Duke Math. J. 39 (1972), 521-527.

ON THE NUMBER OF DISTINGUISHED REPRESENTATIONS OF A GROUP ELEMENT

DAVID JACOBSON AND KENNETH S. WILLIAMS

1. Introduction. Let Δ denote a property which an element of a group may possess. We are interested in the number of representations of an element in a finite group as a product of r elements possessing Δ.

More generally, let D be a nonempty subset of a finite group G and denote by $N_r^D(a) = N_r(a)$ the number of solutions of the equation

$$x_1 \cdots x_r = a \tag{1}$$

where a is an element of G and $x_1, \cdots, x_r$ belong to D. Of course, if a is not in the subgroup generated by D, then $N_r(a) = 0$ for all r.

In Proposition 1 we note that the evaluation of $N_r^D(a)$ reduces to the corresponding question for a certain quotient group of G.

If D itself is a subgroup of G, then trivially $N_r(a) = |D|^{r-1}$ for a in D.

For arbitrary D the calculation of $N_r^D(a)$ seems quite difficult. One of our main results is the explicit determination in Theorem 2 of $N_r^D(a)$ when $G \setminus D$, the complement of D in G, is a subgroup of G.

As an application of Theorem 2 we obtain in Corollary 5 the number of representations of a given element in an abelian group G as a product of r elements of maximal order in G. In particular, for G cyclic this number agrees with a formula derived by Rearick [3] and is essentially equivalent to an earlier formula of Dixon [1].

In §4 analogous questions for rings are considered.

2. Main results. For D a nonempty subset of G let $J(D) = J$ denote the largest normal subgroup of G such that $xJ \subseteq D$ for all x in D. We say that G is *D-reduced* if $J = \{1\}$. If $a \in G$, let $\bar{a}$ denote aJ in $\bar{G} = G/J$.

PROPOSITION 1. *If $\bar{D} = \{\bar{x} \mid x \in D\}$, then $\bar{G}$ is $\bar{D}$-reduced and*

$$N_r^D(a) = |J|^{r-1} N_r^{\bar{D}}(\bar{a}). \tag{2}$$

Proof. If $\bar{K} = K/J$ is the largest normal subgroup of $\bar{G}$ such that $\bar{x}\bar{K} \subseteq \bar{D}$ for all $\bar{x}$ in $\bar{D}$, then clearly $xK \subseteq D$ for all x in D. However, K is a normal subgroup of G and thus $K = J$, which establishes that $\bar{G}$ is $\bar{D}$-reduced.

To prove (2) we require the following lemma.

LEMMA. *Let G be a finite group and J a normal subgroup of G. If $x_1, \cdots, x_r$ belong to G, then the number of r-tuples $(y_1, \cdots, y_r)$ satisfying $x_1 \cdots x_r = y_1 \cdots y_r$ and $y_i \in x_iJ$ for $i = 1, \cdots, r$ is equal to $|J|^{r-1}$.*

Received March 13, 1972.

Proof. The result is trivial for $r = 1$. Suppose $r > 1$ and let $b_1, \cdots, b_{r-1}$ be arbitrary elements of J. It suffices to show that $b_1 x_2 \cdots b_{r-1} x_r$ is equal to $x_2 \cdots x_r b$ where $b \in J$. However, this follows easily from the normality of J, which proves the lemma.

Returning to the proof of Proposition 1 we let S denote the set of solutions $(x_1, \cdots, x_r)$ of (1) and introduce an equivalence relation on S by defining $(x_1, \cdots, x_r) \sim (y_1, \cdots, y_r)$ if $y_i \in x_i J$ for $i = 1, \cdots, r$. With each equivalence class $C(x_1, \cdots, x_r)$ of S we associate the r-tuple $(\bar{x}_1, \cdots, \bar{x}_r)$, where $\bar{x}_1 \cdots \bar{x}_r = \bar{a}$ in $\bar{G}$. Clearly this defines a mapping ψ from the set of equivalence classes of S into $\bar{S}$, the set of solutions of the equation $\bar{x}_1 \cdots \bar{x}_r = \bar{a}$, where $\bar{x}_1, \cdots, \bar{x}_r$ belong to $\bar{D}$.

