J. Austral. Math. Soc. (Series A) **55** (1993), 414–420

ON MAXIMAL ABELIAN GROUPS OF MAPS

REINHARD WINKLER

(Received 23 July 1991)

Communicated by H. Lausch

Abstract

The paper gives a rather simple description of all maximal abelian subgroups H of the symmetric group S_M acting on an arbitrary set M. In the case of finite M this result is used to determine the maximal cardinality of such an H and the maximal number of permutations without fixed points contained in an abelian subgroup of S_M.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 22 B 35.

Let M be an arbitrary set, $S_M = \{f \mid f : M \to M \text{ bijective}\}$ the symmetric group on M with the composition $\circ$ of maps. Furthermore let P be any partition of M and for every $K \in P$ let $+_K$ be an abelian group operation on K. For every choice $a = (a_K)_{K\in P}$, $a_K \in K$, put $f_a(b) = a_K +_K b$ for $b \in K \in P$. Now define

$$H_{P,(+_K)_{K\in P}} = \{f_a \mid a = (a_K)_{K\in P},\ a_K \in K\}.$$

The following result seems to be familiar to most mathematicians working on group theory. Nevertheless the author could not find it in the literature, even after having consulted many specialists.

THEOREM 1. (a) *$H = H_{P,(+_K)_{K\in P}}$ is an abelian subgroup of S_M and is maximal with respect to this property if and only if P does not contain more than one singleton class.*

(b) *Every maximal abelian subgroup H of S_M is of this form, that is, there exists a partition P containing not more than one singleton class and a family*

$(+_K)_{K\in P}$ *of abelian group operations* $+_K$ *on* K *for every* $K \in P$ *such that* $H = H_{P,(+_K)_{K\in P}}$.

(c) $H_{P_1,(+_K)_{K\in P_1}} = H_{P_2,(\cdot_K)_{K\in P_2}}$ *if and only if* $P_1 = P_2 = P$ *and for every* $K \in P$ *the groups* $\langle K, +_K\rangle$ *and* $\langle K, \cdot_K\rangle$ *are isomorphic by an isomorphism* π_K *having the form* $\pi_K = t_{a_K} \circ \phi_K$, *where* t_{a_K} *is a translation in* $\langle K, +_K\rangle$, *that is,* $t_{a_K}(b) = a_K +_K b$ *for some* $a_K \in K$ *and every* $b \in K$, *and* ϕ_K *is an automorphism of* $\langle K, +_K\rangle$: $\phi_K \in Aut(\langle K, +_K\rangle)$. *Furthermore in this case such a representation of* π_K *is unique, that is,* $t_{a_K^{(1)}} \circ \phi_K^{(1)} = t_{a_K^{(2)}} \circ \phi_K^{(2)}$ *with* $a_K^{(i)} \in K$ *and* $\phi_K^{(i)} \in Aut(\langle K, +_K\rangle)$, $i = 1, 2$, *implies* $t_{a_K^{(1)}} = t_{a_K^{(2)}}$ *(therefore* $a_K^{(1)} = a_K^{(2)}$*) and* $\phi_K^{(1)} = \phi_K^{(2)}$.

PROOF. (a) It is clear that H is an abelian subgroup of S_M.

Firstly suppose that P contains two singleton classes $\{a_1\}$ and $\{a_2\}$. Put $f(a_1) = a_2$, $f(a_2) = a_1$ and $f(c) = c$ for $c \in M \setminus \{a_1, a_2\}$. Of course $h(a_i) = a_i$, $i = 1, 2$, for every $h \in H$, hence $f \circ h = h \circ f$ and $f \notin H$. Thus H is not a maximal abelian subgroup of S_M.

Now let P contain not more than one singleton class and suppose $f \circ h = h \circ f$ for every $h \in H$ and some $f \in S_M$. We have to show $f \in H$. First we prove $f(K) \subseteq K$ for every $K \in P$. To do this assume $f(a) = b \notin K$ for $a \in K$. If the class of b contains more than one element, we can find an $h \in H$ with $h(b) \neq b$. On the other hand there are $h_1, h_2 \in H$ with $h_1(a) = h_2(a)$ but $h_1(b) = b$ and $h_2(b) = h(b)$. Consequently we have the contradiction

$$\begin{aligned} b = h_1(b) &= h_1 \circ f(a) = f \circ h_1(a) = f \circ h_2(a) \\ &= h_2 \circ f(a) = h_2(b) = h(b) \neq b. \end{aligned}$$

Therefore $f(a) = b \in K$, showing $f(K) \subseteq K$. Since this holds for every $K \in P$ and f is one-to-one on M, we have $f' = f|_K \in S(K)$ for every $K \in P$. Now consider $\langle K, +_K\rangle$ with unit element $0 \in K$. Clearly it suffices to show $f(a) = a +_K f(0)$ for every $a \in K$. Take $a \in K$ arbitrarily and consider $h \in H$, $h(b) = b +_K a$ for every $b \in K$. Now we conclude

$$f(a) = f \circ h(0) = h \circ f(0) = f(0) +_K a.$$

If $\{b\} \in P$ is a singleton class our condition yields that the class of a contains other elements and the inverse map f^{-1} does the same job as f in the first case. Hence $f^{-1} \in H$ and, since H is a group, $f \in H$.

