) \cong \mathbf{G}(d, d)\mathbf{G}(n, n) \quad \text{exactly as above.}\end{aligned}$$

Again let $\frac{n}{2} = \gamma d$, where now γ is an odd integer.

$$\mathbf{G} \cong \mathbf{G}(e, f + n/2)\mathbf{G}(f, e + n/2) = \mathbf{G}(\alpha d, (\beta + \gamma)d)\mathbf{G}(\beta d, (\alpha + \gamma)d).$$

(iv) Suppose $\alpha\beta \equiv 0 \pmod 2$. Looking at g. c. d.'s shows

$$\begin{aligned} \mathbf{G} &\cong \mathbf{G}(2d, 2d)\mathbf{G}(d, d) \cong \mathbf{G}(d, d)\mathbf{G}(-2d, n) \qquad \text{by } (1.11) \\ &\cong \mathbf{G}(d, n/2, d, n/2) \qquad \text{by } (1.15.\text{A.ii}) \\ &\cong \mathbf{G}(d, n/2)\mathbf{G}(-d + n/2, n) \qquad \text{by } (1.15.\text{B.iii}) \\ &\cong \mathbf{G}(d, n/2)\mathbf{G}(n, -d + n/2) \\ &\cong \mathbf{G}(d, d, n/2, n/2) \qquad \text{by } (1.15.\text{A.iii}) \\ &\cong \mathbf{G}(d, d)\mathbf{G}(n, n) \qquad \text{by } (1.15.\text{B.i}). \end{aligned}$$

(v) Suppose $\alpha\beta \equiv 1 \pmod 2$. We have $\beta + \gamma \equiv \alpha + \gamma \equiv 0 \pmod 2$, so

$$\begin{aligned} \mathbf{G} &\cong \mathbf{G}(2d, 2d)\mathbf{G}(2d, 2d) \\ &\cong \mathbf{G}(n, n)\mathbf{G}(2d, 2d) \qquad \text{as in case (ii).} \end{aligned}$$ □

We now do the reverse of what we have just done. That is, we will determine how one of our groups of order n^5 decomposes into a central product of two groups of order n^3. Once we have finished this task, we will be prepared to tackle the problem of decomposing a general group of this type by means of an induction argument. First we make a useful observation:

REMARK 1.17. Let n be an even integer

(a) $d := \text{g.c.d.}(e, f, g, n) = \text{g.c.d.}(e, f, \pm e \pm f \pm g, n)$.

(b) Let $\delta := \text{g.c.d.}(e, f, \pm e \pm f \pm g + \frac{n}{2}, n)$. Then $\delta = d$ or $2d$ if $\frac{n}{d} \equiv 0 \pmod 2$ (i.e. if $d|\frac{n}{2}$), while $\delta = \frac{d}{2}$ if $\frac{n}{d} \equiv 1 \pmod 2$.

PROPOSITION 1.18. *Let*

$$\mathbf{G} = \mathbf{G}(e_1, e_2, e_3, e_4), \qquad d = \text{g.c.d.}(e_1, e_2, e_3, e_4, n).$$

Let k be the number of i's such that $\frac{e_i}{d}$ is even. Then the isomorphism type of $\mathbf{G}$ is determined by the parity of n, the class of $\frac{n}{d} \pmod 4$, and k if $\frac{n}{d} \equiv 2 \pmod 4$, and is given by the table below.

	$n \pmod 2$	$\frac{n}{d} \pmod 4$	k	iso.-type of $\mathbf{G}$
(i)	1	1 or 3	$0 \le k \le 4$	$\mathbf{G}(n, n)\mathbf{G}(d, d)$
(ii)	0	1 or 3	$0 \le k \le 4$	$\mathbf{G}(n, n)\mathbf{G}(\frac{d}{2}, \frac{d}{2})$
(iii)	0	0	$0 \le k \le 3$	$\mathbf{G}(n, n)\mathbf{G}(d, d)$
(iv)	0	2	0 or 1	$\mathbf{G}(n, n)\mathbf{G}(d, d)$
(iv)	0	2	2 or 3	$\mathbf{G}(n, n)\mathbf{G}(2d, 2d)$

Proof. Let

$$d' := \text{g.c.d.}(e_1, e_2, n),$$

$$c := \text{g.c.d.}(e_1 - e_2 + e_3 + n(n-1)/2, e_1 - e_2 + e_4 + n(n-1)/2, n),$$

$$k_i d' := \text{g.c.d.}(e_i, n), \qquad i = 1, 2, \quad \text{and}$$

$$q_j c := \text{g.c.d.}(e_1 - e_2 + e_j + n(n-1)/2, n), \ j = 3, 4.$$

For all cases we then have $\mathbf{G} \cong \mathbf{G}(k_1 d', k_2 d')\mathbf{G}(q_3 c, q_4 c)$ by (1.15.A.i) and (1.9). (i) $\mathbf{G} \cong \mathbf{G}(d', d')\mathbf{G}(c, c)$ by (1.11), $\cong \mathbf{G}(n, n)\mathbf{G}(d, d)$ by (1.16) since $\text{g.c.d.}(d', c) = d$.

(ii) We have $n/d' \equiv 1 \pmod 2$, $n/c \equiv 2 \pmod 4$, and $q_3 q_4 \equiv 1 \pmod 2$, as $d \nmid q_j c$, $j = 3, 4$, but $\frac{d}{2} | c$. Thus $\mathbf{G} \cong \mathbf{G}(d', d')\mathbf{G}(c, c)$ by (1.11). Now $\text{g.c.d.}(d', c) = d/2$, and $\frac{n}{d/2} \equiv 2 \pmod 4$. Therefore, by (1.16) $\mathbf{G} \cong \mathbf{G}(n, n)\mathbf{G}(d/2, d/2)$.

(iii) We have $\mathbf{G}(k_1 d', k_2 d') \cong \mathbf{G}(2d', 2d')$ if $n/d' \equiv 2 \pmod 4$ and $k_1 k_2 \equiv 0 \pmod 2$, and otherwise $\mathbf{G}(k_1 d', k_2 d') \cong \mathbf{G}(d', d')$. Similar conditions apply for $\mathbf{G}(q_3 c, q_4 c)$. Since $\text{g.c.d.}(d'c) = d$, and $\frac{n}{d} \equiv 0 \pmod 4$, we cannot have both $n/d' \equiv 2 \pmod 4$ and $n/c \equiv 2 \pmod 4$. $\mathbf{G}$ is therefore isomorphic to $\mathbf{G}(d', d')\mathbf{G}(c, c)$ with $\text{g.c.d.}(d', c) = d$; $\mathbf{G}(2d', 2d')\mathbf{G}(c, c)$ with $\text{g.c.d.}(2d', c) = d$; or $\mathbf{G}(d', d')\mathbf{G}(2c, 2c)$ with $\text{g.c.d.}(d', 2c) = d$. In all cases (1.16) gives $\mathbf{G} \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$.

