A COMBINATORIAL IDENTITY WITH APPLICATIONS TO REPRESENTATION THEORY

BY
ROBERT GILMAN

Introduction

We apply a combinatorial identity (Proposition 1) to obtain two results. First we characterize the class of finite groups such that similar permutation representations contain the regular representation the same number of times (Proposition 2), thus answering a question of S. Golomb [9]. Secondly we obtain a relatively short and direct proof of the Brauer-Tate and Witt-Berman theorems (Proposition 3).

The proof of these results uses the Möbius function of the lattice of subgroups of a group. P. Hall [4] and L. Weisner [8] have extended the Möbius inversion formula from functions of integers to functions defined on locally finite partially ordered sets, and their work has been generalized by G.-C. Rota [7]. (A partially ordered set is locally finite if each interval $[a, b] = \{c \mid a \leq c \leq b\}$ is finite.) The original Möbius function is multiplicative on relatively prime numbers, and Proposition 1 is an extension of multiplicativity to a relation for the Möbius function of locally finite lattices.

Proposition 1 has also been obtained by Curtis Greene [10].

A combinatorial identity

The Möbius function μ of a locally finite partially ordered set is the unique solution of

$$\begin{aligned} \sum_{c \in [a,b]} \mu(c, b) &= 1 \quad \text{if } a = b \\ &= 0 \quad \text{if } a \neq b. \end{aligned} \tag{1}$$

See [7] for a complete exposition. By [7, §3 Proposition 3], μ also satisfies

$$\begin{aligned} \sum_{c \in [a,b]} \mu(a, c) &= 1 \quad \text{if } a = b \\ &= 0 \quad \text{if } a \neq b. \end{aligned} \tag{1}'$$

PROPOSITION 1. *Let L be a locally finite lattice with Möbius function μ. Suppose $c \in [a, b]$. Then*

$$\mu(a, b) = \sum_{d \vee c = b, d \wedge c = a} \tilde{\mu}(a, d)\mu(d, b) \tag{2}$$

where $\tilde{\mu}$ is the Möbius function of

$$[a, d]^* = \{e \mid e \in [a, d], (e \vee c) \wedge d = e\}.$$

An empty sum is zero.

Received February 1, 1971.

Proof. If $c = a$, the sum in (2) equals $\tilde{\mu}(a, b)\mu(b, b) = \mu(a, b)$, and similarly if $c = b$. We may thus assume that $a < c < b$ and that (2) holds with a replaced by e for $a < e \leq b$. By a result of L. Weisner [8, Theorem 10] [7, page 351],

$$\sum_{e \wedge c = a,\, e \in [a,b]} \mu(e, b) = 0. \tag{3}$$

We complete the proof by solving (3) for $\mu(a, b)$, substituting the right hand side of (2) with e in place of a and $e \vee c$ in place of c for $\mu(e, b)$ if $e \neq a$, reversing summation, and applying (3) for $\tilde{\mu}$ to show that the inner sum is $-\tilde{\mu}(a, d)$.

Now if L' is L with the order inverted, L' has the Möbius function $\mu'(a, b) = \mu(b, a)$ [7, §3 Prop. 3]. Thus applying (2) to L' gives a dual formula. Also for $d \vee c = b$, $d \wedge c = a$ we may define

$$p : [c, b] \to [a, d], \qquad q : [a, d] \to [c, b]$$

by $p(f) = f \wedge d$ and $q(e) = e \vee c$. Then p and q induce isomorphisms between $q(p([c, b]))$ and $p(q([a, d])) = [a, d]^*$. Thus (2) may be rewritten with the Möbius function of $q(p([c, b]))$ in place of $\tilde{\mu}$.

COROLLARY 1. *Let L be as in Proposition* 1. *If $\mu(a, b) \neq 0$, then for any $c \in [a, b]$ there exists d such that $c \vee d = b$, $c \wedge d = a$, and $\mu(d, b) \neq 0$, and (by duality) there exists e such that $c \vee e = b$, $c \wedge e = a$ and $\mu(a, e) \neq 0$.*

COROLLARY 2. *Let L be the lattice of subgroups of finite index in a group G. Let $N(H)$ be the normalizer of a subgroup H and define $(N(H):H)_p$ to be the highest power of a prime p dividing the index $(N(H):H)$. Either $(N(H):H)_p$ divides $\mu(H, G)$ for all $H \in L$ or G has a factor group of order p.*

