PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 103, Number 2, June 1988

POLYNOMIALS ASSOCIATED TO CHARACTERS

ALEXANDRE TURULL

(Communicated by Bhama Srinivasan)

ABSTRACT. The present paper concerns certain divisibility properties of the (integer) values of some polynomials naturally defined from characters and modules of finite groups. A generalization of a theorem of K. Brown is obtained in this context.

Introduction. Let G be a finite group, let $\mathscr{S}$ be the poset of subgroups of G ordered by inclusion and let $\mu : \mathscr{S} \to \mathbf{Z}$ be the Möbius function, defined by, $\mu(1) = 1$ and, if $a \in \mathscr{S}$ and $a \neq 1$, then $\sum_{1 \leq b \leq a} \mu(b) = 0$. If $\mathscr{P}$ is a set of subgroups of G and χ is a character of G, we define the polynomial

$$P(\mathscr{P}, \chi, x) = \sum_{a \in \mathscr{P}} \mu(a) x^{(\chi|_a, 1_a)_a}.$$

In this introduction we state only some consequences for our results.

COROLLARY A. *Let p be a prime and χ a p-rational character of G. Let $\mathscr{P}$ be the set of p-subgroups of G, and let $\mathscr{E}$ be the set of elementary Abelian p-subgroups of G. Let n be any integer not divisible by p.*

Then $P(\mathscr{P}, \chi, x) = P(\mathscr{E}, \chi, x)$ and $|G|_p$ divides $P(\mathscr{P}, \chi, n)$. In particular, if $p \,|\, |G|$, $x^{p-1} - 1$ divides $P(\mathscr{P}, \chi, x)$ in $\mathbf{F}_p[x]$.

For any rational character χ, by setting in Corollary A $n = 1$, we obtain $\sum_{a \in \mathscr{P}} \mu(a) \equiv 0 \bmod |G|_p$, a statement which is equivalent to a theorem of K. Brown [1] for finite groups. Corollary A is in fact a special case of Corollary B.

COROLLARY B. *Let m be a positive integer divisor of $|G|$ and let n be an integer with $(m, n) = 1$. Let χ be a character of G and assume that χ is p-rational for all primes $p|m$. Let $\mathscr{M}$ be the set of subgroups of G of order dividing m, and let $\mathscr{M}^*$ be the set of solvable elements in $\mathscr{M}$.*

Then m divides both $P(\mathscr{M}, \chi, n)$ and $P(\mathscr{M}^*, \chi, n)$. In particular $x^{p-1} - 1$ divides $P(\mathscr{M}, \chi, x)$ and $P(\mathscr{M}^*, \chi, x)$ in $\mathbf{F}_p[x]$ for every prime divisor p of m.

Denote by $m(G)$ the Artin exponent of G, i.e., the smallest positive integer m such that $m1_G$ is an integral linear combination of characters induced from the trivial character of cyclic subgroups of G. $m(G)$ always divides $|G|$. We note that Lam [5] describes a method to calculate $m(G)$.

COROLLARY C. *Let χ be a character of G. Let $\mathscr{C}$ be the collection of the cyclic subgroups of G and n be an integer with $(n, |G|/m(G)) = 1$. Assume that χ is p-rational for every prime divisor p of $|G|/m(G)$.*

Received by the editors December 30, 1986 and, in revised form, May 6, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20C15.
Partially supported by NSF Grant DMS-8601744.

Then $|G|/m(G)$ *divides* $P(\mathscr{C}, \chi, n)$. *In particular if* p *is a prime divisor of* $|G|/m(G)$ *then* $x^{p-1} - 1$ *divides* $P(\mathscr{C}, \chi, x)$ *in* $\mathbf{F}_p[x]$.

Similar results are established for every family of subgroups closed under conjugation, see Theorem 5. We turn now to the modular case. Let $\mathbf{F}_q$ be a finite field and let M be an $\mathbf{F}_q G$-module. If $a \in \mathscr{S}$ we define $d(a) = \dim(C_M(a))$. Then, if $\mathscr{P}$ is a set of subgroups of G, we define

$$P(\mathscr{P}, M, x) = \sum_{a \in \mathscr{P}} \mu(a) x^{d(a)}.$$

COROLLARY D. *Let* m *be a positive integer divisor of* $|G|$ *and let* n *be any nonnegative integer. Let* $\mathscr{M}$ *be the set of subgroup of* G *of order dividing* m *and let* $\mathscr{M}^*$ *be the set of solvable elements of* $\mathscr{M}$. *Let* $\mathscr{C}$ *be the set of all cyclic subgroups of* G.

