NORMAL SUBSETS OF FINITE GROUPS[1]

BY
Ernst Snapper

Introduction

G stands for a finite group of order g. If T is a non-empty subset of G and n a rational integer, we denote the solution set of the equation $x^n \in T$ by $S(T, n)$; i.e.,

$$S(T, n) = \{\sigma \mid \sigma \in G, \sigma^n \in T\}.$$

The absolute value sign $|T|$, $|S(T, n)|$, etc., indicates the number of elements in the set inside the sign. We refer to the following theorem as "the Frobenius theorem": *If C is a class of conjugate elements of G, $|S(C, n)|$ is divisible by* $(|C|n, g)$. See [2, page 136], for an elegant proof of this theorem; the notation $S(T, n)$ is taken from the same source. (Square brackets refer to the references.)

The solution set $S(C, n)$ is closed under inner automorphism of G, i.e., it is a *normal subset* of G. Consequently, the Frobenius theorem gives information about the number of elements in certain normal subsets of the group. In the present paper, we obtain information about the size of many other normal subsets of G, most of which have nothing to do with solving equations.

The main tool is Theorem 1.1 of [4], reviewed in Section 1. It enables us to associate a numerical polynomial with many a normal subset of G (Sections 2, 3); and this polynomial gives the information about the size of that set (Section 4). In Section 5, we discuss the connection with the Frobenius theorem.

1. Review of [4]

A permutation representation (G, D) of G consists of a finite, non-empty set D on which G acts on the left. The unit element of G is unit operator and, if $\rho, \sigma \in G$ and $d \in D$, $(\rho\sigma)d = \rho(\sigma d)$. We introduce a variable x_i for each divisor i of g, and consider the polynomial ring R in these variables with rational numbers as coefficients. (Divisor always means *positive* divisor, and $g = |G|$.) An element $\sigma \in G$ gives rise to a permutation of the set D, and hence to the partitioning of D into the cycles of that permutation. We refer to these cycles also as the cycles of σ. The monomial $M(\sigma) \in R$ of σ is defined as $\prod_{[g]} x_i^{c_i(\sigma)}$; the product $\prod_{[g]}$ is taken over the set $[g]$ of all divisors i of g, and $c_i(\sigma)$ is the number of cycles of σ whose length is i. We observe that every cycle of σ has a length which divides the order of σ, and

Received June 5, 1967.

[1] This research was supported in part by a National Science Foundation grant.

hence divides g. Consequently, every cycle of σ contributes a factor to the monomial $M(\sigma)$. The polynomial $(1 \div g) \sum_G M(\sigma)$ of R, where the sum $\sum_G$ is taken over all $\sigma \in G$, is the *cycle index* $P(G, D)$ of the representation (G, D). This cycle index is used in combinatorial mathematics in the case that (G, D) is faithful (i.e., when the unit element of G is the only unit operator [1]), but is equally useful when (G, D) is not faithful.

A polynomial of R is called *numerical* if its value is an integer, when integers are substituted for the variables. (Integer always means rational integer.) The cycle index $P(G, D)$ is practically never numerical (Section 1 of [4]). Consider now, for each positive integer i, the integral polynomial $F_i = \sum_{[i]} jx_j$, where the sum $\sum_{[i]}$ is taken over the set $[i]$ of all divisors j of i. For instance, $F_6 = x_1 + 2x_2 + 3x_3 + 6x_6$. Theorem 1.1 of [4] states that, *if each variable x_i of $P(G, D)$ is replaced by the polynomial F_i, the resulting polynomial $q(G, D)$ of R is numerical.* We refer to $q(G, D)$ as the *numerical polynomial of the permutation representation* (G, D).

We shall use the following notation.

Notation 1.1. (a) If k is positive integer, $[k]$ denotes the set of divisors of k. We have used this notation already in $[g]$ and $[i]$.

(b) If E is a non empty set, $\prod_E$ indicates that the product is taken over all elements of E; and $\sum_E$ indicates that the sum is taken over all elements of E. We have used this notation already in $\prod_{[g]}$, $\sum_{[i]}$ and $\sum_G$.