The mapping ψ is a bijection. It is one-to-one for if $(\bar{x}_1, \cdots, \bar{x}_r) = (\bar{y}_1, \cdots, \bar{y}_r)$, that is, if $\bar{y}_i = \bar{x}_i$ for $i = 1, \cdots, r$, then $(x_1, \cdots, x_r) \sim (y_1, \cdots, y_r)$ and $C(x_1, \cdots, x_r) = C(y_1, \cdots, y_r)$. To show that ψ is onto let $\bar{x}_1 \cdots \bar{x}_r = \bar{a}$, where $\bar{x}_1, \cdots, \bar{x}_r$ belong to $\bar{D}$. This implies that $x_1 \cdots x_r b = a$, where $x_1, \cdots, x_r$ belong to D and $b \in J$. Thus $(x_1, \cdots, x_r b)$ is a solution of (1) and ψ maps $C(x_1, \cdots, x_r b)$ onto $(\bar{x}_1, \cdots, \bar{x}_r)$ in $\bar{S}$.

Hence the number of equivalence classes of S is equal to $N_r^{\bar{D}}(\bar{a})$. However, by the lemma each equivalence class consists of $|J|^{r-1}$ elements and therefore $N_r^D(a) = |J|^{r-1} N_r^{\bar{D}}(\bar{a})$, which completes the proof of Proposition 1.

We remark that if $G \setminus D$ is a normal subgroup of G, then $J = G \setminus D$ and thus $\bar{D}$ consists of all elements of $\bar{G}$ except the identity. This case is included in the following more general theorem.

THEOREM 2. *Let G be a finite group of order g and D a nonempty subset of G containing d elements. If $H = G \setminus D$ is a subgroup of G, then*

$$N_r(a) = \frac{d^r}{g}\left(1 + \frac{(-1)^r \gamma(a)}{([G:H] - 1)^r}\right) \tag{3}$$

where $[G:H]$ is the index of H in G and $\gamma(a) = -1$ or $[G:H] - 1$ according as $a \in D$ or $a \notin D$.

Proof. Note that we do not assume that H is normal in G. We begin by remarking that

$$\sum_{b \in G} N_r(b) = d^r \tag{4}$$

since the left side merely represents the number of ways of forming all r-tuples $(x_1, \cdots, x_r)$ with each x_i in D.

Next we observe that

$$N_{r+1}(a) = \sum_{b^{-1}a \in D} N_r(b) \tag{5}$$

since all the solutions of the equation

$$x_1 \cdots x_r x_{r+1} = a,$$

with each x_i in D, correspond to the solutions of the simultaneous equations

$$x_1 \cdots x_r = b, \qquad x_{r+1} = b^{-1}a$$

in which $x_1, \cdots, x_r$ and $b^{-1}a$ belong to D.

As H is the complement of D we obtain from (4) and (5) that

$$N_{r+1}(a) = d^r - \sum_{b^{-1}a \in H} N_r(b). \tag{6}$$

However, $b^{-1}a \in H$ if and only if $b \in aH$. Moreover, if $b \in aH$, then $N_r(a) = N_r(b)$. For suppose $b = ac$ with c in H. If $a \in D$, then $b \in D$ and $N_1(a) = 1 = N_1(b)$. If $a \notin D$, then a and b both belong to H so that $N_1(a) = 0 = N_1(b)$. Now if $r > 1$ and if $x_1 \cdots x_{r-1}x_r = a$, where each $x_i \in D$, then $x_1 \cdots x_{r-1}(x_rc) = b$ and $x_rc \in D$, which establishes that $N_r(a) = N_r(b)$. Hence from (6) we obtain

$$N_{r+1}(a) = d^r - hN_r(a) \tag{7}$$

where h denotes the order of H. Applying the recurrence relation (7) successively gives

$$N_r(a) = d^{r-1} - hd^{r-2} + \cdots + (-1)^{r-2}h^{r-2}d + (-1)^{r-1}h^{r-1}N_1(a). \tag{8}$$

