ON THE NUMBER OF DISTINGUISHED REPRESENTATIONS OF A GROUP ELEMENT

DAVID JACOBSON AND KENNETH S. WILLIAMS

1. Introduction. Let $\Delta$ 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 $\Delta$.

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

(1) \[ x_1 \cdots x_r = a \]

where $a$ is an element of $G$ and $x_1, \ldots, x_r$ 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

(2) \[ N_r^\bar{D}(a) = |J|^{r-1}N_r^\bar{G}(\bar{a}). \]

**Proof.** If $K = K/J$ is the largest normal subgroup of $\bar{G}$ such that $\bar{x}K \subseteq \bar{D}$ 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 $x_1, \ldots, x_r$ belong to $G$, then the number of $r$-tuples $(y_1, \ldots, y_r)$ satisfying $x_1 \cdots x_r = y_1 \cdots y_r$ and $y_i \in x_i J$ for $i = 1, \ldots, r$ is equal to $|J|^{r-1}$.

Received March 13, 1972.
Proof. The result is trivial for \( r = 1 \). Suppose \( r > 1 \) and let \( b_1, \ldots, b_{r-1} \) be arbitrary elements of \( J \). It suffices to show that \( b_1x_2 \cdots b_{r-1}x_r \) 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 \((x_1, \ldots, x_r)\) of (1) and introduce an equivalence relation on \( S \) by defining \((x_1, \ldots, x_r) \sim (y_1, \ldots, y_r)\) if \( y_i x_i J \) for \( i = 1, \ldots, r \). With each equivalence class \( C(x_1, \ldots, x_r) \) of \( S \) we associate the \( r \)-tuple \((\xi_1, \ldots, \xi_r)\), where \( \xi_1 \cdots \xi_r = \xi \) in \( \bar{G} \). Clearly this defines a mapping \( \psi \) 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 \( \bar{x}_1, \ldots, \bar{x}_r \) belong to \( \bar{D} \).

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

Hence the number of equivalence classes of \( S \) is equal to \( N_r'(a) \). However, by the lemma each equivalence class consists of \( |J|^{-1} \) elements and therefore \( N_r'(a) = |J|^{-1} N_r(a) \), 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

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

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

\[
\sum_{d \in D} N_r(b) = d^r
\]

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

Next we observe that

\[
N_{r+1}(a) = \sum_{b \in D} N_r(b)
\]

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

\[
x_1 \cdots x_r = b, \quad x_{r+1} = b^{-1}a
\]

in which \( x_1, \ldots, x_r \) and \( b^{-1}a \) belong to \( D \).

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

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

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 \( x_1 \cdots x_{r-1}(x,c) = b \) and \( x,c \in D \), which establishes that \( N_r(a) = N_r(b) \). Hence from (6) we obtain

\[
N_{r+1}(a) = d^r - hN_r(a)
\]

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

\[
N_r(a) = d^{r-1} - hd^{r-2} + \cdots + (-1)^{r-2}h^{r-3}d + (-1)^{r-1}h^{r-2}N_1(a).
\]

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

\[
x_1^{m_1} \cdots x_r^{m_r} = a
\]

where \( a \in G \) and \( x_1, \ldots, x_r \), belong to \( D \), a nonempty subset of \( G \).

Consider the following properties which an integer \( m \) may possess.

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

(b) \( x^m \in G \setminus D \) 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 \( m_1, \ldots, m_r \) are integers such that for some \( i \) the \( m_i \)-th power map is a bijection of \( G_0 \), then

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

Further if \( m_1, \ldots, m_r \) satisfy either (a) or (b) and at least one satisfies (a), then

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

**Proof.** If \( z_1' \cdots z_r' = a^* \) for \( z_1, \cdots, z_r \) in \( D^* \), then \( z_1'' \cdots z_r'' = a \) and \( b_1'' \cdots b_r'' = a_0 \), where \( z_1, \cdots, z_r \) 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 \( b_1'' \cdots b_r'' = a_0 \) is \( |G_0|^{-1} \) and as \( D^* = D \cdot G_0 \) we obtain (10).

Now let \( k \geq 1 \) be the number of \( m_i \) which satisfy (\( \alpha \)). Then for any solution \( (x_1, \cdots, x_r) \) of (9) the terms of \( z_1'' \cdots z_r'' \) 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 \( \alpha^r - k \) distinct solutions of (9) and hence by (3)

\[
\mathfrak{N}_{r}(a) = \alpha^r \mathfrak{N}_{k}(a) = \frac{\alpha^r}{g} \left( 1 + \frac{(-1)^k \gamma(a)}{|G:H| - 1} \right)
\]

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

\[
\mathfrak{N}_{r}^D(a) = \prod_{i=1}^{n} \mathfrak{N}_{r}^{D_i}(a_i).
\]

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 (a) or (b) and at least one satisfies (a) with respect to each group \( G_i \) and subset \( D_i \), then (11) and (12) yield

\[
\mathfrak{N}_{r}^{D_i}(a) = \frac{\alpha^r}{g} \prod_{i=1}^{n} \left( 1 + \frac{\gamma(a_i) \rho(m_i) \cdots \rho(m_r)}{|G_i:H_i| - 1} \right).
\]

3. Applications.

(a) Let \( \Delta \) 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 \( \mathfrak{N}_*(a) \) 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 \( \Delta \) 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 \( \mathfrak{N}_*(a) \) is given by (3).