Observe that in $\prod_E$ and $\sum_E$ the E is not a dummy variable. It should be clear from the context what the dummy variables are. For instance,

$$P(G, D) = (1 \div g) \sum_G (\prod_{[g]} x_i^{c_i(\sigma)})$$

and

$$q(G, D) = (1 \div g) \sum_G (\prod_{[g]} F_i^{c_i(\sigma)}).$$

2. The sets $U(\pi, B)$ and $V(\pi, B)$

We choose a set π of prime divisors of g; π may consist of all the primes of g or may be empty. We also choose a non-empty set B of divisors of g *which are π-numbers*; i.e., each $s \in B$ divides g and all the prime divisors of s belong to π. If $\pi = \emptyset$, the only π-number is 1, and hence then $B = \{1\}$. No matter how π is chosen, 1 counts as a π-number. We follow [3, page 125] and call the largest π-number which divides a positive integer i, the *π-share* of i. We mean by the π-share of a finite, non-empty set Y, the π-share of $| Y |$.

We consider a permutation representation (G, D). The cycles of $\sigma \in G$ all have lengths which divide g, but they may of course not be π-numbers. The π-share of a cycle Y of σ has just been defined as the π-share of the length $| Y |$ of that cycle.

Definition 2.1. $U(\pi, B) = \{\sigma \mid \sigma \in G$, the π-share of every cycle of σ belongs to $B.\}$

It is clear that $U(\pi, B)$ may be empty. We now define the set $V(\pi, B) \subset U(\pi, B)$, which hence may also be empty.

DEFINITION 2.2. $V(\pi, B) = \{\sigma \mid \sigma \in U(\pi, B)$, every $s \in B$ is the π-share of at least one cycle of $\sigma.\}$

We denote the cyclic subgroup, generated by an element σ of G, by $\langle\sigma\rangle$.

DEFINITION 2.3. A subset T of G is called closed if $\sigma \in T$ implies that all the generators of $\langle\sigma\rangle$ also belong to T.

It is convenient to regard the empty subset of G as both normal and closed.

PROPOSITION 2.1. *The sets $U(\pi, B)$ and $V(\pi, B)$ are normal and closed. Furthermore, $U(\pi, B)$ is the disjoint union of the sets $V(\pi, A)$ where A runs through the non empty subsets of B.*

Proof. If ρ and σ are conjugate elements of G, i.e., if they correspond under an inner automorphism of G, the permutations of D to which they give rise are conjugate in the symmetric group of all permutations of D. Consequently, the monomials $M(\rho)$ and $M(\sigma)$ of Section 1 are then the same, which shows that U and V are normal. (We omit (π, B) when this can not lead to confusion.) If $\langle\rho\rangle = \langle\sigma\rangle$, the two partitionings of D into the cycles of ρ respectively σ, are the same and hence again $M(\rho) = M(\sigma)$. This shows that U and V are closed. The remainder of Proposition 2.1 is an immediate consequence of Definitions 2.1 and 2.2.

3. The numerical polynomials of U and V

We study the sets $U(\pi, B)$ and $V(\pi, B)$ of the previous section. To each $\sigma \in U(\pi, B)$ we associate the monomial $M(\pi, B, \sigma) \in R$, defined by: $M(\pi, B, \sigma) = \prod_B x_i^{\gamma_i(\sigma)}$ where the product $\prod_B$ is taken over all $i \in B$, and where $\gamma_i(\sigma)$ is the number of cycles of σ whose π-share is i. If π consists of all the prime divisors of g, $\gamma_i(\sigma)$ is the number of cycles of σ whose length is i. If furtherfore B is the set of all divisors of g, $M(\pi, B, \sigma)$ is the monomial $M(\sigma)$ of Section 1.