Now the right side of (8) is the sum of a geometric progression with common ratio $-h/d$ which has r or $r - 1$ terms according as $a \in D$ or $a \notin D$. Hence we obtain (3) since $[G:H] - 1 = (g/h) - 1 = d/h$.

We note that (3) vanishes if and only if $[G:H] = 2$ and r is even or odd according as $a \in D$ or $a \notin D$.

We also require the following extension of Formula (3).

Let $m_1, \cdots, m_r$ be given integers and denote by $\mathfrak{N}_r^D(a)$ the number of solutions $(x_1, \cdots, x_r)$ of the equation

$$x_1^{m_1} \cdots x_r^{m_r} = a \tag{9}$$

where $a \in G$ and $x_1, \cdots, x_r$ belong to D, a nonempty subset of G.

Consider the following properties which an integer m may possess.

(α) For $x \in D$ the mapping $x \to x^m$ is a bijection of D or

(β) $x^m \in G \setminus D$ for all x in D.

COROLLARY 3. *Suppose that D is a nonempty subset of a finite group G and that $H = G \setminus D$ is a subgroup of G. Let $G^* = G \cdot G_0$ be the direct product of G and any group G_0 and let $D^* = D \cdot G_0$. For $a^* \in G^*$ let $a^* = aa_0$ with $a \in G$ and $a_0 \in G_0$. If $m_1, \cdots, m_r$ are integers such that for some i the m_i-th power map is a bijection of G_0, then*

$$\mathfrak{N}_r^{D^*}(a^*) = [G^*:G]^{r-1}\mathfrak{N}_r^D(a). \tag{10}$$

Further if $m_1, \cdots, m_r$ satisfy either (α) or (β) and at least one satisfies (α), then

$$\mathfrak{N}_r^D(a) = \frac{d^r}{g}\left(1 + \frac{\gamma(a)\rho(m_1) \cdots \rho(m_r)}{([G:H] - 1)^r}\right) \tag{11}$$

where $\gamma(a) = -1$ *or* $[G:H] - 1$ *according as* $a \in D$ *or* $a \notin D$ *and where* $\rho(m_i) = -1$ *or* $[G:H] - 1$ *according as* m_i *satisfies* (α) *or* (β).

Proof. If $z_1^{m_1} \cdots z_r^{m_r} = a^*$ for $z_1, \cdots, z_r$ in D^*, then $x_1^{m_1} \cdots x_r^{m_r} = a$ and $b_1^{m_1} \cdots b_r^{m_r} = a_0$, where $x_1, \cdots, x_r$ belong to D and $b_1, \cdots, b_r$ belong to G_0. Since some m_i induces a bijection on G_0, the number of r-tuples $(b_1, \cdots, b_r)$ of G_0 for which $b_1^{m_1} \cdots b_r^{m_r} = a_0$ is $|G_0|^{r-1}$ and as $D^* = D \cdot G_0$ we obtain (10).

Now let $k \geq 1$ be the number of m_i which satisfy (α). Then for any solution $(x_1, \cdots, x_r)$ of (9) the terms of $x_1^{m_1} \cdots x_r^{m_r}$ can be appropriately grouped to give a product $y_1 \cdots y_k = a$, where $y_1, \cdots, y_k$ belong to D. However, to each such product there correspond d^{r-k} distinct solutions of (9) and hence by (3)

$$\mathfrak{N}_r^D(a) = d^{r-k} N_k^D(a) = \frac{d^r}{g}\left(1 + \frac{(-1)^k \gamma(a)}{([G:H] - 1)^k}\right)$$

which by the definition of $\rho(m_i)$ is Formula (11).