(c) Let \( \Delta \) 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 \( \mathfrak{N}_r^D(a) \) for a nilpotent group \( G \) we may assume \( G \) is a \( p \)-group.
Let $\mathfrak{N}$ denote the class of $p$-groups $G$ for which $H$, the elements not of maximal order, form a subgroup of $G$. Clearly $\mathfrak{N}$ 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 $G \in \mathfrak{N}$, 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 $(\alpha)$ since the mapping $x \rightarrow x^m$ is an order preserving bijection of any $p$-group. On the other hand, if $p \mid m$, then $m$ satisfies $(\beta)$. Thus if $G \in \mathfrak{N}$ and $m_1, \ldots, m_r$ are integers whose greatest common divisor is prime with $p$, then $\mathfrak{N}^p(a)$ is given by (11).

It is now easy to determine $\mathfrak{N}^p(a)$ for any integers $m_1, \ldots, m_r$ if $G$ is a $p$-abelian $p$-group, that is, $(ab)^p = a^pb^p$ for all elements $a, b$ in $G$ [4]. For suppose $p^r$ is the highest power of $p$ dividing $m_1, \ldots, m_r$ and let $m_i/p^r = m'_i$ for $i = 1, \ldots, r$. If $x_1^{m'_1} \cdot \cdots \cdot x_r^{m'_r} = a$, then $(x_1^{m'_1} \cdot \cdots \cdot x_r^{m'_r})^{p^r} = a$ since $G$ is $p$-abelian. For $b$ in $G$ let $\mathfrak{N}^p(b)$ denote the number of solutions of $x_1^{m'_1} \cdot \cdots \cdot x_r^{m'_r} = b$, where $x_1, \ldots, x_r$ belong to $D$. Then clearly

$$\mathfrak{N}^p(a) = \sum_{b^{p^r} = a} \mathfrak{N}^p(b).$$

Now let $f$ denote the endomorphism of $G$ defined by $f(c) = c^a$ for $c$ in $G$. We may assume that $a \in \text{Im} f$ for otherwise $\mathfrak{N}^p(a) = 0$. If $a = b_0^a$ for $b_0$ in $G$, then $f(b) = a$ if and only if $b \in b_0(Ker f)$. If $p^r \leq$ exponent $G$, then $\mathfrak{N}^p(a) = d^r$. Suppose that $p^r <$ exponent $G$. Then $\text{Ker} f \subseteq G \setminus D = H$ and since $G$ is $p$-abelian, $H$ is a subgroup of $G$. However, $(m'_1, \ldots, m'_r, p) = 1$ and hence (11) shows that $\mathfrak{N}^p(b)$ depends only on whether $b \in D$ or $b \in H$. Therefore, $\mathfrak{N}^p(b) = \mathfrak{N}^p(b_0)$ for all $b$ in $b_0(Ker f)$ and from (14) we obtain

$$\mathfrak{N}^p(a) = |\text{Ker} f| \mathfrak{N}^p(b_0) \quad \text{where} \quad a = b_0^a.$$

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 $G \in \mathfrak{N}$ if and only if $G_i \in \mathfrak{N}$ for $i = 1, 2$.

(ii) If exponent $G_1 > $ exponent $G_2$, then $G \in \mathfrak{N}$ if and only if $G_1 \in \mathfrak{N}$.

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 $\mathfrak{N}^p(a)$ 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 $m_1, \ldots, m_r$ are integers such that $(m_1, \ldots, m_r, p) = 1$, then

$$\mathfrak{N}^p(a) = \frac{(p^n - p^{n-k})^r}{p^n} \left( 1 + \gamma(a)\rho(m_1) \cdots \rho(m_r) \frac{p^r - 1^r}{p^r - 1} \right).$$
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 $\mathfrak{P}(a)$ 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 $\mathfrak{P}(a)$ for arbitrary integers $m_1, \ldots, m_*$. 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 $N^\rho(a)$ apply when $a \in G_0$. If $a \notin G_0$, then $N^\rho(a) = 0$ 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 $N^\rho(a)$ 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

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

is what has been denoted by $N^\rho_R(a)$ 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 $N^\rho_U(a)$ is reduced to the case where $R$ is semisimple. Then (12) shows that it suffices to determine $N^\rho_U(a)$ for $F_*$, the ring of $n \times n$ matrices over a finite field $F$.

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

If $F$ is a field, then $U = F \setminus \{0\}$ and $N^\rho_U(a)$ 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 $N^\rho_U(a)$ 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

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

where $0 \leq x_i < n$ and $(x_i, n) = 1$ for $i = 1, \ldots, n$. This number is just $N^\rho_U(a)$ with respect to the ring $Z/(n)$. (In this context an equivalent formula for $N^\rho_U(a)$ 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 \(m_1, \ldots, m_r\) be integers such that \((m_1, \ldots, m_r) = 1\) and denote by \(\mathcal{N}_r(a)\) the number of solutions of the congruence

\[
m_1x_1 + \cdots + m_rx_r = a \pmod{n}
\]

where \(0 \leq x_i < n\) and \((x_i, n) = 1\) for \(i = 1, \ldots, r\). 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

\[
\mathcal{N}_r(a) = \frac{\phi'(n)}{n} \prod_{p \mid n} \left( 1 + \frac{\gamma_p(a) \prod_{i=1}^r \gamma_p(m_i)}{(p - 1)^r} \right),
\]

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

References


Jacobson: Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903

Williams: Department of Mathematics, Carleton University, Ottawa, Ontario, Canada