We denote by π' the set of prime divisors of g which is complementary to π; and by α the π'-share of g. If $U(\pi, B) \neq \emptyset$, we define the polynomial $q(U(\pi, B)) \in R$ as $(1 \div \alpha) \sum_U M(\pi, B, \sigma)$; the sum $\sum_U$ is taken over all $\sigma \in U(\pi, B)$. If $U(\pi, B) = \emptyset$, we define $q(U(\pi, B)) = 0 \in R$.

If π consists of all the primes of g, $\alpha = 1$, and hence $q(U)$ is then an integral polynomial. If furthermore B is the set of all divisors of g, $q(U) = gP(G, D)$ (see Section 1). In general, however, the coefficients of $q(U)$ are not integers.

The polynomial $q(V(\pi, B))$ is defined in the same way. If $V \neq \emptyset$,

$$q(V(\pi, B)) = (1 \div \alpha) \sum_V M(\pi, B, \sigma) \in R,$$

where the sum $\sum_V$ is taken over all $\sigma \in V(\pi, B)$. If

$$V = \emptyset, \qquad q(V(\pi, B)) = 0 \in R.$$

THEOREM 3.1. *The polynomials $q(U(\pi, B))$ and $q(V(\pi, B))$ are numerical.*

Proof. We denote the π-share of g by β and, from now on, will use Notation 1.1 without explanation. In particular, $[\beta]$ is the set of divisors of β and hence $B \subset [\beta]$. We first deal with $q(U)$.

Case 1. $B = [\beta]$. Since $U(\pi, [\beta]) = G$,

$$q(U(\pi, [\beta])) = (1 \div \alpha) \sum_G (\prod_{[\beta]} x_i^{\gamma_i(\sigma)})$$

where we use Notation 1.1, and where $\gamma_i(\sigma)$ denotes again the number of cycles of σ whose π-share is i.

We choose an integer y_i for each divisor i of β, and have to show that

$$\sum_G (\prod_{[\beta]} y_i^{\gamma_i(\sigma)}) \equiv 0 \pmod{\alpha}.$$

Hereto, we consider the system of congruences $F_i \equiv y_i \pmod{\alpha}$, where $F_i = \sum_{[i]} jx_j$ is the integral polynomial of Section 1; there is one congruence for each divisor i of β. It is trivial that this system of congruences has a solution in integers z_j, since each j in $\sum_{[i]} jx_j$ divides β and hence is a unit modulo α. For $i = 1$, we choose $z_1 = y_1$. We then solve the congruences $y_1 + px_p \equiv y_p \pmod{\alpha}$, where p is a prime divisor of β; this determines the integers z_p. Next we solve the congruences $F_i \equiv y_i \pmod{\alpha}$ where the divisor i of β has two prime divisors (not necessarily distinct); and so on. (Actually, the solution is unique modulo α.) Let then $\{z_j \mid j \in [\beta]\}$ be a solution in integers of this system of congruences. We also put $z_j = 0$ when j divides g but $j \notin [\beta]$.

We now return to the numerical polynomial

$$q(G, D) = (1 \div g) \sum_G (\prod_{[g]} F_i^{c_i(\sigma)}) \qquad \text{(Section 1.)}$$

We substitute z_j for x_j and obtain, *since $q(G, D)$ is numerical* and $\alpha \mid g$, that

$$\sum_G (\prod_{[g]} (F_i(z))^{c_i(\sigma)}) \equiv 0 \pmod{\alpha}.$$

(We write $F_i(z)$ for $F_i(z_1, \cdots, z_i)$.) It will hence be sufficient to show that, for each $\sigma \in G$,

$$\prod_{[g]} (F_i(z))^{c_i(\sigma)} \equiv \prod_{[\beta]} y_i^{\gamma_i(\sigma)} \pmod{\alpha}.$$

Select $\sigma \in G$. If a cycle of σ has π-share i, then $i \mid \beta$ and the length of that cycle is ai, where $a \mid \alpha$. Consequently,

$$\gamma_i(\sigma) = \sum_{[\alpha]} c_{ai}(\sigma) \qquad \text{(Notation 1.1)},$$

and hence

$$y_i^{\gamma_i(\sigma)} = \prod_{[\alpha]} y_i^{c_{ai}(\sigma)} \qquad \text{(Notation 1.1)}.$$

