Groups Whose Elements are of Order Two or Three

E. D. Bolker

The American Mathematical Monthly, Vol. 79, No. 9. (Nov., 1972), pp. 1007-1010.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28197211%2979%3A9%3C1007%3AGWEAOO%3E2.0.CO%3B2-S

The American Mathematical Monthly is currently published by Mathematical Association of America.

GROUPS WHOSE ELEMENTS ARE OF ORDER TWO OR THREE

E. D. BOLKER, Bryn Mawr College

In this note we characterize those groups all of whose elements are of order two or three and which contain at least one element of each kind. Call such a group **acceptable.** There are two classes of acceptable groups: some resemble S_3, the symmetric group on three symbols, the others A_4, the alternating group on four. The result, which I state precisely below, is not new; it was first proved by B. H. Neumann in [1] and used by him to settle the Burnside conjecture for $k = 3$: every finitely generated group all of whose elements have order $\leqq k = 3$ is finite. I rediscovered Neumann's theorem while solving a special case of a problem posed in this MONTHLY [2]: Characterize those pairs $A < G$ ("$<$" means "is a subgroup of") for which for all x, $A \cup \{x, x^{-1}\} < G$. When $A = \{e\}$, $A \cup \{x, x^{-1}\} < G$ just when x has order two or three. To solve the problem then means to characterize acceptable groups. There are two reasons for publishing this new proof. First, it is easy and elementary. The little the reader needs to know about group extensions is explained in the course of the argument. Second, recent progress has been made on characterizing groups whose elements have orders less than or equal to five, so it seemed worthwhile to have this easier case accessible.

Let G be a group. Write S (T) for the set of elements of G of order two (three) and, when $R \subseteq G$, write R^* for $R \cup \{e\}$. Then G is acceptable when neither S nor T is empty and $G = S^* \cup T$. Before we can characterize acceptable groups, we must study two almost acceptable cases.

Suppose T is empty, so that every element of G has order two. Then G is abelian and is naturally a vector space over the field $\mathbb{Z}_2$, so that it is characterized by its dimension d. Let Γ be a set of cardinality d; then G is isomorphic to $\perp_\Gamma \mathbb{Z}_2$, the group of functions from Γ to $\mathbb{Z}_2$ each of which is 0 except at finitely many points of Γ.

If S is empty, so that all elements are of order three, then G is said to have exponent three. Finding all such groups is nontrivial. If, however, G is abelian, then it is easy to verify that it is naturally a vector space over $\mathbb{Z}_3$ and hence is just $\perp_\Gamma \mathbb{Z}_3$; the cardinality of Γ determines G. We shall need to know later that, whether or not G is abelian, if it has more than three elements then it contains a subgroup isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$.

We prove that it suffices to find a nontrivial pair of commuting elements. If we knew that G had a finite subgroup with more than three elements that would follow from the well-known nontriviality of the center of such a group. But without that knowledge we proceed as follows. Since G has more than three elements, we can find $x, y \neq e$ with $x \neq y, y^{-1}$. If x and y do not commute, then we shall show that xy and yx do. First note that, by assumption, $e \neq xy \neq yx$. Moreover,

$xy \neq (yx)^{-1}$ because $xy = (yx)^{-1} = x^{-1}y^{-1} = x^2y^2$ implies $e = xy$. Finally, xy and yx commute because

$$(xyyx)(yxxy)^{-1} = (xy^2x)(y^2xy^2) = (xy^2)^3 = e.$$

Now we can build all the acceptable groups.

Groups of type T. Let Γ be a set of given cardinality and let $H = \perp_\Gamma \mathbb{Z}_3$. The map sending each element of H to its inverse is an automorphism of order two, so we can form the semidirect product (splitting extension) $G = H \textcircled{S} \mathbb{Z}_2$ determined by this automorphism: G is the set $H \times \{\pm 1\}$ with multiplication $\langle h, a\rangle\langle k, b\rangle = \langle hk^a, ab\rangle$. Then it is easy to see that G is an acceptable group in which $T^* = H < G$. When Γ has one element, G is isomorphic to S_3.

Groups of type S. Let Γ be a set of given cardinality, V the Klein four-group and $K = \perp_\Gamma V$. A cyclic permutation α of the three nonidentity elements of V is an automorphism of order three of V and hence determines such an automorphism of K. Let G be the semidirect product $K \textcircled{S} \mathbb{Z}_3$ determined by this action. That is, G is the set $K \times \mathbb{Z}_3$ with multiplication $\langle h, a\rangle\langle k, b\rangle = \langle h \cdot \alpha^a(k), a + b\rangle$, where we think of $\mathbb{Z}_3$ as $\{0, 1, 2\}$ under addition modulo three. Then G is an acceptable group in which $S^* = K < G$. When Γ has one element, G is isomorphic to A_4.