(iv) and (v) Again we begin by analyzing the various possibilities for the isomorphism types of $\mathbf{G}(k_1 d', k_2 d')$ and $\mathbf{G}(q_3 c, q_4 c)$. As before $\mathbf{G}(k_1 d', k_2 d') \cong \mathbf{G}(2d', 2d')$ if $n/d' \equiv 2 \pmod 4$ and $k_1 k_2 \equiv 0 \pmod 2$, and $\cong \mathbf{G}(d', d')$ otherwise. Similarly $\mathbf{G}(q_3 c, q_4 c) \cong \mathbf{G}(2c, 2c)$ or $\mathbf{G}(c, c)$. Suppose $k = 3$. We may assume $2 | (e_1/d)$, (e_2/d), (e_3/d). In this case, $n/d' \equiv 1 \pmod 2$, $n/c \equiv 2 \pmod 4$, and $q_3 q_4$ is even, so $\mathbf{G} \cong \mathbf{G}(d', d')\mathbf{G}(2c, 2c)$. Also $\text{g.c.d.}(d', 2c) = 2d$, so $\mathbf{G} \cong \mathbf{G}(n, n)\mathbf{G}(2d, 2d)$ by (1.16). Next let $k = 2$. We may assume either $2 | (e_1/d)$, (e_2/d) or $2 | (e_1/d)$, (e_3/d). In the first case, we see n/d' and n/c are both odd, and $\text{g.c.d.}(d', c) = 2d$, so $\mathbf{G} \cong \mathbf{G}(d', d')\mathbf{G}(c, c) \cong \mathbf{G}(n, n)\mathbf{G}(2d, 2d)$ as above. In the second case, n/d' and n/c are both $\equiv 2 \pmod 4$ and $k_1 k_2$ and $q_3 q_4$ are both even, so although $\text{g.c.d.}(d', c) = d$, $\mathbf{G} \cong \mathbf{G}(2d', 2d')\mathbf{G}(2c, 2c)$ by (1.11), so $\mathbf{G} \cong \mathbf{G}(n, n)\mathbf{G}(2d, 2d)$ by (1.16). Suppose now $k = 1$. We may assume $2 | (e_1/d)$. In this situation, $\mathbf{G} \cong \mathbf{G}(2d', 2d')\mathbf{G}(c, c)$, and $\text{g.c.d.}(2d', c) = d$, giving $\mathbf{G} \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$ by (1.16). Finally, if $k = 0$, then $n/d' \equiv 2 \pmod 4$, while $n/c \equiv 1 \pmod 2$, and g.c.d.$(d', c) = d$. Again by (1.16) we obtain $\mathbf{G} \cong \mathbf{G}(d', d')\mathbf{G}(c, c) \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$. □

2. The decomposition theorem for general n. We are now ready to complete steps 3 and 4 of our program. The Decomposition Theorem which we prove next is the major result of this paper.

THEOREM 2.1 (*Decomposition Theorem*). *Let* $\mathbf{G} \cong \langle \omega, a_1, \dots, a_r\rangle \cong \mathbf{G}(e_1, \dots, e_r)$. *Let* $d = \text{g.c.d.}(e_1, \dots, e_r, n)$, *and if* r *is odd, let* $e = \text{g.c.d.}(e_1 - e_2 + e_3 - \cdots + e_r + \binom{n}{2}\binom{r}{2}, n)$. *Also let* $s := |\{i\colon e_i/d \equiv 1 \pmod 2\}|$, $t := |\{j\colon e_j/d \equiv 0 \pmod 2\}|$. *The isomorphism type of* $\mathbf{G}$ *is determined by* r *and* d, *and by* e *if* r *is odd, and by* s *and* t *if* $n/d \equiv 2 \pmod 4$. *We have the following*:

(I) *If* $r \equiv 0 \pmod 2$ *then* $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d)$ *except in the following two cases*:

(A) $n \equiv 0 \pmod 2$, $\frac{n}{d} \equiv 1 \pmod 2$, *and* $r \equiv 4$ *or* $6 \pmod 8$, *when* $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d/2, d/2)$.

(B) $n \equiv 0 \pmod 2$, $\frac{n}{d} \equiv 2 \pmod 4$, *and* $t = s \equiv 0$ *or* $2 \pmod 8$, *when* $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(2d, 2d)$.

(II) *If* $r \equiv 1 \pmod 2$ *then* $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d, d)\mathbf{G}(e)$ *except in the following two cases*:

(A) $n \equiv 0 \pmod 2$, $\frac{n}{d} \equiv 1 \pmod 2$, *and* $r \equiv 5 \pmod 8$, *when* $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d/2, d/2)\mathbf{G}(e)$. ($\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2} \cdot \mathbf{G}(d/2, d/2)\mathbf{G}(e)$ *if* $r \equiv 3$ *or* $7 \pmod 8$ *as well*; *then* $\mathbf{G}(d/2, d/2)\mathbf{G}(e) \cong \mathbf{G}(d, d)\mathbf{G}(e)$.)

(B) $n \equiv 0 \pmod 2$, $\frac{n}{d} \equiv 2 \pmod 4$, *and* $t - s \equiv 1, 3$, *or* $7 \pmod 8$, *when* $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(2d, 2d)\mathbf{G}(e)$. ($\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d, d)\mathbf{G}(e)$ *also if* $t - s \equiv 3$ *or* $7 \pmod 8$, *since* $\mathbf{G}(d, d)\mathbf{G}(e) \cong \mathbf{G}(2d, 2d)\mathbf{G}(e)$ *in this case.*)

The groups $\mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d_0, d_0)$ *for* d_0 *a divisor of* n *provide a complete irredundant set of isomorphism types for our groups when* r *is even, while the groups* $\mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d_0, d_0)\mathbf{G}(e_0)$ *for* d_0, e_0 *divisors of* n *provide such a set when* r *is odd, except for the redundancies noted above.*

Proof. We postpone showing uniqueness (irredundancy) until the next proposition. As for the decomposition, all cases are done by an induction on r. Notice that for r odd and z as defined in (1.1.2), $\langle \omega, z\rangle \cong \mathbf{G}(e)$. For r even, set $d' = \text{g.c.d.}(e_1, \dots e_{r-2}, n)$, $\Delta_{r-1} = e_1 - e_2 + \cdots - e_{r-2} + e_{r-1}$, $\Delta_r = e_1 - e_2 + \cdots - e_{r-2} + e_r$. We make the important initial observation that for r even, $\mathbf{G} \cong \langle a_1, \dots, a_{r-2}\rangle\langle a_1a_2^{-1}\cdots a_{r-2}^{-1}a_{r-1}, a_1a_2^{-1}\cdots a_{r-2}^{-1}a_r\rangle$.