We conclude that

$$\prod_{[\beta]} y_i^{\gamma_i(\sigma)} = \prod_{[\beta]} \prod_{[\alpha]} y_i^{c_{ai}(\sigma)}.$$

In this product, i runs through the divisors of β and a runs through the divisors of α, while i is the π-share of ai. Consequently,

$$\textstyle\prod_{[\beta]} y_i^{\gamma i(\sigma)} = \prod_{[g]} y_{i(\pi)}^{c_i(\sigma)},$$

where the product $\prod_{[g]}$ is taken over all divisors i of g and where $i(\pi)$ denotes the π-share of i.

We now compute $F_i(z) = \sum_{[i]} jz_j$, where $i \mid g$. We put $i = ai(\pi)$, where a is the π'-share of i and $i(\pi)$ is again the π-share of i. Since $z_j = 0$ when $j \nmid \beta$, $F_i(z) = \sum' jz_j$ where the sum $\sum'$ is now taken over only the divisors j of $i(\pi)$. The congruences, discussed above, have $\{z_j \mid j \text{ divides } \beta\}$ as solution and hence $F_i(z) = y_{i(\pi)} \pmod{\alpha}$. We conclude that

$$\textstyle\prod_{[g]} (F_i(z))^{c_i(\sigma)} \equiv \prod_{[g]} y_{i(\pi)}^{c_i(\sigma)} \pmod{\alpha}$$

and Case 1 is done.

Case 2. The set B is an arbitrary non-empty subset of $[\beta]$. In the numerical polynomial $q(U(\pi, [\beta]))$ of Case 1, we put $x_i = 0$ if $i \notin B$. The resulting numerical polynomial is $q(U(\pi, B))$ and Case 2 is done.

We now discuss $q(V(\pi, B))$. If $|B| = 1$, $V(\pi, B) = U(\pi, B)$ and hence $q(V(\pi, B))$ is then numerical. We now make induction on $|B|$ and assume that $q(V(\pi, A))$ is numerical for all proper, non-empty subsets A of B. By Proposition 2.1,

$$q(U(\pi, B)) = q(V(\pi, B)) + \textstyle\sum q(V(\pi, A)),$$

where the sum $\sum$ is taken over all proper, non-empty subsets A of B. Since $q(U(\pi, B))$ is numerical and, by induction, each $q(V(\pi, A))$ is numerical, $q(V(\pi, B))$ is numerical. Done.

Example 3.1. We return to Case 1 of the proof of Theorem 3.1, where $B = [\beta]$. We saw that then

$$q(U(\pi, [\beta])) = (1 \div \alpha) \textstyle\sum_G (\prod_{[\beta]} x_i^{\gamma i(\sigma)}).$$

We showed that $\prod_{[\beta]} y_i^{\gamma i(\sigma)} = \prod_{[g]} y_{i(\pi)}^{c_i(\sigma)}$, and the same reasoning shows that $\prod_{[\beta]} x_i^{\gamma i(\sigma)} = \prod_{[g]} x_{i(\pi)}^{c_i(\sigma)}$. Consequently,

$$q(U(\pi, [\beta])) = (1 \div \alpha) \textstyle\sum_G (\prod_{[g]} x_{i(\pi)}^{c_i(\sigma)}).$$

We now carry out the substitution $x_i = x_{i(\pi)}$ in the cycle index

$$P(G, D) = (1 \div g) \textstyle\sum_G (\prod_{[g]} x_i^{c_i(\sigma)}) \qquad \text{(Section 1)}$$

We obtain the polynomial

$$\begin{aligned} P(G, D; x_i = x_{i(\pi)}) &= (1 \div g) \textstyle\sum_G (\prod_{[g]} x_{i(\pi)}^{c_i(\sigma)}) \\ &= (\alpha \div g) q(U(\pi, [\beta])) = (1 \div \beta) q(U(\pi, [\beta])). \end{aligned}$$