(b) Let H be a maximal abelian subgroup of S_M with the partition P given by its transitivity classes, that is, induced by the equivalence

$$a \sim_H b \Leftrightarrow \exists\, h \in H : h(a) = b.$$

https://doi.org/10.1017/S1446788700034145 Published online by Cambridge University Press

Take $K \in P$, $a \in K$ arbitrarily and consider $H' = \{h|_K \mid h \in H\}$. By transitivity of H' on K, for every $b \in K$ there is an $h_b \in H'$ such that $h_b(a) = b$. This h_b is unique, since $h_b(a) = h'_b(a) = b$, $h'_b \in H'$, $c \in K$, $h_c(a) = c$ and $h_c \in H'$ imply

$$h_b(c) = h_b \circ h_c(a) = h_c \circ h_b(a) = h_c \circ h'_b(a) = h'_b \circ h_c(a) = h'_b(c).$$

Now it is clear that $b +_K c = h_b \circ h_c(a)$ defines an abelian group operation $+_K$ on K and that every $h_b \in H'$ allows the representation $h_b(c) = b +_K c$. (Note that in fact $\langle K, +_K\rangle$ and H' are isomorphic by $b \mapsto h_b$.) Therefore it is obvious that $H \subseteq H_{P,(+_K)_{K\in P}}$ and, by maximality, $H = H_{P,(+_K)_{K\in P}}$. By (a) P does not contain more than one singleton class and the proof of (b) is finished.

(c) Since the classes of a partition P of M are the transitivity classes of $H_{P,(+_K)_{K\in P}}$,

$$H_{P_1,(+_K)_{K\in P_1}} = H_{P_2,(\cdot_K)_{K\in P_2}} = H$$

implies $P_1 = P_2$. Therefore we are allowed to restrict our considerations to the case $P_1 = P_2 = \{M\} = \{K\}$. Furthermore clearly

$$\langle M, +_M\rangle \cong H \cong \langle M, \cdot_M\rangle.$$

Thus Theorem 1 follows from the following

LEMMA. *Let $\langle M, +\rangle$ and $\langle M, \cdot\rangle$ be abelian groups, $\pi : \langle M, +\rangle \to \langle M, \cdot\rangle$ an isomorphism, $H = \{t_a \mid a \in M\}$, $H' = \{t'_a \mid a \in M\}$, with $t_a : x \mapsto x + a$, respectively $t'_a : x \mapsto x \cdot a$. Then $H = H'$ if and only if there is an automorphism $\phi \in Aut(\langle M, +\rangle)$ and a translation $t \in H$ such that $\pi = t \circ \phi$. Furthermore in this case such a representation is unique, that is, $\pi = t_1 \circ \phi_1 = t_2 \circ \phi_2$ with $t_i \in H$ and $\phi_i \in Aut(\langle M, +\rangle)$ for $i = 1, 2$ implies $t_1 = t_2$ and $\phi_1 = \phi_2$.*

PROOF. ($\Rightarrow$): If $H = H'$, there is a (one-to-one) correspondence between a and $a' \in M$ such that $t_a = t'_{a'}$, that is, $x + a = x \cdot a'$ for all $x \in M$. Hence

$$a' = \pi(\pi^{-1}(a') + 0) = a' \cdot \pi(0) = a + \pi(0)$$

for all $a \in M$. For arbitrary $x, y = z'$ this implies

$$x \cdot y = x \cdot z' = x + z = x + z' - \pi(0) = x + y - \pi(0).$$

Putting $\phi(x) = \pi(x) - \pi(0)$ and $t(x) = x + \pi(0)$, we obtain $\pi = t \circ \phi$. Since $\phi = t^{-1} \circ \pi$, ϕ is a bijection, and since

$$\begin{aligned}\phi(x+y) &= \pi(x+y) - \pi(0) = \pi(x) \cdot \pi(y) - \pi(0) \\ &= \pi(x) + \pi(y) - \pi(0) - \pi(0) = \phi(x) + \phi(y)\end{aligned}$$

it is an endomorphism, hence an automorphism, proving the assertion.