Proof. Choose H of minimal index so that $(N(H):H)_p$ does not divide $\mu(H, G)$ and pick K satisfying $H \leq K \leq N(H)$, $(K:H) = (N(H):H)_p$. Clearly $H \neq G$. By (2), $\mu(H, G)$ equals the sum of $\tilde{\mu}(H, R)\mu(R, G)$ over all R such that $R \vee K = G$, $R \wedge K = H$. If $R = H$ occurs, then $K = G$ and G has a factor group of order p. If not, K acts on $\{R\}$ by conjugation. Conjugation induces isomorphisms of intervals, and so by the uniqueness of the Möbius function

$$\tilde{\mu}(H, R^x)\mu(R^x, G) = \tilde{\mu}(H, R)\mu(R, G) \quad \text{for } x \in K.$$

Suppose T is the stabilizer of R;

$$(T:H) = (TR:R) \mid (N(R):R)_p \mid \mu(R, G)$$

because R has smaller index than H. Summing over K orbits we obtain $(K:H) \mid \mu(H, G)$.

DEFINITION. Let n be a positive integer, p a prime and G a group of order g. G is n elementary with respect to p if G has a cyclic normal subgroup M of order prime to p such that G/M is a p group and all n^{th} roots of

unity in M are in $Z(G)$, the center of G. G is n elementary if it is n elementary w.r.t. p for some prime p. A 1 elementary group is called hyperelementary.

Remark. If F is a subfield of the complex numbers and n is the largest divisor of g such that F contains all n^{th} roots of unity, then n elementary is the same as F elementary [1, page 71].

COROLLARY 3. *Let L be the partially ordered set consisting of a finite group G and all subgroups hyperelementary with respect to a prime p. If G is not hyperelementary w.r.t. p, then*

$$(N(H):H)_p \mid \mu(H, G) \quad \text{for all } H \in L.$$

Proof. L is a lattice with the usual definition of $\wedge$ and $\vee$ except that $H \vee K = G$ if the subgroup generated by H and K is not in L. The preceding proof works; one need only notice that K and TR are in L, and that the case $R = H$ cannot occur.

A question of S. Golomb

The question is which finite groups satisfy Proposition 2(a). Let $(\ ,\ )_H$ be the usual inner product of complex-valued class functions of a group H, and recall that a generalized character is an integral linear combination of characters of complex representations of a group.

LEMMA 1. *Let L be a set of subgroups of a noncyclic finite group G, and suppose L contains G and all cyclic subgroups of G. We have*

$$\sum_{R \in L} \mu(R, G) r 1_R^G = 0 \tag{4}$$

where r is the order of R, 1_R^G is the principal character of R induced to G, and μ is the Möbius function of L (partially ordered by inclusion).

Proof. Let θ be the sum in (4). $\theta(x)$ is the sum over all y in G of $\sum' \mu(R, G)$; $\sum'$ means that the sum is over all R in L which contain x^y. By (1), $\theta(x) = 0$.

PROPOSITION 2. *G is a group of order g; μ is the Möbius function of the lattice of subgroups of G. The following are equivalent:*

(a) *The character of each permutation representation of G determines the number of orbits of length g.*

(b) *$\mu(1, H) = 0$ for all noncyclic subgroups H.*

(c) *G has a complex-valued class function θ such that $(\theta, 1_H)_H = 0$ if and only if $H \neq 1$.*

(d) *Every subgroup of order the product of two primes is cyclic.*

Proof. Suppose (a) is valid. By Lemma 1, $\sum \mu(R, H) r 1_R^H = 0$ with R running over all subgroups of a noncyclic $H \leq G$. Thus $\sum \mu(R, H) r 1_R^G = 0$, and putting all negative terms on the right gives two permutation repre-

sentations with equal characters. Since only one of the representations can have orbits of length g, (corresponding to the term $\mu(1, H)1_1^G$), we must have $\mu(1, H) = 0$, and (a) implies (b).

Assume (b). $\mu(1, H^y) = \mu(1, H)$ for $y \in G$ because conjugation by y includes an isomorphism between $[1, H^y]$ and $[1, H]$, and μ is uniquely determined by (1). Thus setting $\theta(x)$ equal to $\mu(1, \langle x \rangle)$ divided by the number of generators of the cyclic group $\langle x \rangle$ defines a rational-valued class function on G. By (1)′ and (b), θ satisfies (c). Further, if θ is any choice for (c), then the number of orbits of length g in a permutation with character $\chi = \sum a_H 1_H^G$ is a_1, which equals $(\chi, \theta)_G$ divided by $\theta(1)$. Now we have that (a), (b), (c), are equivalent.