Consequently, $\beta P(G, D; x_i = x_{i(\pi)})$ is the numerical polynomial $q(U(\pi, [\beta]))$ which proves:

THEOREM 3.2. *Let π be a set of prime divisors of g and β that π-share of g. The polynomial $\beta P(G, D;\, x_i = x_{i(\pi)})$ is numerical. Here, $i(\pi)$ is the π-share of i.*

Theorem 3.2 gives an easy method to obtain a numerical polynomial from the *non* numerical cycle index $P(G, D)$ for each set of prime divisors π of g. If $\pi = \emptyset$, $\beta = 1$ and $x_{i(\pi)} = x_1$. Hence, in this case, we merely put all the variables of $P(G, D)$ equal to one another. The resulting numerical polynomial is $(1 \div g) \sum_G x^{e(\sigma)}$, where $e(\sigma)$ is the total number of cycles of σ. This polynomial was also obtained in Section 1 of [4].

Example 3.2. Suppose that B consists of only one divisor i of β. Then,

$$U(\pi, \{i\}) = V(\pi, \{i\})$$

and

$$q(U(\pi, \{i\})) = (1 \div \alpha) \textstyle\sum_U x_i^{\gamma_i(\sigma)}.$$

There is only one variable x_i and we write x for x_i. Furthermore, since $\sigma \in U(\pi, \{i\})$, $\gamma_i(\sigma)$ is the total number of cycles $e(\sigma)$ of σ. We hence obtain the numerical polynomial $(1 \div \alpha) \sum_U x^{e(\sigma)}$. If $\pi = \emptyset$, then $i = 1$ and $U(\emptyset, \{1\}) = G$, and we obtain the polynomial $(1 \div g) \sum_G x^{e(\sigma)}$ of Example 3.1.

Example 3.3. Let (G, D) be the regular representation; i.e., $D = G$ and G acts on G by left multiplication. Then,

$$U(\pi, B) = \{\sigma \mid \sigma \in G, \quad \text{the } \pi\text{-share of the order of } \sigma \text{ belongs to } B\};$$

and $V(\pi, B) = \emptyset$ if $|B| > 1$. Consequently, by Proposition 2.1, $U(\pi, B)$ is the disjoint union of the sets $U(\pi, \{i\})$ for $i \in B$; and $q(U(\pi, B))$ is the sum of the polynomials $q(U(\pi, \{i\})$. Furthermore, by Example 3.2,

$$q(U(\pi, \{i\})) = (1 \div \alpha) \textstyle\sum_U x^{e(\sigma)};$$

in the present case, $e(\sigma) = g \div$ order (σ), and U consists of those group elements whose order is equal to ai where $a \mid \alpha$. It follows that, if k_s denotes the number of elements of G of order s,

$$q(U(\pi, \{i\})) = (1 \div \alpha) \textstyle\sum_{[\alpha]} k_{ai} x^{g \div ai}$$

where the sum $\sum_{[\alpha]}$ is taken over all divisors a of α. If we put $x = 1$ in this numerical polynomial, we conclude that $\sum_{[\alpha]} k_{ai} \equiv 0 \pmod{\alpha}$. If $\alpha = p^n$ where p is a prime, we obtain the congruence

$$k_i + k_{pi} + \cdots + k_{p^n i} \equiv 0 \pmod{p^n}$$

of Section 2 of [4].

4. Sizes of U, V and related sets

If we put all the variables in the numerical polynomials $q(U(\pi, B))$ and $q(V(\pi, V))$ equal to 1, we obtain:

THEOREM 4.1. $|U(\pi, B)| \equiv 0 \pmod{\alpha}$ *and* $|V(\pi, B)| \equiv 0 \pmod{\alpha}$.

