3-1991

Finite Abelian Groups in which the Probability of an Automorphism Fixing an Element is Large

Gary J. Sherman

Rose-Hulman Institute of Technology

FINITE ABELIAN GROUPS IN WHICH THE PROBABILITY OF AN AUTOMORPHISM FIXING AN ELEMENT IS LARGE

Gary J. Sherman

MS TR 91-01

March 1991

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198 Phone: (812) 877-8391

Finite Abelian Groups in which the Probability of an Automorphism Fixing an Element is Large

Gary J. Sherman

Department of Mathematics
Rose-Hulman Institute of Technology, Terre Haute, IN 47803

Let G be a finite group and let A be its automorphism group. We are concerned with the probability, denoted by $P_A(G)$, that a random element of A fixes a random element of G. It is well known [**3**] that $P_A(G) = k/|G|$ where k is the number of automorphism orbits (For $g \in G$, the automorphism orbit of g is $\{g\sigma|\sigma \in A\}$.) in G. Laffey and MacHale [**2**] have shown that

$$k \leq \begin{cases} |G|/p_s + 1 & \text{if } G \text{ is abelian} \\ |G|/p_s & \text{if } G \text{ is non abelian} \end{cases},$$

where p_s is the smallest prime divisor of $|G|$. Thus

$$\text{(i)} \qquad P_A(G) \leq \begin{cases} 1/p_s + 1/|G| \leq 2/p_s & \text{if } G \text{ is abelian} \\ 1/p_s & \text{if } G \text{ is non-abelian} \end{cases}.$$

The purpose of this note is to show that the abelian groups for which $P_A(G) > 1/p_s$ are $\mathbf{Z}_2, \mathbf{Z}_4$ and $\mathbf{Z_2} \oplus \mathbf{Z_3}$, if $p_s = 2$, and $\mathbf{Z}_{p_s}$, if $p_s \geq 3$. We will refer to such groups as exceptional.

For the remainder of the paper G denotes an abelian group. The following results concerning $P_A(G)$ appear in [**3**].

(ii) If $G \neq \mathbf{Z}_2$, then $P_A(G) \leq 3/4$.

(iii) If G is decomposable, say $G = \bigoplus_{i=1}^{n} G_i$, then, $P_A(G) \leq \prod_{i=1}^{n} P_{A_i}(G_i)$ with equality prevailing if the G_i's are the Sylow subgroups of G.

(iv) If $|G| = p^k$, then $P_A(G) \leq 2 \cdot (3/p^2)^{k/2}$.

(v) If $|G| = p^k$ and G is cyclic, then $P_A(G) = (k+1)/p^k$.

(vi) If $|G| = p^k$ and G is elementary abelian, then $P_A(G) = 2/p^k$.

Fact 1. An exceptional group is a p-group or has order $2^a \cdot 3^b$.

Proof: If $|G|$ is divisible by primes p and q such that $p < q$ and $q \geq 5$ then, $P_A(G) \leq (2/p) \cdot (2/q) < 1/p$ by (i) and (iii).

Fact 2. The only exceptional p-groups for $p \geq 3$ are the cyclic groups of order p.

Proof: Comparing the bounds on $P_A(G)$ given in (i) and (iv), one observes that the bound in (iv) is sharper except for"small" n. Specifically, $1/p < 2 \cdot (3/p^2)^{k/2}$ if, and only if

$$p = 2 \quad \text{and} \quad 1 \leq n \leq 9$$

or

$$p = 3 \quad \text{and} \quad 1 \leq n \leq 3$$

or

$$p = 5 \quad \text{and} \quad 1 \leq n \leq 2$$

or

$$p \geq 7 \quad \text{and} \quad n = 1.$$

But, $P_A(\mathbf{Z}_{27}) = 4/27$, $P_A(\mathbf{Z}_9 \oplus \mathbf{Z}_3) \leq 2/9$, $P_A(\mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3) = 2/27$, $P_A(\mathbf{Z}_9) = 1/3$, $P_A(\mathbf{Z}_3 \oplus \mathbf{Z}_3) = 2/9$, $P_A(\mathbf{Z}_{25}) = 3/25$ and $P_A(\mathbf{Z}_5 \oplus \mathbf{Z}_5) = 2/15$ follow from (iii) through (vi).

Fact 3. The only exceptional group of order $2^a \cdot 3^b$ is $\mathbf{Z}_2 \oplus \mathbf{Z}_3$.