We begin with the cases where n is odd, as they are considerably simpler than the even cases. First let r be even. We have seen that the theorem holds for $r = 2, 4$ already. Now suppose it to hold for $r - 2$. By induction and the observation above, we have $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d', d')\mathbf{G}(\Delta_{r-1}, \Delta_r)$. Since $\text{g.c.d.}(d', \Delta_{r-1}, \Delta_r, n) = d$, it is easy to see from (1.9) and (1.16) that $\mathbf{G}(d', d')\mathbf{G}(\Delta_{r-1}, \Delta_r) \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$, so $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d)$ as claimed. If r is odd, then by the result for even r obtained above,

$$\mathbf{G} \cong \mathbf{G}(e_1, e_2, \dots, e_{r-1})\mathbf{G}(e) \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d'', d'')\mathbf{G}(e),$$

where $d'' := \text{g.c.d.}(e_1, \dots, e_{r-1}, n)$. Since $\text{g.c.d.}(d'', e, n) = d$, we see by (1.12) that $\mathbf{G}(d'', d'')\mathbf{G}(e) \cong \mathbf{G}(d, d)\mathbf{G}(e)$, and $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d, d)\mathbf{G}(e)$.

For the remainder of the proof we assume n to be even. For the moment we will also assume r to be even, as the odd cases follow quite easily once the even ones have been proved. Again we know the result holds for $r = 2, 4$. Let $q_i c = \text{g.c.d.}(\Delta_i + \frac{n}{2}\binom{r-1}{2}, n)$, where $i = r-1, r$ and $\text{g.c.d.}(q_{r-1}, q_r) = 1$. Then

$$\begin{aligned}\mathbf{G} &\cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d_1, d_1)\mathbf{G}\left(\Delta_{r-1} + \frac{n}{2}\binom{r-1}{2}, \Delta_r + \frac{n}{2}\binom{r-1}{2}\right) \\ &\cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d_1, d_1)\mathbf{G}(q_{r-1}c, q_r c),\end{aligned}$$

where d_1 depends on d' and the inductive case we are in.

Assume first that $n/d \equiv 1 \pmod 2$. Then $n/d' \equiv 1 \pmod 2$ as well. Assume our result holds for $r - 2 \equiv 2 \pmod 8$. We go through a four-step induction "by 2" on r:

(1) $r \equiv 4 \pmod 8$: $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d', d')\mathbf{G}(q_{r-1}c, q_r c)$. Now $\binom{r-1}{2} \equiv 1 \pmod 2$, so $n/(q_i c) \equiv 2 \pmod 4$, and $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d', d')\mathbf{G}(c, c)$. Also, $\text{g.c.d.}(d', c) = d/2$, so $\mathbf{G}(d', d')\mathbf{G}(c, c) \cong \mathbf{G}(n, n)\mathbf{G}(d/2, d/2)$ by (1.16), and $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d/2, d/2)$.

(2) $r \equiv 6 \pmod 8$: $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d'/2, d'/2)\mathbf{G}(q_{r-1}c, q_r c)$. Here $n/(q_i c) \equiv 1 \pmod 2$, $n/c \equiv 1 \pmod 2$, and $\text{g.c.d.}(d'/2, c) = d/2$. Thus (1.16) again shows $\mathbf{G}(d'/2, d'/2)\mathbf{G}(q_{r-1}c, q_r c) \cong \mathbf{G}(n, n)\mathbf{G}(d/2, d/2)$, so $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d/2, d/2)$.

(3) $r \equiv 0 \pmod 8$: $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d'/2, d'/2)\mathbf{G}(q_{r-1}c, q_r c)$: Now $n/(q_i c) \equiv n/c \equiv 2 \pmod 4$, $\text{g.c.d.}(d'/2, c) = d/2$. By (1.16),

$$\mathbf{G}(d'/2, d'/2)\mathbf{G}(c, c) \cong \mathbf{G}(n, n)\mathbf{G}(d, d), \quad \text{and}$$
$$\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d).$$

(4) $r \equiv 2 \pmod 8$: $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d', d')\mathbf{G}(q_{r-1}c, q_r c)$. We have $n/c \equiv 1 \pmod 2$, g.c.d.$(d', c) = d$. Then $\mathbf{G}(d', d')\mathbf{G}(c, c) \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$ by (1.16), and $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d)$. This completes the proof when $n/d \equiv 1 \pmod 2$.

Next assume $n/d \equiv 2 \pmod 4$. Here there are a number of subcases to consider, since $n/d' \equiv 1 \pmod 4$ and $n/d' \equiv 2 \pmod 4$ are both possible. However, a short reflection allows the reduction to the case when $n/d' \equiv 2 \pmod 4$. For if $d_2 := $ g.c.d.$(e_3, \dots, e_r, n)$, then $d = $ g.c.d.(d', d_2), and either $n/d' \equiv 2 \pmod 4$ or $n/d_2 \equiv 2 \pmod 4$. If $n/d' \not\equiv 2 \pmod 4$, we consider

$$\mathbf{G} \cong \mathbf{G}\left(e_1 - e_3 + \cdots + e_r + \frac{n}{2}\binom{r-1}{2},\right.$$
$$\left. e_2 - e_3 + \cdots + e_r + \frac{n}{2}\binom{r-1}{2}\right)\mathbf{G}(e_3, \dots, e_r),$$

and an analogous argument to that given below will give identical results. Thus we may assume $n/d' \equiv 2 \pmod 4$. We again use an induction on r. Let $t' = |\{j\colon e_j/d \equiv 0 \pmod 2, 1 \le i \le r-2\}|$, $s' = |\{i\colon e_i/d \equiv 1 \pmod 2, 1 \le i \le r-2\}|$. First we analyze $\mathbf{G}(q_{r-1}c, q_r c)$.

(a) $n/c \equiv 1 \pmod 2$ if (i) $r \equiv 0 \pmod 4$ and either $t - s = t' - s' + 2$, $s \equiv 1 \pmod 2$ or $t - s = t' - s - 2$, $s \equiv 0 \pmod 2$, or (ii) $r \equiv 2 \pmod 4$ and either $t - s = t' - s' - 2$, $s \equiv 1 \pmod 2$ or $t - s = t' - s + 2$, $s \equiv 0 \pmod 2$.

(b) $n/c \equiv 2 \pmod 4$ and $q_{r-1}q_r \equiv 1 \pmod 2$ if (i) $r \equiv 0 \pmod 4$ and either $t - s = t' - s' + 2$, $s \equiv 0 \pmod 2$ or $t - s = t' - s - 2$, $s \equiv 1 \pmod 2$, or (ii) $r \equiv 2 \pmod 4$ and either $t - s = t' - s' - 2$, $s \equiv 0 \pmod 2$ or $t - s = t' - s + 2$, $s \equiv 1 \pmod 2$.

(c) $n/c \equiv 2 \pmod 4$ and $q_{r-1}q_r \equiv 0 \pmod 2$ if $t - s = t' - s'$. Then $\mathbf{G}(q_{r-1}c, q_r c) \cong \mathbf{G}(c', c')$, where $n/c' \equiv 1 \pmod 2$ if we are in cases (a) or (c) above, and $n/c' \equiv 2 \pmod 4$ if we are in case (b). We can now apply an induction by 2 on r. Suppose the result holds for $r - 2$. If $t' - s' \equiv 4$ or $6 \pmod 8$, then $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d', d')\mathbf{G}(c', c')$, g.c.d.$(d', c') = d$, and $\mathbf{G}(d', d')\mathbf{G}(c', c') \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$ if in case (a) or (c), $\mathbf{G}(n, n)\mathbf{G}(2d, 2d)$ if in case (b). Thus $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d)$ if $t - s = t' - s' \equiv 4$ or $6 \pmod 8$ (case (c)), or if (case (a)):

(i) $r = t + s = t - s + 2s \equiv 0 \pmod 4$, and if s is odd, $t - s = t' - s' + 2$, while if s is even, $t - s = t' - s' - 2$. If s is odd, we see $2s \equiv 2 \pmod 4$, so $t - s = t' - s' + 2 \equiv 2 \pmod 4$, and since

$t'-s' \equiv 4, 6 \pmod 8$, we see that in this case we must have $t'-s' \equiv 4 \pmod 8$ and $t-s \equiv 6 \pmod 8$. A similar argument shows that if s is even, $t-s \equiv 4 \pmod 8$.

(ii) $r = t+s = t-s+2s \equiv 2 \pmod 4$, and if s is odd, $t-s = t'-s'-2$, while if s is even, $t-s = t'-s'+2$. An argument identical to that above shows here that if s is odd, $t-s \equiv 4 \pmod 8$, while if s is even, $t-s \equiv 6 \pmod 8$.

On the other hand, $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(2d, 2d)$ if we are in case (b):

(iii) $r = t+s = t-s+2s \equiv 0 \pmod 4$, and if s is odd, $t-s = t'-s'-2$, while if s is even, $t-s = t'-s'+2$. This time our argument yields $t-s \equiv 2 \pmod 8$ if s is odd, while $t-s \equiv 0 \pmod 8$ if s is even.

(iv) $r = t+s = t-s+2s \equiv 2 \pmod 4$, and if s is odd, $t-s = t'-s'+2$, while if s is even, $t-s = t'-s'-2$. Here $t-s \equiv 0 \pmod 8$ if s is odd, while $t-s \equiv 2 \pmod 8$ if s is even.

If $t'-s' \equiv 4$ or $t \pmod 8$, then

$$\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(2d', 2d')\mathbf{G}(c', c'),$$

and $\text{g.c.d.}(2d', c') = 2d$ if in case (a) or case (c), $\text{g.c.d.}(2d', c) = d$ if in case (b). Thus in cases (a) and (c) we have

$$\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(2d, 2d),$$

while in case (b) we have $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d)$. Analyzing each possibility as we did above, we see that in cases (a) and (c), $t-s \equiv 0$ or $2 \pmod 8$, while in case (b), $t-s \equiv 4$ or $6 \pmod 8$. This completes the proof for $n/d \equiv 2 \pmod 4$.

Now let us assume that $n/d \equiv 0 \pmod 4$. We have the possibilities that $n/d \equiv 1 \pmod 2$, $2 \pmod 4$, or $0 \pmod 4$. However, by an argument parallel to that in the $n/d \equiv 2 \pmod 4$ situation, we may assume that $n/d' \equiv 0 \pmod 4$, and in fact that $d'/d \equiv 1 \pmod 2$. Then by induction we know

$$\mathbf{G} \cong \mathbf{G}(n, n)^{(r-4)/2}\mathbf{G}(d', d')\mathbf{G}(c', c'),$$

where $\mathbf{G}(c', c') \cong \mathbf{G}(q_{r-1}c, q_rc)$. Moreover, since $d'/d \equiv 1 \pmod 2$, it is easily seen that $\text{g.c.d.}(d', c') = d$. Then by (1.16), we have $\mathbf{G}(d', d')\mathbf{G}(c', c') \cong \mathbf{G}(n, n)\mathbf{G}(d, d)$, and $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d)$, completing the proof for the case when r is even.

We may now assume r to be odd. Since $\exists i$ such that $e_i/d \equiv 1 \pmod 2$, by the remarks in (1.13) we may assume without loss of generality that $d''/d \equiv 1 \pmod 2$, where $d'' = \text{g.c.d.}(e_1, \dots, e_{r-1}, n)$

as before. Suppose first $n/d \equiv 0 \pmod 4$. Then

$$\mathbf{G} \cong \mathbf{G}(e_1, \dots, e_{r-1})\mathbf{G}(e) \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d'', d'')\mathbf{G}(e)$$

by the even case. Since g.c.d.$(d'', e) = d$, we see by (1.12) that $\mathbf{G}(d'', d'')\mathbf{G}(e) \cong \mathbf{G}(d, d)\mathbf{G}(e)$, and $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d, d)\mathbf{G}(e)$.

Next suppose $n/d \equiv 1 \pmod 2$. Then of course $n/d'' \equiv \pmod 2$. We have

$$\mathbf{G} \cong \mathbf{G}(e_1, \dots, e_{r-1})\mathbf{G}(e),$$

which is isomorphic to $\mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d'', d'')\mathbf{G}(e)$ if $r \equiv 1$ or $3 \pmod 8$, and isomorphic to $\mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d''/2, d''/2)\mathbf{G}(e)$ if $r \equiv 5$ or $7 \pmod 8$. If $r \equiv 1 \pmod 4$, then $d|e$. If $r \equiv 3 \pmod 4$, then $d \nmid e$, but $\frac{d}{2}|e$. In both cases g.c.d.$(d'', e) \in \{d, d/2\}$. Using (1.12), we see $\mathbf{G}(d'', d'')\mathbf{G}(e) \cong \mathbf{G}(d, d)\mathbf{G}(e)$ if $r \equiv 1, 3 \pmod 8$, while $\mathbf{G}(d''/2, d''/2)\mathbf{G}(e) \cong \mathbf{G}(d/2, d/2)\mathbf{G}(e)$ if $r \equiv 5 \pmod 8$, but $\mathbf{G}(d''/2, d''/2)\mathbf{G}(e) \cong \mathbf{G}(d, d)\mathbf{G}(e)$ if $r \equiv 7 \pmod 8$. (Note, however, that if $d \nmid e$, i.e. if $r \equiv 3$ or $7 \pmod 8$, then by (1.12) we have $\mathbf{G}(d, d)\mathbf{G}(e) \cong \mathbf{G}(d/2, d/2)\mathbf{G}(e)$.) Thus $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d, d)\mathbf{G}(e)$ if $r \equiv 1, 3$, or $7 \pmod 8$, while $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d/2, d/q)\mathbf{G}(e)$ if $r \equiv 3, 5$, or $7 \pmod 8$, but for $r \equiv 3$ or $7 \pmod 8$, we prefer the first form.

If $n/d \equiv 2 \pmod 4$, we may assume that $n/d'' \equiv 2 \pmod 4$. Let $t_0 := |\{j : e_j/d \equiv 0 \pmod 2,\ 1 \le j \le r-1\}|$, $s_0 := |\{i : e_i/d \equiv 1 \pmod 2,\ 1 \le i \le r-1\}|$. Then $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d'', d'')\mathbf{G}(e)$ if $t_0 - s_0 \equiv 4$ or $6 \pmod 8$, $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(2d'', 2d'')\mathbf{G}(e)$ if $t_0 - s_0 \equiv 0$ or $2 \pmod 8$. Also, $2d|e$ if $s \equiv 1 \pmod 2$, $r \equiv 3 \pmod 4$ or if $s \equiv 0 \pmod 2$, $r \equiv 1 \pmod 4$, while $2d \nmid e$ if $s \equiv 1 \pmod 2$, $r \equiv 1 \pmod 4$ or if $s \equiv 0 \pmod 2$, $r \equiv 3 \pmod 4$. Now $t - s = t_0 - s_0 \pm 1$. Working through each case we see $\mathbf{G}(d'', d'')\mathbf{G}(e) \cong \mathbf{G}(d, d)\mathbf{G}(e)$ for any r, but also

$$\mathbf{G}(d'', d'')\mathbf{G}(e) \cong \mathbf{G}(2d, 2d)\mathbf{G}(e)$$

if $2d \nmid e$ (by (1.12)). This happens if $t - s = t_0 - s_0 \pm 1 = r - 2s \equiv 3 \pmod 4$, i.e. if $t - s \equiv 3$ or $7 \pmod 8$. Then $\mathbf{G}(2d'', 2d'')\mathbf{G}(e) \cong \mathbf{G}(2d, 2d)\mathbf{G}(e)$ for any r, but also $\mathbf{G}(2d'', 2d'')\mathbf{G}(e) \cong \mathbf{G}(d, d)\mathbf{G}(e)$ if $2d \nmid e$, i.e. $t - s \equiv 3 \pmod 4$ as before. Thus we may conclude that $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(2d, 2d)\mathbf{G}(e)$ if $t - s \equiv 1, 3$ or $7 \pmod 8$, while $\mathbf{G} \cong \mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d, d)\mathbf{G}(e)$ if $t - s \equiv 3, 5$, or $7 \pmod 8$, but for $t - s \equiv 3$ or $7 \pmod 8$, we again prefer the first form. □

Once we complete the proof of (2.4), which will show uniqueness of our "canonical forms", we will have completed the proof of the Decomposition Theorem. We summarize the final result in the following corollary.

COROLLARY 2.2. *Any group* $\mathbf{G}$ *which can be presented as*

$$\mathbf{G} = \langle \omega, a_1, \ldots, a_r | \omega^n = 1,\ a_i^n = \omega^{e(i)}\ \forall i, \\ a_i a_j = \omega a_j a_i\ \forall i < j,\ \omega a_i = a_i \omega\ \forall i \rangle$$

can be written in exactly one of the following canonical forms:

(i) $\mathbf{G}(n, n)^{(r-2)/2}\mathbf{G}(d, d)$ *for some* $d|n$ (*if* r *is even*), *or*

(ii) $\mathbf{G}(n, n)^{(r-3)/2}\mathbf{G}(d, d)\mathbf{G}(e)$ *for some* $d, e|n$ (*if* r *is odd*), *where*

$\text{g.c.d.}(d, e) = d$ *if* $n \equiv 1 \pmod 2$,

$\text{g.c.d.}(d, e) \in \{\frac{d}{2}, d\}$ *if* $n \equiv 0 \pmod 2$, $\frac{n}{d} \equiv 1 \pmod 2$,

$\text{g.c.d.}(2d, e) = 2d$ *if* $n \equiv 0 \pmod 2$, $\frac{n}{d} \equiv 2 \pmod 4$, *and*

$\text{g.c.d.}(d, e) = d$ *if* $n \equiv 0 \pmod 2$, $\frac{n}{d} \equiv 0 \pmod 4$.

Proof. The proof of the Decomposition Theorem shows that each group can be written in one of the forms given above. Uniqueness will follow from the next proposition. □

The next proposition calculates the number of elements in $\mathbf{G}$ whose nth powers are 1. Uniqueness of our canonical forms will follow from this, since we will see that the value is different for each of our canonical forms. We can first obtain a partial result on uniqueness by making two elementary observations:

Observations 2.3. (1) If r is odd, then $n^2/e = \exp \mathbf{Z}(\mathbf{G})$, and e is therefore uniquely determined. (2) If $\mathbf{G} \cong \mathbf{G}(n, n)^i\mathbf{G}(d, d)$ or if $\mathbf{G} \cong \mathbf{G}(n, n)^i\mathbf{G}(d, d)\mathbf{G}(e)$ as above, then $\mathbf{G}^n := \{g^n : g \in \mathbf{G}\} = \langle \omega^d \rangle$ if $n/d \equiv 0 \pmod 2$ or $n \equiv 1 \pmod 2$, while $\mathbf{G}^n = \langle \omega^{d/2} \rangle$ if $n/d \equiv 1 \pmod 2$ and $n \equiv 0 \pmod 2$. Thus, at worst $\mathbf{G}(n, n)^i\mathbf{G}(d, d) \cong \mathbf{G}(n, n)^i\mathbf{G}(2d, 2d)$, $\mathbf{G}(n, n)^i\mathbf{G}(d, d)\mathbf{G}(e) \cong \mathbf{G}(n, n)^i\mathbf{G}(2d, 2d)\mathbf{G}(e)$ when $n/d \equiv 2 \pmod 4$. The next proposition will rule out this possibility.

PROPOSITION 2.4. *For any finite group* $\mathbf{G}$, *let* $I_n(\mathbf{G}) = |\{g \in \mathbf{G}: g^n = 1\}|$. *The chart below gives* $I_n(\mathbf{G})$ *for any of our canonical groups* $\mathbf{G}$.

Proof. Let $\mathbf{G}_0 \in \{\mathbf{G}(d, d), \mathbf{G}(d, d)\mathbf{G}(e)\}$, and define integers $p_j(\mathbf{G}_0) = p_j$, $q_j(\mathbf{G}_0) = q_j$ by $p_j = |\{g \in \mathbf{G}(n, n)^j\mathbf{G}_0 : g^n = 1\}|$,

$\mathbf{G}(n, n)^{i-1}\mathbf{G}(d, d)$	$I_n(\mathbf{G})$	$\mathbf{G}(n, n)^{i-1}\mathbf{G}(d, d)\mathbf{G}(e)$	$I_n(\mathbf{G})$
n odd	$n^{2i}d$	n odd, $d \mid e$	$n^{2i+1}d$
n even, $\frac{n}{d} \equiv 1(2)$	$\frac{2^i+1}{2^{i+1}}n^{2i}d$	n even, $\frac{n}{d} \equiv 1(2)$, $d \mid e$	$\frac{2^i+1}{2^{i+1}}n^{2i+1}d$
		n even, $\frac{n}{d} \equiv 1(2)$, $\frac{d}{2} \mid e$, $d \nmid e$	$\frac{1}{2}n^{2i+1}d$
$\frac{n}{d} \equiv 2(4)$	$\frac{2^i-1}{2^i}n^{2i}d$	$\frac{n}{d} \equiv 2(4)$, $2d \mid e$	$\frac{2^i-1}{2^i}n^{2i+1}d$
$\frac{n}{d} \equiv 0(4)$	$n^{2i}d$	$\frac{n}{d} \equiv 0(4)$, $d \mid e$	$n^{2i+1}d$

$q_j = |\{g \in \mathbf{G}(n, n)^j\mathbf{G}_0 \colon g^n = \omega^{n/2}\}|$, where q_j is defined only if n is even. Suppose we know p_j, q_j for some j. Then we can determine p_{j+1}, q_{j+1}. The nth powers of the group $\mathbf{G}(n, n)$ are just $\{1\}$ if n is odd, and $\{1, \omega^{n/2}\}$ if n is even. Thus, if n is odd, $p_{j+1} = n^2p_j$. If n is even, $p_0(\mathbf{G}(n, n)) = (3/4)n^3$, $q_0(\mathbf{G}(n, n)) = (1/4)n^3$, and so $p_{j+1} = (n^2/4)(3p_j + q_j)$, $q_{j+1} = (n^2/4)(3q_j + p_j)$. We can express this recursion formula by

$$\begin{aligned}\begin{pmatrix} p_j \\ q_j \end{pmatrix} &= \frac{n^2}{2^2}\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} p_{j-1} \\ q_{j-1} \end{pmatrix} \\ &= \frac{n^2}{2^2}\begin{pmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} p_{j-1} \\ q_{j-1} \end{pmatrix}\end{aligned}$$

and therefore

$$\begin{aligned}\begin{pmatrix} p_j \\ q_j \end{pmatrix} &= \frac{n^{2j}}{2^{2j}}\begin{pmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{pmatrix}\begin{pmatrix} 2^j & 0 \\ 0 & 2^{2j} \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} p_0 \\ q_0 \end{pmatrix} \\ &= \frac{n^{2j}}{2^{j+1}}\begin{pmatrix} 2^j+1 & 2^j-1 \\ 2^j-1 & 2^j+1 \end{pmatrix}\begin{pmatrix} p_0 \\ q_0 \end{pmatrix}.\end{aligned}$$

In particular, if we can determine p_0, q_0 for all $\mathbf{G}_0 \in \{\mathbf{G}(d, d), \mathbf{G}(d, d)\mathbf{G}(e)\}$, we can determine $I_n(\mathbf{G}(n, n)^{i-1}\mathbf{G}_0)$ by the formulae

$$\begin{aligned}I_n(\mathbf{G}(n, n)^{I-1}\mathbf{G}_0) &= \frac{n^{2i-2}}{2^i}[2^{i-1}(p_0 + q_0) + p_0 - q_0] \quad \text{if } n \text{ is even}, \\ I_n(\mathbf{G}(n, n)^{i-1}\mathbf{G}_0) &= n^{2i-2}p_0 \quad \text{if } n \text{ is odd}.\end{aligned}$$

We now determine p_0, q_0, beginning with the cases when r is even (left-hand side of the chart), as they are simpler. Let $\mathbf{G}_0 = \mathbf{G}(d, d) = \langle \omega, a, b \rangle$, By (1.1.4) we have $(\omega^i a^j b^k)^n = \omega^{ni+(j+k)d+jkn(n-1)/2}$, so $p_0 = |\{(i, j, k) \colon (j+k)d + jkn(n-1)/2 \equiv 0 \pmod n\}|$. First let n be odd. Then $(j+k)d \equiv 0 \pmod n \Leftrightarrow j + k \equiv 0 \pmod{n/d} \Leftrightarrow k = -j + m(n/d)$, $0 \le m \le d - 1$. Therefore there are $n^2 d$ triples (i, j, k) which work, and $p_0 = n^2 d$.

Now let n be even. Then

$$q_0 = |\{(i, j, k) : (j+k)d + jkn(n-1)/2 \equiv n/2 \pmod{n}\}|.$$

First let $n/d \equiv 1 \pmod{2}$. To determine p_0 we must calculate the number of pairs (j, k) satisfying $(j+k)djk(n/2) \equiv 0 \pmod{n}$. We need $jk \equiv 0 \pmod{2}$, $j+k \equiv 0 \pmod{n/d}$. Write $k = -j + m(n/d)$. If $j \equiv 0 \pmod{2}$, any value of m will work. If $j \equiv 1 \pmod{2}$, we must have $m \equiv 1 \pmod{2}$ in order for k to be even. Therefore we see $p_0 = n((n/2)d + (n/2)(d/2)) = (3/4)n^2 d$. For q_0 we need $jk \equiv 1 \pmod{2}$, $j+k \equiv 0 \pmod{n/d}$. Therefore we must have $j \equiv 1 \pmod{2}$ and $m \equiv 0 \pmod{2}$. We then see $q_0 = (1/4)n^2 d$. Next let $n/d \equiv 2 \pmod{4}$, so $d|\frac{n}{2}$. For p_0 we need either $j+k \equiv 0 \pmod{n/d}$ and $jk \equiv 0 \pmod{2}$ or $j+k \equiv n/(2d) \pmod{n/d}$ and $jk \equiv 1 \pmod{2}$. Inspecting these conditions reveals there are $(n/2)d$ pairs (j, k) satisfying the first set, and no pairs satisfying the second set, giving $p_0 = (1/2)n^2 d$. For q_0 we need instead $j+k \equiv 0 \pmod{n/d}$ and $jk \equiv 1 \pmod{2}$ or $j+k \equiv n/(2d) \pmod{n/d}$ and $jk \equiv 0 \pmod{2}$. There are $nd/2$ pairs satisfying the first condition, and nd pairs satisfying the second, so we have $q_0 = (3/2)n^2 d$. Finally, suppose $n/d \equiv 0 \pmod{4}$. The conditions which must be satisfied by the pair (j, k) are the same as in the $n/d \equiv 2 \pmod{4}$ case. In this case we have $nd/2$ possible pairs satisfying each set of conditions, so $p_0 = q_0 = n^2 d$.

Now we consider the case when r is odd. This is considerably more complicated. Let $\mathbf{G}_0 = \mathbf{G}(d, d)\mathbf{G}(e) = \langle \omega, a, b\rangle\langle \omega, c\rangle$. Then $(\omega^i a^j b^k c^h)^n = \omega^{ni+d(j+k)+eh+jkn(n-1)/2}$. We must determine when $d(j+k) + eh + jkn(n-1)/2 \equiv 0$ or $n(n-1)/2 \pmod{n}$. First suppose n to be odd. Then $d|e$, so we may write $e = h'd$ for some integer h'. We want $(j+k+hh')d \equiv 0 \pmod{n}$, so $(j+k+hh') \equiv 0 \pmod{n/d}$. Set $k = -j - hh' + m(n/d)$. There are n possible values for j and h, and d possibilities for m, so $p_0 = n^3 d$. For the rest of the proof n will be even. Suppose first $n/d \equiv 1 \pmod{2}$. To begin with let $d|e$, and write $e = h'd$ as above, so h' is odd. For p_0 we must have $j + k + hh' \equiv 0 \pmod{2}$ and $jk \equiv 0 \pmod{2}$. Again setting $k = -j - hh' + m(n/d)$, we see that if $j \equiv 0 \pmod{2}$, all choices for h and m will work. If $j \equiv 1 \pmod{2}$, k must be even, and so we must have $h \not\equiv m \pmod{2}$, so we have $nd/2$ choices for h and m. This gives $p_0 = (3/4)n^3 d$. For q_0 we need $j + k + hh' \equiv 0 \pmod{2}$ and $jk \equiv 1 \pmod{2}$, which means $j \equiv 1 \pmod{2}$ and $h \equiv m \pmod{2}$. This gives $q_0 = (1/4)n^3 d$. Now suppose still $n/d \equiv 1 \pmod{2}$, but $d \nmid e$. Then $\frac{d}{2}|e$, and we may write $e = h''(d/2)$, where again h'' is odd. For p_0 we must have

$$(2(j+k)+hh'')(d/2)+jk(n/2) \equiv 0 \pmod{n}.$$

There are two ways this can happen: either

$$2(j+k)+hh'' \equiv 0 \pmod{2n/d} \quad \text{and} \quad jk \equiv 0 \pmod{2},$$

or

$$2(j+k)+hh'' \equiv n/d \pmod{2n/d} \quad \text{and} \quad jk \equiv 1 \pmod{2}.$$

Counting possibilities as before reveals that in the first case, there are $(3/8)n^2 d$ triples (j, k, h) which fit the criteria, while in the second case, there are $(1/8)n^2 d$ such triples. Then $p_0 = (1/2)n^3 d$. To calculate q_0, we see that we want either $2(j+k)+hh'' \equiv 0 \pmod{2n/d}$ and $jk \equiv 1 \pmod{2}$, or $2(j+k)+hh'' \equiv n/d \pmod{2n/d}$ and $jk \equiv 0 \pmod{2}$. Here the first case yields $(1/8)n^2 d$ acceptable triples, while the second case gives $(3/8)n^2 d$ triples. This shows $q_0 = (1/2)n^3 d$ as well. Now let $n/d \equiv 2 \pmod{4}$. We have $2d|e$, so write $e = 2h^* d$. We must determine the triples (j, k, h) for which $(j+k+2hh^*)d + jk(n/2) \equiv 0$ or $n/2 \pmod{n}$, to determine p_0 and q_0 respectively. Calculations similar to those done above show $p_0 = (1/2)n^3 d$ and $q_0 = (3/2)n^3 d$. In the final case, where $n/d \equiv 0 \pmod{4}$, $d|e$ and we write $e = h' d$. Here we must determine triples (j, k, h) satisfying $(j+k+hh')d + jk(n/2) \equiv 0$ or $n/2 \pmod{n}$. Again we apply the methods used above, this time deriving $p_0 = q_0 = n^3 d$. From the formula giving $I_n(\mathbf{G})$ in terms of p_0 and q_0, we can now directly obtain the values in the chart, completing the proof. (Notice that for even n, we have calculated q_j as well as p_j, so we have actually determined more than is asserted in the statement of the proposition.) □

COROLLARY 2.5. *Any generalized Clifford-Littlewood-Eckmann group* $\mathbf{G}$ *is isomorphic to* exactly *one of the canonical forms* (*and therefore we are justified in so calling them*).

Proof. We have already seen (2.3) that the only possible duplications are

$$\mathbf{G}(n, n)^{i-1}\mathbf{G}(d, d) \cong \mathbf{G}(n, n)^{i-1}\mathbf{G}(2d, 2d)$$

or

$$\mathbf{G}(n, n)^{i-1}\mathbf{G}(d, d)\mathbf{G}(e) \cong \mathbf{G}(n, n)^{i-1}\mathbf{G}(2d, 2d)\mathbf{G}(e)$$

when $n/d \equiv 2 \pmod 4$, and $2d|e$. However, by examining the chart in the proposition above, we see that

$$I_n(\mathbf{G}(n, n)^{i-1}\mathbf{G}(d, d)) = 2^{-i}(2^i - 1)n^{2i} d,$$

while

$$I_n(\mathbf{G}(n, n)^{i-1}\mathbf{G}(2d, 2d)) = 2^{-i}(2^i + 1)n^{2i} d.$$

As these are not equal, the groups cannot be isomorphic. Similarly,

$$I_n(\mathbf{G}(n, n)^{i-1}\mathbf{G}(d, d)\mathbf{G}(e)) = 2^{-i}(2^i - 1)n^{2i+1} d,$$

but

$$I_n(\mathbf{G}(n, n)^{i-1}\mathbf{G}(d, d)\mathbf{G}(e)) = 2^{-i}(2^i + 1)n^{2i+1} d.$$

These groups are therefore not isomorphic either. □

COROLLARY 2.6. *The isomorphism type of* $\mathbf{G} = \mathbf{G}(e_1, \dots, e_r)$ *depends only on the following*: n, d, *and* r, *and* $\sigma := \sum(-1)^{i+1}e_i$ *if* r *is odd, and* $t-s$ *if* $\frac{n}{d} \equiv 2 \pmod 4$. (*In particular, let* $m_i =$ *the number of* e_j *such that* $e_j = (-1)^{j+1}i$, *and set* $m(\mathbf{G}) = (m_1, m_2, \dots, m_n)$. *Then* $\mathbf{G}$ *depends only on* $m(\mathbf{G})$.).

Proof. The first part is clear from the statement of the Decomposition Theorem. The second part follows because n is the "dimension" of $m(\mathbf{G})$, $d = \text{g.c.d.}(\{i\colon m_i \neq 0\}, n)$, $r = \sum_{i=1}^n m_i$, $\sigma = \sum_{i=1}^n im_i$, $t = \sum_{i/d\equiv 0(2)} m_i$, and $s = \sum_{i/d\equiv 1(2)} m_i$, so all the necessary invariants of $\mathbf{G}$ can be calculated from $m(\mathbf{G})$. (Notice that for $n = 2$, $m_1 = s$ and $m_2 = t$.) □

REFERENCES

[CVO] S. Caenepeel and F. Van Oystaeyen, *A note on generalized Clifford algebras and representations*, preprint, Antwerp, 1986.

[CC] J. S. R. Chisholm and A. K. Common (Editors), *Clifford Algebras and Their Applications in Mathematical Physics*, D. Reidel, 1986.

[Cl] W. K. Clifford, *Mathematical Papers*, Macmillan, London, 1882.

[E] B. Eckmann, *Gruppentheoretischer Beweis des Satzes von Hurwitz-Radon über die Komposition der quadratischen Formen*, Comment. Math. Helv., **15** (1942/43), 358–366.

[H1] A. Hurwitz, *Über die Komposition der quadratischen Formen von Beliebig vielen Variabeln*, Nach. Ges. Wiss. Göttingen, Math.-Phys. K., (1898), 309–316. Reprinted in Math. Werke II, 565–571.

[H2] ——, *Über die Komposition der quadratischen Formen*, Math. Ann., **88** (1923), 1–25. Reprinted in Math. Werke II, 641–666.

[LS] T. Y. Lam and T. L. Smith, *On the Clifford-Littlewood-Eckmann groups*: *A new look at periodicity* mod 8, Rocky Mountain J. Math., **19** (1989), 749–786.

[Li] D. E. Littlewood, *Note on the anticommuting matrices of Eddington*, J. London Math. Soc., **9** (1934), 41–50.

[Lo] J. S. Lomont, *Applications of Finite Groups*, Academic Press, Inc., New York, 1959.

[Mo1] A. O. Morris, *On a generalized Clifford algebra*, Quart. J. Math. Oxford, **18** (1967), 7–12.

[Mo2] ——, *On a generalized Clifford algebra*, II, Quart. J. Math. Oxford, **19** (1968), 289–299.

[PG] I. Popovici and C. Ghéorghe, *Algèbres de Clifford généralisées*, C. R. Acad. Sci. Paris, Sér. A-B, **262** (1966), 682–685.

[R] J. Radon, *Lineare Scharen orthogonaler Matrizen*, Abh. Math. Sem. Univ. Hamburg, **1** (1922), 1–14.

[Ra] A. Ramakrishnan, *L-matrix Theory or the Grammar of Dirac Matrices*, Tata McGraw-Hill Publishing Co., Bombay-New Delhi, 1972.

[Sm1] T. L. Smith, *Some 2-Groups Arising in Quadratic Form Theory and Their Generalizations*, Ph.D. Dissertation, University of California, Berkeley, 1988.

[Sm2] ——, *Generalized Clifford-Littlewood-Eckmann groups* II: *Linear representations and applications*, Pacific J. Math., **149** (1991), 185–199.

[Sm3] ——, *Decomposition of generalized Clifford algebras*, to appear in Quart. J. Math. Oxford.

[We] H. Weyl, *The Theory of Groups and Quantum Mechanics*, Dover Publications, Inc., New York. (Translated by H. P. Robertson from *Gruppentheorie und Quantenmechanik*, 1931.)

[Ya] K. Yamazaki, *On projective representations and ring extensions of finite groups*, J. Fac. Sci. Univ. Tokyo, Sect. I, **10** (1964), 147–195.

Received November 20, 1989. This paper was supported in part by NSF Grant DMS-8908258. This paper is based in part on the author's doctoral dissertation (University of California, Berkeley, 1988).

THE OHIO STATE UNIVERSITY
COLUMBUS, OH 43210-1174