We want to strengthen Theorem 4.1 so that it can handle the Frobenius theorem. Hereto, we introduce the number $\delta(e, E)$, where e is a positive integer and E is a set of divisors of e; E may be empty or may consist of all the divisors of e. Let $\psi = p_1^{m_1} \cdots p_k^{m_k}$ be the factorization into prime factors of the greatest common divisor ψ of all those divisors of e which do *not* belong to E. *We define*

$$\delta(e, E) = p_1^{m_1-1} \cdots p_k^{m_k-1}.$$

If $\psi = 1$, we put $\delta(e, E) = 1$; if E consists of all the divisors of e, we put $\delta(e, E) = e$. Under all circumstances $\delta(e, E) \mid e$.

Example 4.1. Let $e = p_1^{n_1} \cdots p_w^{n_w}$ be the factorization of e into prime factors. We denote $n_1 + \cdots + n_w = n$ and call n "the order of e"; for instance, the order of 1 is 0. The greatest common divisor of those divisors of e whose order is h $(0 \leq h \leq n)$, is equal to $p_1^{k_1} \cdots p_w^{k_w}$, where $k_i = \max(n_i - n + h, 0)$ for $i = 1, \cdots, w$. It follows easily that this number $p_1^{k_1} \cdots p_w^{k_w}$ is equal to $\delta(e, E)$, if E consists of al divisors of e whose order is at most h. For instance, if $e = p^n$ and $0 \leq h \leq n$, then $E = \{1, p, \cdots, p^h\}$ and $\delta(e, E) = p^h$. We also observe that, if e is arbitrary but E consists of precisely one divisor of e, $\delta(e, E) = 1$.

The reason for introducing the number $\delta(e, E)$ is the following lemma; φ denotes the Euler number.

Lemma 4.1. *If $\sigma \in G$ and $\sigma \notin U(\pi, B)$, then*

$$\varphi(\text{order }(\sigma)) \equiv 0 \pmod{\delta(\beta, B)}.$$

Proof. Since $\sigma \notin U(\pi, B)$, B can not consist of all the divisors of β (see Example 3.1), and it will be sufficient to show that there exists a divisor r of β, satisfying: (1) $r \notin B$; (2) if $r = p_1^{k_1} \cdots p_w^{k_w}$ is the factorization of r into prime factors,

$$\varphi(\text{order }(\sigma)) \equiv 0 \pmod{p_1^{k_1-1} \cdots p_w^{k_w-1}}.$$

Since $\sigma \notin U(\pi, B)$, σ has a cycle whose π-share r does not belong to B; this shows that r has property (1). Furthermore, the length of that cycle is divisible by r and in turn divides order (σ). Consequently, $r \mid \text{order }(\sigma)$ from which it follows that $\varphi(r) \mid \varphi(\text{order }(\sigma))$. Since $p_1^{k_1-1} \cdots p_w^{k_w-1} \mid \varphi(r)$, r has also property (2). Done.

Corollary 4.1. *Let T be a closed subset of G (Definition 2.3) and $T \cap U(\pi, B) = \emptyset$. Then,* $|T| \equiv 0 \pmod{\delta(\beta, B)}$.

Proof. The corollary is trivial when $T = \emptyset$ and hence we assume that $T \neq \emptyset$. We consider the partitioning Ω of T, corresponding to the equivalence relation "$\rho \sim \sigma$ if $\langle\rho\rangle = \langle\sigma\rangle$". Every element $\sigma \in T$ belongs to a unique "cycle" Ω_σ of Ω and, since T is closed, $|\Omega_\sigma| = \varphi(\text{order }(\sigma))$. By Lemma 4.1, $|\Omega_\sigma| \equiv 0 \pmod{\delta(\beta, B)}$. Done.

We now combine Theorem 4.1 and Corollary 4.1. Hereto, we choose two sets of prime divisors π_1 and π_2 of g, where $\pi_1 \cap \pi_2 = \emptyset$. We choose a set of divisors B_1 of the π_1-share β_1 of g, and a set of divisors B_2 of the π_2-share β_2 of g. We also denote the set of prime divisors of g which do not occur in $\pi_1 \cup \pi_2$ by π, and the π-share of g by α.

THEOREM 4.2. *$|U(\pi_1, B_1) \cap U(\pi_2, B_2)|$ is divisible by $\alpha\delta(\beta_1, B_1)\delta(\beta_2, B_2)$.*

Proof. We put $|U(\pi_1, B_1) \cap U(\pi_2, B_2)| = c$ and, since α, $\delta(\beta_1, B_1)$ and $\delta(\beta_2, B_2)$ are relatively prime in pairs, we only have to show that c is divisible by each of these three numbers individually. We observe that

$$U(\pi_1, B_1) \cap U(\pi_2, B_2) = U(\pi_1 \cup \pi_2, B_1 B_2),$$

where $B_1 B_2 = \{rs \mid r \in B_1 \text{ and } s \in B_2\}$. Consequently, Theorem 4.1 gives that $\alpha \mid c$. Since the sets $U(\pi_1, B_1)$ and $U(\pi_2, B_2)$ play symmetrical roles, there only remains to be shown that $\delta(\beta_1, B_1) \mid c$. Using again Theorem 4.1, $|U(\pi_2, B_2)|$ is divisible by the π_2'-share of g, where π_2' is the set of prime divisors of g which is complementary to π_2. Since $\pi_1 \subset \pi_2'$, $|U(\pi_2, B_2)|$ is divisible by β_1 and hence certainly by $\delta(\beta_1, B_1)$. We denote the subset of $U(\pi_2, B_2)$ whose elements do not belong to $U(\pi_1, B_1)$ by T, and hence we only have to prove that $|T|$ is divisible by $\delta(\beta_1, B_1)$. Since $U(\pi_1, B_1)$ and $U(\pi_2, B_2)$ are closed (Proposition 2.1), and intersections of closed sets and complements (in G) of closed sets are evidently closed, T is closed. Hence, by Corollary 4.1, $|T|$ is divisible by $\delta(\beta_1, B_1)$. Done.

COROLLARY 4.2. *In the notation of Theorem* 4.1,

$$|U(\pi, B)| \equiv 0 \pmod{\alpha\delta(\beta, B)}.$$

Proof. Using Theorem 4.1 and the fact that α and $\delta(\beta, B)$ are relatively prime, we only have to show that $|U(\pi, B)| \equiv 0 \pmod{\delta(\beta, B)}$. If we choose in Theorem 4.2, B_2 equal to the set of all divisors of β_2, $U(\pi_2, B_2) = G$ and we conclude that

$$|U(\pi_1, B_1)| \equiv 0 \pmod{\delta(\beta_1, B_1)}.$$

Done.

THEOREM 4.3. $|U(\pi_1, B_1) \cap V(\pi_2, B_2)| \equiv 0 \pmod{\delta(\beta_1, B_1)}$.

Proof. The reasoning in the proof of Theorem 4.2 that $\delta(\beta_1, B_1)$ divides $|U(\pi_2, B_2)|$, now gives that $|V(\pi_2, B_2)| \equiv 0 \pmod{\delta(\beta_1, B_1)}$. We conclude again from Proposition 2.1 that the subset T of $V(\pi_2, B_2)$, whose elements do not belong to $U(\pi_1, B_1)$, is closed. Consequently, by Corollary 4.1, $|T| \equiv 0 \pmod{\delta(\beta_1, B_1)}$, and the theorem follows.

Example 4.2. We study the set $U(\pi, B)$ and choose a prime divisor p of g, where $p \notin \pi$. If p^n is the p-share of g, every cycle of an element $\sigma \in G$ has p-share equal to p^h, where $0 \leq h \leq n$. We now consider only those elements of $U(\pi, B)$ whose cycles have p-share at most equal to p^h for some fixed $0 \leq h \leq n$. These elements form the set

$$T = U(\pi, B) \cap U(\{p\}, \{1, p, \cdots, p^h\})$$

and hence, by Theorem 4.2 and Example 4.1, $| T | \equiv 0 \pmod{\delta(\beta, B)p^h}$. If B consists of only one divisor of β, $\delta(\beta, B) = 1$ (Example 4.1) and we can only conclude that $| T | \equiv 0 \pmod{p^h}$.

Example 4.3. Let (G, D) be the regular representation, and p a prime divisor of g where p^n is the p-share of g. Suppose that s is a divisor of g where $p \nmid s$. We choose for π the set of prime divisors of g, distinct from p, and choose $B = \{s\}$. The set T of Example 4.2 now consists of those elements of G whose order is $p^m s$, where $0 \leq m \leq h$. Hence, if k_i has the same meaning as in Example 3.3,

$$| T | = k_s + k_{ps} + \cdots + k_{p^h s} \equiv 0 \pmod{p^h}$$

for $h = 1, \cdots, n$. These congruences express the Frobenius theorem in the special case that $C = \{1\}$ (see the Introduction), as proved in Proposition 2.1 of [4].

5. The Frobenius theorem

See the introduction for the formulation "$| S(C, n)|$ is divisible by $(| C | n, g)$" of this theorem. It follows immediately that, if T is a normal subset of G, $| S(T, n)|$ is divisible by (n, g); merely partition T into classes of conjugate elements and apply the Frobenius theorem to each class. If (G, D) is a permutation representation, its kernel K is defined as the normal subgroup of G whose elements leave all points of D fixed. Hence, by the above remark, $| S(K, n)|$ is divisible by (n, g). This result can also be obtained as follows from Example 4.2.

It is clear that $S(K, n) = S(K, (n, g))$ and hence we only have to show: If $n \mid g$, $| S(K, n)| \equiv 0 \pmod{n}$. Let $M(\sigma) = \prod_{[g]} x_i^{c_i(\sigma)}$ be the monomial of an element $\sigma \in G$ (Section 1). The number of points of D, left fixed by σ^n, is equal to $\sum_{[n]} jc_j(\sigma)$ where the sum is taken over the set $[n]$ of all divisors j of n. Hence $\sigma^n \in K$ if and only if $\sum_{[n]} jc_j(\sigma) = | D |$. Since, obviously, $\sum_{[g]} jc_j(\sigma) = | D |$, this means that every cycle of σ has a length which divides n. Consequently, we have to show:

Proposition 5.1. *Let* $n \mid g$ *and* $T = \{\sigma \mid \sigma \in G$, *every cycle of* σ *has a length which divides* $n\}$. *Then*, $| T | \equiv 0 \pmod{n}$.

Proof. We choose a prime divisor p of n and denote the p-share of n by p^h. We only have to show that $| T | \equiv 0 \pmod{p^h}$. Now

$$T = U(\pi, B) \cap U(\{p\}, \{1, p, \cdots, p^h\}),$$

where π is the set of prime divisors of g different from p, and where B consists of all the divisors of $n \div p^h$. By Example 4.2, $| T | \equiv 0 \pmod{p^h}$. Done.

If K is an arbitrary normal subgroup of G, the transitive permutation representation $(G, G/K)$ has K as kernel, and hence $|S(K, n)|$ is divisible by (n, g). Although it is easy to prove the general Frobenius theorem from this special case, we are not able to do this by the methods of this paper. The reason is that the only normal subsets of G which our theory can handle directly, are the closed ones; this could have been predicted from Proposition 2.1. Observe that the normal set $S(K, n)$, above is closed. In order to obtain a theory which can deal directly with *all* the normal subsets of G, it will be necessary to extend the theory of the cycle index, in particular the theorems of Pólya and de Bruyn [1], from permutation representations to linear representations.

References

1. N. G. de Bruijn, *Polya's theory of counting,* Applied Combinatorial Mathematics, Wiley, 1964, Chapter 5, pp. 144–184.
2. Marshall Hall Jr., *The theory of groups*, Macmillan, New York, 1959.
3. Eugene Schenkman, *Group theory,* Van Nostrand, Princeton, New Jersey, 1965.
4. E. Snapper, *The polynomial of a permutation representation*, J. Combinatorial Theory, vol. 5 (1968), pp. 105–114.

Dartmouth College
Hanover, New Hampshire