($\Leftarrow$): Now let $\phi \in \mathrm{Aut}(\langle M, +\rangle)$, $t \in H$ and $\pi = t \circ \phi$, that is, $\pi(x) = \phi(x) + \pi(0)$ for all $x \in M$. Since $y = \pi^{-1}(x)$ if and only if $\pi(y) = x$, if and only if $x = \phi(y) + \pi(0)$, we have

$$\pi^{-1}(x) = y = \phi^{-1}(x - \pi(0)) = \phi^{-1}(x) - \phi^{-1}(\pi(0)).$$

For an arbitrary $t'_{a'}$ this gives

$$\begin{aligned}t'_{a'}(x) = x \cdot a' &= \pi(\pi^{-1}(x \cdot a')) = \pi(\pi^{-1}(x) + \pi^{-1}(a')) \\ &= \phi(\phi^{-1}(x) - \phi^{-1}(\pi(0)) + \phi(\phi^{-1}(a') - \phi^{-1}(\pi(0))) + \pi(0) \\ &= x - \pi(0) + a' - \pi(0) + \pi(0) = x + a' - \pi(0),\end{aligned}$$

which means $t'_{a'} = t_{a'-\pi(0)} \in H$. Thus $H' \subseteq H$. Now pick an arbitrary $t_a \in H$. By the preceding, we know $t_a = t'_{a+\pi(0)} \in H'$, hence also $H \subseteq H'$. Putting both parts together we have the desired equality $H = H'$.

For the proof of the last assertion, let $\pi = t_1 \circ \phi_1 = t_2 \circ \phi_2$, $t_i \in H$ and $\phi_i \in \mathrm{Aut}(\langle M, +\rangle)$ for $i = 1, 2$. This implies

$$t_1(0) = t_1(\phi_1(0)) = t_2(\phi_2(0)) = t_2(0),$$

hence $t_1 = t_2$ and $\phi_1 = t_1^{-1} \circ \pi = t_2^{-1} \circ \pi = \phi_2$. This proves the lemma and, finally, Theorem 1.

In cryptology there is great interest in abelian groups of transformations on finite sets. Maximality is important not only with respect to the set inclusion but also with respect to cardinality. Furthermore transformations without fixed points play an important role. Therefore we finish with the following result.

THEOREM 2. *Consider the following numbers:*

A_n = *Maximal cardinality of an abelian subgroup of the symmetric group* S_n *acting on a set* M *with* n *elements.*

B_n = *Maximal number of maps without fixed points in an abelian subgroup of the group* S_n.

C_n = Maximal probability of choosing a map without fixed points from an abelian subgroup of the group S_n, that is,

$$C_n = \max \frac{1}{|H|} |\{f \in H \mid \forall a \in M : f(a) \neq a\}|,$$

where the maximum is taken over all abelian subgroups H of S_n. Then

(a) $A_1 = 1$, $A_2 = 2$; $A_{3m} = 3^m$, $A_{3m+1} = 3^{m-1}4$ *and* $A_{3m+2} = 3^m 2$ *for* $m \geq 1$.

(b) $B_k = k - 1$ *for* $k = 1, \dots, 7$, $B_{11} = 20$ *and*

$$\begin{array}{lcll} B_{5m+0} & = & 4^m & \text{for } m \geq 1, \\ B_{5m+1} & = & 4^{m-3}3^4 & \text{for } m \geq 3, \\ B_{5m+2} & = & 4^{m-2}3^3 & \text{for } m \geq 2, \\ B_{5m+3} & = & 4^{m-1}3^2 & \text{for } m \geq 1, \\ B_{5m+4} & = & 4^m 3 & \text{for } m \geq 0. \end{array}$$

(c) $C_n = 1 - 1/n$.

PROOF. (a) Using Theorem 1, it is clear how to simplify the subsequent proof of (b) to get a proof of (a). Furthermore statement (a) already has been published and proved originally by Bercov and Moser [1]. We omit details.

(b) f_a, $a = (a_{K_i})_{K_i \in P}$, has no fixed point if and only if every $a_{K_i} \in K_i$, $K_i \in P$, is not the identity in $\langle K_i, +_i \rangle$. Hence by Theorem 2 every maximal abelian subgroup of S_n corresponding to a partition $P = \{K_1, \dots, K_{l_P}\}$ contains exactly

$$\prod_{i=1}^{l_P} (|K_i| - 1)$$

maps without fixed point. Of course we may restrict our considerations to such maximal subgroups. Thus our problem is to find those tuples $(k_1, \dots, k_l)$ of positive integers such that $\prod_{i=1}^{l}(k_i - 1)$ achieves the maximal value under the restriction $\sum_{i=1}^{l} k_i = n$. To do this we establish a list of formulas like

$$(n_1, \dots, n_r) \to (m_1, \dots, m_s)$$

indicating that $\sum_{i=1}^{r} n_i = \sum_{j=1}^{s} m_j$ and $\prod_{i=1}^{r}(n_i - 1) < \prod_{j=1}^{s}(m_j - 1)$.