If $m_1 = \cdots = m_r = 1$, then (10) holds and (11) reduces to (3).

Suppose that G is a direct product of groups $G_1, \cdots, G_n$ and let $D = D_1 \cdots D_n$, where D_i is a nonempty subset of G_i for $i = 1, \cdots, n$. For $a \in G$ let $a = a_1 \cdots a_n$ with a_i in G_i. If $m_1, \cdots, m_r$ are integers, then a standard argument shows that

$$\mathfrak{N}_r^D(a) = \prod_{i=1}^{n} \mathfrak{N}_r^{D_i}(a_i). \tag{12}$$

Also suppose that $H_i = G_i \setminus D_i$ is a subgroup of G_i for $i = 1, \cdots, n$. If $m_1, \cdots, m_r$ satisfy either (α) or (β) and at least one satisfies (α) with respect to each group G_i and subset D_i, then (11) and (12) yield

$$\mathfrak{N}_r^D(a) = \frac{d^r}{g} \prod_{i=1}^{n} \left(1 + \frac{\gamma(a_i)\rho(m_1) \cdots \rho(m_r)}{([G_i : H_i] - 1)^r}\right). \tag{13}$$

3. Applications.

(a) Let Δ be the property that an element of a group is non-central. Since the central elements of a group form a subgroup, the formula for $N_r(a)$ in Theorem 2 applies when G is a finite non-abelian group, D is the set of non-central elements of G, and H is the center of G.

(b) Let Δ be the property that an element of a group is a generator. (Recall that an element x of a group G is a generator if there exists a subset T of G such that $\langle T, x \rangle = G$ but $\langle T \rangle \neq G$.) Since the set H of non-generators is the Frattini subgroup of G, the formula for $N_r(a)$ is given by (3).

(c) Let Δ be the property that an element of a finite group has maximal order and let D be the set of elements of maximal order in a group G. If G is a direct product of groups $G_1, \cdots, G_n$ whose orders are pairwise relatively prime, then $D = D_1 \cdots D_n$, where D_i is the set of elements of maximal order in G_i. Thus by (12) in order to evaluate $N_r^D(a)$ for a nilpotent group G we may assume G is a p-group.

Let $\mathfrak{M}$ denote the class of p-groups G for which H, the elements not of maximal order, form a subgroup of G. Clearly $\mathfrak{M}$ contains the class of abelian p-groups and indeed the class of regular p-groups [2; 185, Theorem 12.4.3].

We note that if $G \in \mathfrak{M}$, then H is a fully invariant subgroup of G and G/H is of exponent p.

If m is an integer relatively prime to p, then m satisfies (α) since the mapping $x \to x^m$ is an order preserving bijection of any p-group. On the other hand, if $p \mid m$, then m satisfies (β). Thus if $G \in \mathfrak{M}$ and $m_1, \cdots, m_r$ are integers whose greatest common divisor is prime with p, then $\mathfrak{N}_r^D(a)$ is given by (11).

It is now easy to determine $\mathfrak{N}_r^D(a)$ for any integers $m_1, \cdots, m_r$ if G is a p-abelian p-group, that is, $(ab)^p = a^p b^p$ for all elements a, b in G [4]. For suppose p^s is the highest power of p dividing $m_1, \cdots, m_r$ and let $m_i/p^s = m_i'$ for $i = 1, \cdots, r$. If $x_1^{m_1} \cdots x_r^{m_r} = a$, then $(x_1^{m_1'} \cdots x_r^{m_r'})^{p^s} = a$ since G is p-abelian. For b in G let $\mathfrak{N}_r'^D(b)$ denote the number of solutions of $x_1^{m_1'} \cdots x_r^{m_r'} = b$, where $x_1, \cdots, x_r$ belong to D. Then clearly