Proof: By the multiplicative property of $P_A(G)$ and Fact 2 we must have $b = 1$ and therefore $P_A(G) = P_A(H) \cdot (2/3)$ where $|H| = 2^a$. Thus $P_A(G) > (1/2)$ implies $P_A(H) > (3/4)$; i.e., $a = 1$.

Fact 4. The only exceptional groups of order 2^a are $\mathbf{Z}_2$ and $\mathbf{Z}_4$.

Proof: We observed in the proof of Fact 2 that $1 \le a \le 9$. Applying (iii) through (vi) to G for $1 \le a \le 4$ yields:

a	G	$P_A(G)$
1	$\mathbf{Z}_2$	$= 1$
2	$\mathbf{Z}_4$	$= 3/4$
	$\mathbf{Z}_2 \oplus \mathbf{Z}_2$	$= 1/2$
3	$\mathbf{Z}_8$	$= 1/2$
	$\mathbf{Z}_4 \oplus \mathbf{Z}_2$	$\le 3/4$
	$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$	$= 1/4$
4	$\mathbf{Z}_{16}$	$= 5/16$
	$\mathbf{Z}_8 \oplus \mathbf{Z}_2$	$\le 1/2$
	$\mathbf{Z}_4 \oplus \mathbf{Z}_4$	$\le 9/16$
	$\mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$	$\le 3/8$
	$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$	$= 1/8$

Thus $\mathbf{Z}_2$ and $\mathbf{Z}_4$ are exceptional and we need to look more closely at $\mathbf{Z}_4 \oplus \mathbf{Z}_2$ and $\mathbf{Z}_4 \oplus \mathbf{Z}_4$.

Consider $G = \mathbf{Z}_4 \oplus \mathbf{Z}_2$. G contains three elements of order two and four elements of order four. Notice that $B_1 = ((1,0),(2,1))$, $B_2 = ((1,0),(0,1))$, $B_3 = ((3,0),(2,1))$, $B_4 = ((1,1),(2,1))$ and $B_5 = ((3,1),(2,1)$ are ordered bases of G ([**1**], page 37). Mapping B_1 to B_i, $2 \le i \le 5$, component by component uniquely determines an automorphism, σ_i of G. Thus the four elements of order four in G form an orbit. Moreover, $(2,1)\sigma_1 = (0,1)$ so there are at most two orbits among the three elements of order two. This implies $P_A(G) \leq 1/2$. Actually $P_A(G) = 1/2$ as one can easily verify by constructing the automorphisms determined by the remaining three ordered bases of G.

Consider $G = \mathbf{Z}_4 \oplus \mathbf{Z}_4$. G contains three elements of order two and twelve elements of order four. As above the elements of order four form an orbit. To see this let a and c be elements of order four in G. By examining the five cyclic subgroups of order four in G one can find elements b and d of order four such that $\langle a \rangle \cap \langle b \rangle = \langle c \rangle \cap \langle d \rangle = \{(0,0)\}$; i. e., such that (a,b) and (c,d) are ordered bases of G. The automorphism determined by these two ordered bases places a and c in the same orbit. It follows that $P_A(G) \leq 5/16$. Actually $P_A(G) = 3/16$ since the elements of order two also form an orbit as one can check with CAYLEY.

Suppose $5 \leq a \leq 9$. If G has an invariant factor of 3 or greater (i.e., $\mathbf{Z}_{2^k}$, $k \geq 3$, is a direct summand of G), then $P_A(G) \leq P_A(\mathbf{Z}_{2^k}) \leq 1/2$. If the invariant factors of G are 2's or 1's, there must be at least two 2's or at least two 1's. In the first case $P_A(G) \leq P_A(\mathbf{Z}_4 \oplus \mathbf{Z}_4) \leq 1/2$ and in the second case $P_A(G) \leq P_A(\mathbf{Z}_2 \oplus \mathbf{Z}_2) = 1/2$.

REFERENCES

1. M. Hall, Jr., The Theory of Groups, Macmillan, New York, 1959.

2. T. J. Laffey and D. MacHale, Automorphism orbits of finite groups, J. Austral. Math. Soc. (Series A), 40 (1986) 253-260.

3. G. J. Sherman, What is the probability an automorphism fixes a group element?, Amer. Math. Monthly 82 (1975) 261-264.