(i) $(1, k) \to (k + 1)$ for every k

(ii) $(2, k) \to (k + 2)$ for every k

(iii) $(3, 3) \to (6)$

(iv) $(3, 4, 4) \to (5, 6)$

(v) $(3,5) \to (4,4)$
(vi) $(3,6) \to (4,5)$
(vii) $(3,7) \to (5,5)$
(viii) $(4,4,4,4,4) \to (5,5,5,5)$
(ix) $(4,6) \to (5,5)$
(x) $(4,7) \to (5,6)$
(xi) $(5,5,6) \to (4,4,4,4)$
(xii) $(5,7) \to (4,4,4)$
(xiii) $(6,6) \to (4,4,4)$
(xiv) $(6,7) \to (4,4,5)$
(xv) $(7,7) \to (4,5,5)$
(xvi) $(k) \to (\frac{k}{2}, \frac{k}{2})$ for even $k \geq 8$
(xvii) $(k) \to (\frac{k-1}{2}, \frac{k+1}{2})$ for odd $k \geq 9$

The proofs of (i)-(xv) are obvious, (xvi) follows from

$$\left(\frac{k}{2} - 1\right)\left(\frac{k}{2} - 1\right) = \frac{k^2}{4} - k + 1 \geq 2k - k + 1 > k - 1$$

for $k \geq 8$ and (xvii) from a similar computation. Now let us consider $(k_1, \dots, k_l)$ giving the maximal value $\prod_{i=1}^{l}(k_i - 1) = B_n$.

By (i), $k_i = 1$ only in the case $l = n = k_1 = 1$.

By (ii), $k_i = 2$ only in the case $n = k_1 = 2, l = 1$.

By (xvi) and (xvii), $k_i \leq 7$ for all i.

By (iii)-(vii), $k_i = 3$ only in the case $n = 7, l = 2, \{k_1, k_2\} = \{3, 4\}$.

By (viii), there are not more than four indices i_1, i_2, i_3, i_4 with $k_{i_1} = k_{i_2} = k_{i_3} = k_{i_4} = 4$.

By (vi),(ix),(xi),(xiii) and (xiv), $k_i = 6$ only in the cases $n = 6, l = 1, k_1 = 6$ or $n = 11, l = 2, \{k_1, k_2\} = \{5, 6\}$.

By (vii),(x),(xii),(xiv) and (xv), $k_i = 7$ only in the case $n = k_1 = 7, l = 1$.

Hence $1 = 1, 2 = 2, 3 = 3, 4 = 4, 5 = 5, 6 = 6, 7 = 7 = 3 + 4, 8 = 4 + 4, 9 = 4 + 5, 10 = 5 + 5, 11 = 5 + 6, 12 = 4 + 4 + 4, 13 = 4 + 4 + 5, 14 = 4 + 5 + 5,$

$$5m + 0 = 5 + \ldots + 5,$$
$$5m + 1 = 5 + \ldots + 5 + 4 + 4 + 4 + 4,$$
$$5m + 2 = 5 + \ldots + 5 + 4 + 4 + 4,$$
$$5m + 3 = 5 + \ldots + 5 + 4 + 4 \text{ and}$$
$$5m + 4 = 5 + \ldots + 5 + 4$$

https://doi.org/10.1017/S1446788700034145 Published online by Cambridge University Press

for $m \geq 3$ are the partitions giving rise to the corresponding values of B_n claimed in Theorem 2.

(c) The investigated probability corresponding to a partition $P = \{K_1, \dots, K_{l_P}\}$ with $|K_i| = k_i$ is

$$\prod_{i=1}^{l_P}(1 - \frac{1}{k_i}).$$

It is obvious that this value is maximal if l_P is minimal and k_i is maximal. This can be managed for $l_P = 1$ and $K_1 = M$. Now the proof of Theorem 2 is finished.

References

[1] R. Bercov and L. Moser, 'On abelian permutation groups', *Canad. Math. Bull.* **8** (1965), 627–630.

[2] O. Tamaschke, *Permutationsstrukturen* (Bibliographisches Institut, Mannheim–Wien–Zürich, 1969).

[3] H. Wielandt, *Finite Permutation Groups* (Academic Press, New York, 1964).

Institut für Algebra und Diskrete Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8-10
1040 Vienna
AUSTRIA

https://doi.org/10.1017/S1446788700034145 Published online by Cambridge University Press