$$\mathfrak{N}_r^D(a) = \sum_{b^{p^s}=a} \mathfrak{N}_r'^D(b). \tag{14}$$

Now let f denote the endomorphism of G defined by $f(c) = c^{p^s}$ for c in G. We may assume that $a \in \operatorname{Im} f$ for otherwise $\mathfrak{N}_r^D(a) = 0$. If $a = b_0^{p^s}$ for b_0 in G, then $f(b) = a$ if and only if $b \in b_0(\operatorname{Ker} f)$. If $p^s \geq$ exponent G, then $\mathfrak{N}_r^D(a) = d^r$. Suppose that $p^s <$ exponent G. Then $\operatorname{Ker} f \subseteq G \setminus D = H$ and since G is p-abelian, H is a subgroup of G. However, $(m_1', \cdots, m_r', p) = 1$ and hence (11) shows that $\mathfrak{N}_r'^D(b)$ depends only on whether $b \in D$ or $b \in H$. Therefore, $\mathfrak{N}_r'^D(b) = \mathfrak{N}_r'^D(b_0)$ for all b in $b_0(\operatorname{Ker} f)$ and from (14) we obtain

$$\mathfrak{N}_r^D(a) = |\operatorname{Ker} f|\, \mathfrak{N}_r'^D(b_0) \quad \text{where} \quad a = b_0^{p^s}. \tag{15}$$

PROPOSITION 4. *Let G be the direct product of p-groups G_1 and G_2.*
(i) *If exponent G_1 = exponent G_2, then $G \in \mathfrak{M}$ if and only if $G_i \in \mathfrak{M}$ for $i = 1, 2$.*
(ii) *If exponent $G_1 >$ exponent G_2, then $G \in \mathfrak{M}$ if and only if $G_1 \in \mathfrak{M}$.*

Proof. Let D_i be the set of elements of maximal order in G_i and let $H_i = G_i \setminus D_i$ for $i = 1, 2$. Let D and H denote the corresponding sets for G.

If exponent G_1 = exponent G_2, then $H = H_1 \cdot H_2$ and thus H is a subgroup of G if and only if H_i is a subgroup of G_i for $i = 1, 2$, which proves (i).

If exponent $G_1 >$ exponent G_2, then $D = D_1 \cdot G_2$ and $H = H_1 \cdot G_2$, which by the above argument proves (ii).

It is of interest to calculate $\mathfrak{N}_r^D(a)$ for an abelian p-group.

COROLLARY 5. *Let G be an abelian group of order p^n and let D denote the set of elements of maximal order in G. If the exponent of G appears exactly k times in the set of invariants of G and if $m_1, \cdots, m_r$ are integers such that $(m_1, \cdots, m_r, p) = 1$, then*

$$\mathfrak{N}_r^D(a) = \frac{(p^n - p^{n-k})^r}{p^n}\left(1 + \frac{\gamma(a)\rho(m_1) \cdots \rho(m_r)}{(p^k - 1)^r}\right) \tag{16}$$

where $\gamma(a) = -1$ *or* $p^k - 1$ *according as* $a \in D$ *or* $a \notin D$ *and where* $\rho(m_i) = -1$ *or* $p^k - 1$ *according as* $(p, m_i) = 1$ *or* $p \mid m_i$.

Proof. Since the index of the subgroup of elements not of maximal order in a cyclic p-group is p, (16) follows from Proposition 4 and Formulas (10) and (11) of Corollary 3.

Setting $k = 1$ in (16) yields $\mathfrak{N}_r^D(a)$ for a cyclic group of order p^n.

In view of (15) the reader may provide the slight modification needed in Corollary 5 to express $\mathfrak{N}_r^D(a)$ for arbitrary integers $m_1, \cdots, m_r$.