(b) implies (d) because it is easy to show by computing μ using (1) that a group H of order pq, p and q two primes, is cyclic if $\mu(1, H) = 0$.

Finally suppose G satisfies (d). It suffices to show that G satisfies (b). Because (d) is inherited by subgroups, we may assume (b) holds for all proper subgroups of G. Suppose G is solvable and let M be a normal subgroup of prime order. By Corollary 1, $\mu(1, G) = 0$ and (b) holds unless M has a complement H with $\mu(1, H) \neq 0$. By assumption H must be cyclic, and by a result of P. Hall [4] [7, page 349] H is generated by its subgroups of prime order. Now (d) implies G is cyclic and (b) is valid. If G is not solvable, then since all Sylow subgroups of G are cyclic or quaternion, G must have a quaternion Sylow 2 subgroup Q. Any two distinct involutions generate a dihedral group, which has a noncyclic subgroup of order pq. Hence G has a normal subgroup N of order 2. N cannot have a complement in G because it does not have one in Q. Thus $\mu(1, G) = 0$ and we are done.

For solvable groups (d) is equivalent to saying that G is a Frobenius complement [6, page 228]. The only nonsolvable Frobenius complement is essentially $SL(2, 5)$ [6, Theorem 18.6], and it can be shown that the nonsolvable groups satisfying (a) are essentially $\{SL(2, q) \mid q \text{ is a Fermat prime}\}$. By [3], G is essentially $SL(2, q)$, and by [5, II, §8], (d) forces q to be a Fermat prime.

The Witt-Berman induction theorem

We give a short proof of the main step in the proof of the above theorem, (see [1, 15.5]).

PROPOSITION 3. *Let $Q(n)$ be the rationals with an n^{th} root of unity adjoined. The principal character, 1_G, of a group G of order g is an integral linear combination of characters induced by characters of degree one which are defined on n elementary subgroups and afforded by $Q(n)$.*

Proof. It suffices to show that for each prime p dividing g the conclusion holds for $m1_G$ where $g = p^a m$, $p \nmid m$. The proposition follows because 1_G is a linear combination of $\{m1_G\}$. We may assume G is not n elementary with respect to p. If $n = 1$, pick L as in Corollary 3. Combining terms for

conjugate subgroups in (4) and applying Corollary 3 yield $\sum a_H 1_H^G = 0$ with $H \in L$, $p^a \mid a_H$, and $a_G = g$. Thus we can solve for $m1_G$ with integer coefficients. Now we may assume $n > 1$ and G hyperelementary w.r.t. p. We argue by induction on g; $g = 1$ is trivial. If G is n elementary w.r.t. p, there is nothing to prove. If not, there is an n^{th} root of unity $x \in M$, $x \notin Z(G)$ (see the definition). Because p is prime to the order of M, we can find a factor group $\bar{G} = P.N$ a semidirect product with P a p group, N of prime order $q \mid n$, and P acting faithfully on N [2, page 174]. Let χ_N be a sum of P orbit representatives of the nonprincipal one dimensional characters of N. We have $1_{\bar{G}} = 1_P^{\bar{G}} - \chi_N^{\bar{G}}$. Thus $1_G = 1_R^G - \chi_S^G$ for some proper subgroups R, S of G. We complete the proof by applying the proposition to 1_R and 1_S and multiplying the equation for 1_S by χ_S.

References

1. W. Feit, *Characters of finite groups*, W. A. Benjamin, New York, 1967.
2. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
3. M. Suzuki, *On finite groups with cyclic Sylow subgroups for all odd primes*, Amer. J. Math., vol. 77 (1955), pp. 657–691.
4. P. Hall, *The Eulerian functions of a group*, Quart. J. Math., vol. 7 (1936), pp. 134–151.
5. B. Huppert, *Endliche Gruppen I*, Springer-Verlag, New York, 1967.
6. D. Passman, *Permutation groups*, W. A. Benjamin, New York, 1968.
7. G.-C. Rota, *On the foundations of combinatorial theory*, Z. Wahrscheinlichkeitsth., vol. 2 (1964), pp. 340–368.
8. L. Weisner, *Abstract theory of inversion of finite series*, Trans. Amer. Math. Soc., vol. 38 (1935), pp. 474–484.
9. S. Golomb, *A mathematical theory of discrete classification*, Proc. Fourth London Symposium on Information Theory, Butterworth, London, 1961.
10. C. Greene, *On the Möbius algebra of a partially ordered set*, to appear.

Stevens Institute of Technology
Hoboken, New Jersey