We shall show that every acceptable group is of type S or T. We write $a, b, c, \cdots$ (resp. $\cdots x, y, z$) for elements of S (resp. T). When p and q commute, write $p \sim q$. Our argument begins with some elementary observations, clearly true in groups of types S or T, which we prove for an arbitrary acceptable group.

1. $a \nsim x$. (If $ax = xa$, then ax has order six, a contradiction.)
2. $a \sim b \Leftrightarrow ab \in S^*$. ($ab = ba \Rightarrow (ab)^2 = a^2b^2 = e \Rightarrow ab \in S^* \Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.)

Note that in groups of type S we always have $a \sim b$, while in groups of type T, $a \neq b$ implies $a \nsim b$. This motivates the next observation.

3. $\sim$ is transitive on S. (If $ab = ba$ and $bc = cb$ then $b \sim ac$. Hence $ac \notin T$ ($\neq 1$) so $ac \in S^*$ and thus $a \sim c$ ($\neq 2$).)
4. $a \nsim b \Rightarrow ab \in T$ ($\neq 2$) $\Rightarrow$ $ababab = e \Rightarrow aba = bab$.
5. $ay \in S \Rightarrow ayay = e \Rightarrow aya^{-1} = aya = y^{-1}$.
6. $x \sim y \Rightarrow (xy)^3 = x^3y^3 = e \Rightarrow xy \in T^*$.

LEMMA. *If G is acceptable, then either $S^* < G$ or $T^* < G$.*

Proof. If every pair of elements of S commutes then $S^* < G$, and conversely ($\neq 2$), so suppose there is a noncommuting pair and $S^* \not< G$. We shall show that no two distinct elements of S commute. For $a \in S$, let C_a be the centralizer of a. Then $C_a \subset S^*$ ($\neq 1$) and $S^* \neq C_a < G$, for if they were equal, S^* would be a subgroup of G. Suppose $b \nsim a$ and $c \sim a$; we shall show $c = a$ or e. If $c \neq e$, then

since $\sim$ is transitive, $c \nsim b$. Let $d = bcab$. Then

$$(*) \qquad \begin{aligned} da &= bc(aba) \\ &= (bcb)ab \qquad (\#4) \\ &= cbcab \qquad (\#4 \text{ again}) \\ &= cd. \end{aligned}$$

Now $d^2 = e$ because $a \sim c$. If $d \sim a$ then (*) implies $a = c$, while if $d \nsim a$ then

$$\begin{aligned} da &= adad \qquad (\#4) \\ &= acdd \qquad (*) \\ &= ac = ca \end{aligned}$$

so $d = c \sim a$, a contradiction.

Now we can show T^* is closed under multiplication. If $xy \notin T^*$, then $xy \in S$ so $xyxy = e$ and $yxyx = y(xyxy)y^{-1} = e$ and $yx \in S$ as well. We must have $x \nsim y$ lest $xy \in T^*$ $(\#6)$ so $xy \neq yx$ and hence $xy \nsim yx$. Then

$$z = xyyx = xy^2x \notin S^* \ (\#2) \text{ so } e = z^3 = xy^2x^2(y^2x^2)y^2x.$$

But $y^2x^2 = y^{-1}x^{-1} = (xy)^{-1} = xy$ so substituting in the last equation yields

$$e = z^3 = xy^2x^2(xy)y^2x = z$$

so $z = e$, a contradiction. Thus $xy \in T^*$ and $T^* < G$.

THEOREM. *Every acceptable group is of type S or T.*

Proof. We shall show that if S^* $(T^*) < G$ then G is of type S (T). Suppose $T^* < G$. If $a \in S$ and $y \in T$ then $ay \notin T^*$ lest a be in T^*, which is closed under multiplication. Thus $ay \in S$, so, fixing $a \in S$ and applying $\#5$, we see that the map $y \rightsquigarrow aya^{-1} = y^{-1}$ is an automorphism of T^*. Hence T^* is abelian and so is a product $\perp\!\!\!\perp_\Gamma \mathbb{Z}_3$. Now suppose $a, b \notin T^*$. Then $abyb^{-1}a^{-1} = ay^{-1}a^{-1} = y$ so $ab \sim y$. Thus $ab \in T^*$, so T^* is of index two in G, which is therefore a semidirect product of T^* with $\mathbb{Z}_2$, with the induced action $y \rightsquigarrow y^{-1}$ making G of type T.