We remark that if G is a p-group not in $\mathfrak{M}$ but G_0, the subgroup generated by D, belongs to $\mathfrak{M}$, then the previous formulas for $N_r^D(a)$ apply when $a \in G_0$. If $a \notin G_0$, then $N_r^D(a) = 0$ for all r. The dihedral group of order $2 \cdot 2^{n+1}$ is such an example.

However, an open question is the evaluation of $N_r^D(a)$ for a p-group G which is generated by D but G is not in $\mathfrak{M}$.

4. Analogue for rings. If R is a finite ring and D a nonempty subset of R, then the number of solutions of the equation

$$x_1 + \cdots + x_r = a \quad \text{for} \quad a \in R \quad \text{and} \quad x_1, \cdots, x_r \quad \text{in} \quad D$$

is what has been denoted by $N_r^D(a)$ with respect to $(R, +)$, the additive group of R.

Note that the analogue of Proposition 1 for a ring R is valid, where $J = J(D)$ is taken to be the largest ideal of R such that $x + J \subseteq D$ for all x in D.

In case $U = D$ denotes the set of units in a ring R with identity, then $J(U)$ becomes the usual Jacobson radical of R. Thus by (2) the evaluation of $N_r^U(a)$ is reduced to the case where R is semisimple. Then (12) shows that it suffices to determine $N_r^U(a)$ for F_n, the ring of $n \times n$ matrices over a finite field F.

One may verify that U generates F_n, that is, every matrix is a sum of invertible matrices. Moreover, $N_r^U(a)$ depends only on the rank of the matrix a. At present we are not able to compute $N_r^U(a)$ for F_n, where $n > 1$, even when $a = 0$.

If F is a field, then $U = F \setminus \{0\}$ and $N_r^U(a)$ is given by (3) of Theorem 2. Thus if C denotes the class of rings R for which R/J is a direct product of fields, then $N_r^U(a)$ can be explicitly determined for any R in C. Note local rings, and hence commutative rings, belong to C.

For positive integral r, n and integral a Rearick determined the number of solutions of the linear congruence

$$x_1 + \cdots + x_r \equiv a \pmod{n}$$

where $0 \leq x_i < n$ and $(x_i, n) = 1$ for $i = 1, \cdots, n$. This number is just $N_r^U(a)$ with respect to the ring $Z/(n)$. (In this context an equivalent formula for $N_r^U(a)$ was given by Dixon [1].) Since U coincides with the set of elements of maximal order in the cyclic group $(Z/(n), +)$, we can apply Corollary 5 to obtain the following more general result.

Let $m_1, \cdots, m_r$ be integers such that $(m_1, \cdots, m_r) = 1$ and denote by $\mathfrak{N}_r(a)$ the number of solutions of the congruence

$$m_1x_1 + \cdots + m_rx_r \equiv a \pmod{n}$$

where $0 \leq x_i < n$ and $(x_i, n) = 1$ for $i = 1, \cdots, r$. If m is an integer and p is a prime, define $\gamma_p(m) = -1$ or $p - 1$ according as $(p, m) = 1$ or $p \mid m$. Then

$$\mathfrak{N}_r(a) = \frac{\phi^r(n)}{n} \prod_{p \mid n} \left(1 + \frac{\gamma_p(a)\gamma_p(m_1) \cdots \gamma_p(m_r)}{(p-1)^r}\right),$$

which reduces to Rearick's result when $m_1 = \cdots = m_r = 1$.

REFERENCES

1. J. D. DIXON, *A finite analogue of the Goldbach problem*, Canad. Math. Bull., vol. 3(1960), pp. 121–126.
2. MARSHALL HALL, JR., *The Theory of Groups*, New York, 1959.
3. DAVID REARICK, *A linear congruence with side conditions*, Amer. Math. Monthly, vol. 70(1963), pp. 837–840.
4. PAUL M. WEICHSEL, *On p-abelian groups*, Proc. Amer. Math. Soc., vol. 18(1967), pp. 736–737.

Jacobson: DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEW BRUNSWICK, NEW JERSEY 08903

Williams: DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA