ON T-SYSTEMS OF GROUPS

M. J. DUNWOODY

(received 5 June 1962)

1. Introduction

Let G be an n-generator group and let $\mathfrak{g} = (g_1, g_2, \cdots, g_n)$ be an ordered set of n elements which generate G, then $\mathfrak{g}$ is called a *generating n-vector of* G. Let Γ_G^n denote the set of all generating n-vectors of G.

If $x_1, x_2, \cdots, x_n$ is a set of generators of the free group F_n of rank n and if α is an automorphism of F_n such that

$$x_i\alpha = w_i(x_1, x_2, \cdots, x_n) \quad \text{for} \quad i = 1, 2, \cdots, n,$$

then the elements

$$g'_i = w_i(g_1, g_2, \cdots, g_n) \quad \text{for} \quad i = 1, 2, \cdots, n$$

define a generating n-vector

$$\mathfrak{g}' = (g'_1, g'_2, \cdots, g'_n).$$

In this way there is assigned to every automorphism α of F_n a permutation α_G of Γ_G^n. If β is an automorphism of G, then a permutation β_G of Γ_G^n is defined by

$$\mathfrak{g}\beta_G = (g_1\beta, g_2\beta, \cdots, g_n\beta).$$

Let P be the group generated by all the permutations of Γ_G^n arising in this way from automorphisms of F_n and automorphisms of G. The transitivity sets of Γ_G^n under P are the *T-systems* of G. The number of T-systems of generating n-vectors of a group G will be denoted by $t_n(G)$. A full discussion of the significance of T-systems can be found in [1].

An abelian group which can be generated by n elements has one T-system of generating n-vectors. In answer to the question — raised by Gaschütz — of whether finite nilpotent groups also have one T-system, B. H. Neumann [2] constructed a finite 2-group which is nilpotent of class 10 and soluble of length 3 and has at least two T-systems of generating 2-vectors. This example led Neumann to ask: "What is the least possible class of a nilpotent group, or the least possible derived length of a soluble group, with more than one T-system?". In this note the following theorem will be proved which completely answers the above question.

THEOREM 1. *To every pair of integers $n > 1$ and $N > 0$ and every prime p, there exists a p-group which is nilpotent of class 2 and has at least N T-systems of generating n-vectors.*

The method devised for proving this theorem does not in general give the exact number of T-systems of a group. In particular the method does not distinguish between the T-systems of some groups for which the Higman criterion does (e.g. Neumann's example in [2]).

In § 2 a lower bound for the number of T-systems of a certain type of group is established by showing that each T-system of such a group can be mapped into a set of transitivity of a certain abelian group under a subgroup of its right regular representation. In § 3, Theorem 1 is proved by calculating this lower bound for some class 2 groups.

The work for this note was carried out while I was receiving generous financial help from the Australian National University in the form of a Research Scholarship.

I thank Professor B. H. Neumann F. R. S. for suggesting this topic. I am greatly indebted to Dr. M. F. Newman who supervised my researches.

2. T_k-systems

The verbal subgroup of a group G generated by all the commutators and all the k-th powers (k a positive integer) of elements of G will be written $V_k(G)$ or, where there is little likelihood of confusion, simply V_k or even V.

For positive integers k, n a group G is said to be a (k, n)-*group* if

(a) G can be generated by n elements

and

(b) G/V_k is the direct product of n cyclic subgroups of order k.

The integers $0, 1, \cdots, k-1$ with operations addition modulo k and multiplication modulo k form a ring which will be denoted R_k. The set of $n \times n$ matrices with elements in R_k also form a ring which will be denoted R_k^n. The determinant of an element A of R_k^n which is an element of R_k will be denoted det A. The elements of R_k which are coprime to k form a group Λ_k under multiplication modulo k. The set of $n \times n$ matrices of R_k^n with determinants in Λ_k also form a group (see, for example, [3], Theorem 37, p. 185) which will be denoted Λ_k^n.

In the remainder of this section G will denote a finite (k, n)-group, $h_1, h_2, \cdots, h_n$ will denote a fixed basis of G/V_k and θ will denote the mapping of the automorphism group of G/V_k into R_k^n defined as follows:

If τ is an automorphism of G/V_k and

$$h_i\tau = h_1^{\tau_{i1}} h_2^{\tau_{i2}} \cdots h_n^{\tau_{in}} \qquad (i = 1, 2, \cdots, n)$$

where $0 \leqq \tau_{ij} < k (i, j = 1, 2, \cdots, n)$, then

https://doi.org/10.1017/S1446788700027919 Published online by Cambridge University Press

$$\tau\theta = (\tau_{ij}).$$

If $\mathfrak{g} = (g_1, g_2, \cdots, g_n)$ is a generating n-vector of G, then $\mathfrak{g}V = (g_1V, g_2V, \cdots, g_nV)$ is a generating n-vector of G/V. Thus there is a unique automorphism γ of G/V such that

$$h_i\gamma = g_iV \qquad (i = 1, 2, \cdots, n); \tag{1}$$

hence a mapping D of Γ_G^n into R_k is defined by

$$D(\mathfrak{g}) = \det(\gamma\theta).$$

LEMMA 1. *The image of Γ_G^n under D is Λ_k.*

PROOF. It is easy to see that if τ, σ are automorphisms of G/V, then

$$(\tau\sigma)\theta = (\tau\theta)(\sigma\theta)\,. \tag{2}$$

Since the identity automorphism of G/V maps onto the identity matrix of R_k^n under θ, it follows that every matrix belonging to the image set of θ has an inverse in R_k^n. Therefore (see [3], Theorem 37, p. 185) the image set of θ is contained in Λ_k^n and consequently the image set of D is contained in Λ_k. Since ([4], Satz 1) there is, for each λ in Λ_k, a generating n-vector $\mathfrak{g}$ of G such that $\mathfrak{g}V = (h_1, h_2, \cdots, h_{n-1}, h_n^\lambda)$, the image set of D is Λ_k itself.

LEMMA 2. *There is a mapping D_F of the automorphism group $A(F_n)$ of the free group of rank n into the right regular representation $R(\Lambda_k)$ of Λ_k such that $D(\mathfrak{g})D_F(\alpha) = D(\mathfrak{g}\alpha_G)$ for all $\mathfrak{g} \in \Gamma_G^n$ and all $\alpha \in A(F_n)$, where α_G is the induced permutation of Γ_G^n defined in § 1. The range of D_F consists of two elements: the identity and the element which maps every element to its negative.*

PROOF. Let $x_1, x_2, \cdots, x_n$ be a set of generators of F_n and let α be an arbitrary automorphism of F_n such that

$$x_i\alpha = w_i(x_1, x_2, \cdots, x_n) \quad \text{for} \quad i = 1, 2, \cdots, n,$$

then there is a unique automorphism α^V of G/V such that

$$h_i\alpha^V = w_i(h_1, h_2, \cdots, h_n) \quad \text{for} \quad i = 1, 2, \cdots, n.$$

Moreover

$$h_i\alpha^V\gamma = w_i(g_1V, g_2V, \cdots, g_nV) \quad \text{for} \quad i = 1, 2, \cdots, n$$

where γ is the automorphism of G/V as defined in (1). Now,

$$\mathfrak{g}\alpha_G V = (g_1'V, g_2'V, \cdots, g_n'V)$$

where

$$\begin{aligned} g_i'V &= w_i(g_1, g_2, \cdots, g_n)V \quad \text{for} \quad i = 1, 2, \cdots, n \\ &= w_i(g_1V, g_2V, \cdots, g_nV). \end{aligned}$$

https://doi.org/10.1017/S1446788700027919 Published online by Cambridge University Press

Therefore

$$\mathfrak{g}\alpha_G V = (h_1\alpha^V\gamma, h_2\alpha^V\gamma, \cdots, h_n\alpha^V\gamma)$$

and

$$D(\mathfrak{g}\alpha_G) = \det((\alpha^V\gamma)\theta).$$

So, by (2),

$$D(\mathfrak{g}\alpha_G) = D(\mathfrak{g})\det(\alpha^V\theta).$$

Let $D_F(\alpha)$ be the element of $R(\Lambda_k)$ corresponding to det $(\alpha^V\theta)$; the first part of the lemma follows.

It is easy to see that D_F is a homomorphism. In order to prove the second part of the lemma it is only necessary, therefore, to consider a set of generators of $A(F_n)$. The four automorphisms μ, ν, π, ρ defined by:

$$\begin{array}{llll} x_1\mu = x_2, & x_2\mu = x_1, & x_i\mu = x_i & (i = 3, \cdots, n); \\ x_1\nu = x_1, & x_n\nu = x_2, & x_{i-1}\nu = x_i & (i = 3, \cdots, n); \\ x_1\pi = x_1, & x_2\pi = x_2^{-1}, & x_i\pi = x_i & (i = 3, \cdots, n); \\ x_1\rho = x_1, & x_2\rho = x_1x_2, & x_i\rho = x_i & (i = 3, \cdots, n), \end{array}$$

form a generating set of $A(F_n)$ (see [1], § 6).

Hence

$$\mu^V\theta = \left(\begin{array}{cc|c} 0 & 1 & \multirow{2}{*}{0} \\ 1 & 0 & \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \end{array}\right);$$

$$\nu^V\theta = \left(\begin{array}{cc|c} 1 & 0 & 0 \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \\ \hline 0 & 1 & 0 \end{array}\right);$$

$$\pi^V\theta = \left(\begin{array}{cc|c} 1 & 0 & \multirow{2}{*}{0} \\ 0 & -1 & \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \end{array}\right);$$

$$\rho^V\theta = \left(\begin{array}{cc|c} 1 & 0 & \multirow{2}{*}{0} \\ 1 & 1 & \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \end{array}\right).$$

(Here -1 represents the negative of 1 in the ring R_k, and I_{n-2} the identity matrix of R_k^{n-2}).

Hence

https://doi.org/10.1017/S1446788700027919 Published online by Cambridge University Press

$$\begin{aligned}
\det(\mu^V\theta) &= -1;\\
\det(\nu^V\theta) &= 1 \quad \text{if } n \text{ is even,}\\
&= -1 \text{ if } n \text{ is odd;}\\
\det(\pi^V\theta) &= -1;\\
\det(\rho^V\theta) &= 1.
\end{aligned}$$

The result follows immediately.

LEMMA 3. *There is a mapping D_G of the automorphism group $A(G)$ of G into $R(\Lambda_k)$ such that*

$$D(\mathfrak{g})D_G(\beta) = D(\mathfrak{g}\beta_G)$$

for all $\mathfrak{g} \in \Gamma_G^n$ and all $\beta \in A(G)$, where β_G is the induced permutation of Γ_G^n defined in § 1.

PROOF. Since V is a characteristic subgroup of G an automorphism β of G induces an automorphism β^V of G/V given by

$$gV\beta^V = g\beta V$$

for all $g \in G$. Now,

$$\begin{aligned}
\mathfrak{g}\beta_G V &= (g_1\beta V, g_2\beta V, \cdots, g_n\beta V)\\
&= (g_1 V\beta^V, g_2 V\beta^V, \cdots, g_n V\beta^V)\\
&= (h_1\gamma\beta^V, h_2\gamma\beta^V, \cdots, h_n\gamma\beta^V)
\end{aligned}$$

where γ is the automorphism of G/V as defined in (1). So

$$\begin{aligned}
D(\mathfrak{g}\beta_G) &= \det((\gamma\beta^V)\theta)\\
&= D(\mathfrak{g})\det(\beta^V\theta).
\end{aligned}$$

Let $D_G(\beta)$ be the element of $R(\Lambda_k)$ corresponding to det $(\beta^V\theta)$; the lemma follows.

Let P_k denote the subgroup of $R(\Lambda_k)$ generated by all the $D_F(\alpha)$ and $D_G(\beta)$ arising in the above manner from automorphisms of F_n and G respectively. The transitivity sets of Λ_k under P_k will be called the T_k-*systems* of G, and $t_{n,k}(G)$ will denote the number of T_k-systems of G.

Clearly T-systems map into T_k-systems under D and so a lower bound is obtained for the number $t_n(G)$ of T-systems of generating n-vectors of G.

THEOREM 2. *If G is a finite (k, n)-group, then*

$$t_n(G) \geqq t_{n,k}(G).$$

Inequality can hold here, as has been indicated in the introduction.

3. Examples

In this section p denotes a prime and n, r are integers such that $n > 1$, $r > 0$; let $q = p^r$.

Let $A_{q,n}$ be the abelian group generated by $a_2, \cdots, a_n$ with the relations $a_i^{q^{2(i-1)}} = a_n^{q^{3n-2-i}}$ $(i = 2, \cdots, n-1)$ and $a_n^{q^{3n-2}} = e$; i.e.

$$A_{q,n} = \mathrm{gp}\{a_2, \cdots, a_n | [a_i, a_j] = e (i, j = 2, \cdots, n),\\ a_i^{q^{2(i-1)}} = a_n^{q^{3n-2-i}} (i = 2, \cdots, n-1), a_n^{q^{3n-2}} = e\}.$$

(Here and below e denotes the identity element, and $[x, y]$ denotes the commutator $x^{-1}y^{-1}xy$). Since

$$(a_i^{1+q^{2(i-1)}})^{q^{2(i-1)}} = a_i^{q^{2(i-1)}} \qquad (i = 2, \cdots, n-1)$$

and

$$(a_n^{1+q^{2(n-1)}})^{q^{3n-2-i}} = a_n^{q^{3n-2-i}} \qquad (i = 2, \cdots, n-1),$$

there is a unique automorphism ψ of $A_{q,n}$ such that

$$a_i\psi = a_i^{1+q^{2(i-1)}} \qquad (i = 2, \cdots, n).$$

The order of ψ is q^n. Let $B_{q,n}$ be the splitting extension of $A_{q,n}$ by a cyclic group of order q^{3n-1} generated by an element b which induces ψ in $A_{q,n}$; i.e.

$$B_{q,n} = \mathrm{gp}\{a_2, \cdots, a_n, b| \text{ relations of } A_{q,n},\\ b^{-1}a_ib = a_i^{1+q^{2(i-1)}} (i = 2, \cdots, n), b^{q^{3n-1}} = e\}.$$

The elements b^{q^n} and $a_n^{q^{3(n-1)}}$ are in the centre of $B_{q,n}$, so that $a_n^{q^{3(n-1)}}b^{-q^{3n-2}}$ is self-conjugate in $B_{q,n}$. Let $G_{q,n}$ be the group $B_{q,n}/\{a_n^{q^{3(n-1)}}b^{-q^{3n-2}}\}$.

Thus

$$G_{q,n} = \mathrm{gp}\{a_2, \cdots, a_n, b| \text{ relations of } A_{q,n};\\ b^{-1}a_ib = a_i^{1+q^{2(i-1)}} (i = 2, \cdots, n), b^{q^{3n-2}} = a_n^{q^{3(n-1)}}\}.$$

Clearly $G_{q,n}$ is nilpotent of class 2, so every element can be written uniquely in the form

$$a_2^{\xi_2} \cdots a_n^{\xi_n} b^{\eta}[a_n, b]^{\zeta}$$
$$0 \leqq \xi_i < q^{2(i-1)}, \qquad 0 \leqq \eta < q^{3n-2},$$
$$0 \leqq \zeta < q^n \qquad (i = 2, \cdots, n).$$

Let β be an automorphism of $G_{q,n}$ and let

$$a_i\beta = a_2^{\alpha_{i2}} \cdots a_n^{\alpha_{in}} b^{\delta_i}[a_n, b]^{\varepsilon_i},$$
$$b\beta = a_2^{\alpha_2} \cdots a_n^{\alpha_n} b^{\delta}[a_n, b]^{\varepsilon}$$
$$0 \leqq \alpha_{ij} < q^{2(i-1)}, 0 \leqq \delta_i < q^{3n-2}, 0 \leqq \varepsilon_i < q^n \qquad (i, j = 2, \cdots, n),$$
$$0 \leqq \alpha_i < q^{2(i-1)}, \ 0 \leqq \delta < q^{3n-2}, \ 0 \leqq \varepsilon < q^n \qquad (i = 2, \cdots, n).$$

https://doi.org/10.1017/S1446788700027919 Published online by Cambridge University Press

Since $(a_i\beta)^{q^{2(i-1)}}$ belongs to the derived group, it follows that $q^{2(j-i)}$ divides α_{ij} if $j > i$, and q^{3n-2i} divides δ_i for every i. Now $G_{q,n}$ is a (q, n)-group and, if $a_2V_q, \cdots, a_nV_q, bV_q$ is chosen as the basis for reference of $G_{q,n}/V_q$, then

$$\det(\beta^V\theta) \equiv \delta \prod_{i=2}^{n} \alpha_{ii} (\mathrm{mod}\ q).$$

The $a_i\beta$'s and $b\beta$ must satisfy the same relations as the a_i's and b. In particular

$$(3) \qquad [a_i\beta, b\beta] = (a_n\beta)^{q^{3n-2-i}} \quad \text{for} \quad i = 2, \cdots, n$$

and

$$(4) \qquad (b\beta)^{q^{3n-2}} = (a_n\beta)^{q^{3(n-1)}}.$$

Now,

$$\begin{aligned}[a_i\beta, b\beta] &= \prod_{j=2}^{n} [a_j, b]^{\alpha_{ij}\delta - \delta_i\alpha_j} \\ &= [a_n, b]^{\sum_{j=2}^{n} (\alpha_{ij}\delta - \delta_i\alpha_j)q^{(n-j)}}\end{aligned}$$

and

$$\sum_{j=2}^{n} (\alpha_{ij}\delta - \delta_i\alpha_j)q^{(n-j)} \equiv \alpha_{ii}\delta q^{(n-i)} \ (\mathrm{mod}\ q^{(n-i+1)}).$$

Also

$$(a_n\beta)^{q^{3n-2-i}} = a_n^{\alpha_{nn}q^{3n-2-i}} a$$

where $a \in \{a_n^{q^{3n-1-i}}\}$. It follows from (3) that

$$\alpha_{ii}\delta \equiv \alpha_{nn} \ (\mathrm{mod}\ q) \quad \text{for} \quad i = 2, \cdots, n.$$

Similarly

$$\delta \equiv \alpha_{nn} \ (\mathrm{mod}\ q)$$

follows from (4). Hence

$$\begin{aligned}\alpha_{ii} &\equiv \delta \ (\mathrm{mod}\ q) \quad \text{for} \quad i = 2, \cdots, n \\ &\equiv 1 \ (\mathrm{mod}\ q).\end{aligned}$$

Therefore

$$\det\,(\beta^V\theta) = 1.$$

Thus, for $G_{q,n}$, the group P_q consists of just two elements, namely the identity and the element which maps every element to its negative. But Λ_q has order $(p-1)p^{r-1}$, so

$$t_{n,q}(G_{q,n}) = \max(1, \tfrac{1}{2}(p-1)p^{r-1}).$$

Theorem 1 then follows from Theorem 2.

References

[1] Bernhard H. Neumann und Hanna Neumann, Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen. *Math. Nachr.* **4** (1951) 106—125.
[2] B. H. Neumann, On a Question of Gaschütz. *Archiv der Mathematik* **7** (1956) 87—90.
[3] Claude Chevalley, *Fundamental Concepts of Algebra*. Academic Press Inc., New York (1956).
[4] Wolfgang Gaschütz, Zu einem von B. H. und H. Neumann gestellten Problem, *Math. Nachr.* **14** (1955—56) 249—252.

Australian National University,
Canberra.