Suppose, on the other hand, that $S^* < G$. Since S^* is abelian, it is a product $\perp\!\!\!\perp_\Delta \mathbb{Z}_2$. S^* is normal in G; let K be any subgroup of G/S^*. Then K acts on S^* by conjugation. Let R be an orbit of that action; we shall show $R^* < S^*$. Suppose $a, b \in R \neq \{e\}$ and $a \neq b$. Then there is a $y \in G$ with $yS^* \in K$ and $yay^{-1} = b$. Let $c = yby^{-1} \in R$; then $a = ycy^{-1}$ since y has order three. Then $y(abc)y^{-1} = bca = abc \in S^*$. Since $y \sim abc$, $\#1$ implies $abc = e$, so $ab = c$. Thus $R^* < S^*$. Moreover, since no y fixes an $a \in R$, $\#R = \#K$. Now if G/S^* had more than three elements, we could take for K a nine element subgroup and thus produce a

ten element subgroup of S^*. Since every such subgroup has order a power of two, we must have G/S^* isomorphic to $\mathbb{Z}_3$ and for each orbit $R \neq \{e\}$ of the action of $\mathbb{Z}_3$ on S^*, R^* is isomorphic to V and $R^* \textcircled{S} \mathbb{Z}_3$ is isomorphic to A_4 and hence is of type S.

Call a family $\{R_\gamma\}_{\gamma \in \Gamma}$ of orbits **independent** if in the subgroup H of S^* they generate, each element has a unique expansion $\prod_{\gamma \in \Gamma} a_\gamma$ where $a_\gamma \in R_\gamma^*$ and $a_\gamma = e$ for almost all γ. Then $H \textcircled{S} \mathbb{Z}_3$ is of type S. Let Γ index a maximal independent family. Then H is invariant under the action of $\mathbb{Z}_3$ on S^*. If it were a proper subgroup of S^* there would be an orbit R disjoint from H and $\{R_\gamma\} \cup \{R\}$ would be a larger independent family. Thus $H = S^*$ and G is of type S.

References

1. B. H. Neumann, Groups whose elements have bounded orders, J. London Math. Soc., 12 (1937) 195.

2. A. P. Street, Advanced Problem $\neq$ 5742, this MONTHLY, 77 (1970) 655, and 78 (1971) 799.

SUMS OF FINITE SETS OF INTEGERS

MELVIN B. NATHANSON, Southern Illinois University

Let $\mathscr{A}$ be a finite set of integers. The h-fold sum of $\mathscr{A}$, denoted by $h\mathscr{A}$, is the set of all sums of h elements of $\mathscr{A}$, repetitions being allowed. In this note we describe exactly all sufficiently high sums of any finite set of integers.

All latin letters stand for integers, and script letters for finite sets of integers. Denote by $(a_1, a_2, \cdots, a_k)$ the greatest common divisor of $a_1, a_2, \cdots, a_k$. Let $[p, q]$ be the set of integers n such that $p \leqq n \leqq q$. Let $z - \mathscr{D} = \{z - d \mid d \in \mathscr{D}\}$ and $z + \mathscr{D} = \{z + d \mid d \in \mathscr{D}\}$.

THEOREM. *Let $\mathscr{A} = \{a_0, a_1, \cdots, a_k\}$ be a finite set of integers with $a_0 = 0 < a_1 < \cdots < a_k = a$ and $(a_1, a_2, \cdots, a_k) = 1$. Then there exist non-negative integers C and D and sets $\mathscr{C} \subset [0, C-2]$ and $\mathscr{D} \subset [0, D-2]$ such that for all $h \geqq a^2 k$*

$$h\mathscr{A} = \mathscr{C} \cup [C, ha - D] \cup ha - \mathscr{D}. \tag{1}$$

We require the following lemma:

LEMMA. *Let $a_1, a_2, \cdots, a_k = a$ be positive integers with $(a_1, a_2, \cdots, a_k) = 1$. Assume that*

$$(a-1) \sum_{i=1}^{k-1} a_i \leqq n \leqq ha - (k-1)(a-1)a.$$

Then there exist non-negative integers $u_1, u_2, \cdots, u_k$ such that

$$n = u_1 a_1 + u_2 a_2 + \cdots + u_k a_k$$