Then m *divides both* $P(\mathscr{M}, M, q^n)$ *and* $P(\mathscr{M}^*, M, q^n)$, *and* $|G|/m(G)$ *divides* $P(\mathscr{C}, M, q^n)$.

If $G \neq 1$, $P(\mathscr{S}, M, 1) = 0$ by the definition of μ. Furthermore if $n > 0$, $P(\mathscr{S}, M, q^n)$ is exactly the number of elements in $M \otimes \mathbf{F}_{q^n}$ which belong to some regular G-orbit, see Lemma 2 below. These facts allow one to calculate easily $P(\mathscr{S}, M, x)$ in certain cases. For example, if $G = GL(n, q)$ and M is its natural module, then

$$P(\mathscr{S}, M, x) = \prod_{\alpha=0}^{n-1} (x - q^\alpha),$$

as $P(\mathscr{S}, M, x)$ is a monic polynomial of degree n with roots $1, q, \ldots, q^{n-1}$. Similarly if G is any finite group, M is any $\mathbf{F}_q G$-module and $P(\mathscr{S}, M, x) = f(x)$, then the corresponding polynomial for the wreath product $S_n \sim G$, of order $n!|G|^n$, acting on $M^{(n)}$ is

$$f(x)(f(x) - |G|)(f(x) - 2|G|) \cdots (f(x) - (n-1)|G|),$$

and for the wreath product $\mathbf{Z}_p \sim G$, of order $p|G|^p$, where p is a prime, acting on $M^{(p)}$ is $f(x)^p(|G|^{p-1})f(x)$, facts which follow from counting the number of elements in regular orbits in $[M \otimes \mathbf{F}_q m]^{(n)}$ for all $m > 0$.

The above property shows that, when G is a finite group, M is an $\mathbf{F}_q G$-module with Brauer character χ and $(q, |G|) = 1$, then $P(\mathscr{S}, \chi, x) = P(\mathscr{S}, M, x)$ is in fact the polynomial defined in [**8** and **9**]. The research in this paper was stimulated by some conversations with T. Hawkes in which I learned that T. Hawkes and M. Isaacs had independently considered the polynomials $P(\mathscr{S}, \chi, x)$ for different reasons.

Proofs. Denote by Ω the Burnside ring of G, that is the Grothendieck ring of finite G-sets. If H is a subgroup of G, denote by (H) the conjugacy class of H in G and denote by $C(G)$ the set of conjugacy classes of subgroups of G. The set $\{G/H : (H) \in C(G)\}$ of transitive G-sets is a $\mathbf{Z}$-basis for Ω. If H is a subgroup, we define the map ϕ_H from G-sets to natural numbers by, if X is a G-set,

$$\phi_H(X) = |C_X(H)|.$$

This can be extended in a natural way to a ring homomorphism $\phi_H : \Omega \to \mathbf{Z}$. We denote by $\mathbf{Z}^{C(G)}$ the ring of integer valued functions on $C(G)$ and we define

$\phi : \Omega \to \mathbf{Z}^{C(G)}$ by $[\phi(X)]((H)) = \phi_H(X)$ for $X \in \Omega$ and $(H) \in C(G)$. ϕ is an injective ring homomorphism. $\phi(\Omega)$ is an additive subgroup of $\mathbf{Z}^{C(G)}$ of finite index and $|G|\mathbf{Z}^{C(G)} \subseteq \phi(\Omega)$. Proofs of these elementary properties of Burnside rings may be found, for example, in [**2**]. The following lemma is well known.

LEMMA 1. *If X is a G-set then*

$$|\{x \in X : C_G(x) = 1\}| = \sum_{H \in \mathcal{S}} \mu(H)\phi_H(X).$$

Furthermore, if $Y \in \Omega$, then $|G|$ divides $\sum_{H \in \mathcal{S}} \mu(H)\phi_H(Y)$.

PROOF. The number of elements in X which belong to some regular orbit is a multiple of $|G|$, so the second part follows from the first by linearity. The first part is an easy computation:

$$|\{x \in X : C_G(x) = 1\}| = \sum_{x \in X} \sum_{1 \leq H \leq C_G(x)} \mu(H) = \sum_{H \in \mathcal{S}} \mu(H)\phi_H(X).$$

LEMMA 2. *Let M be an $\mathbf{F}_qG$-module. Consider $M \otimes \mathbf{F}_{q^n}$ as a G-set. Then, for every subgroup H of G,*

$$\phi_H(M \otimes \mathbf{F}_{q^n}) = q^{nd(H)}.$$

The number of elements in $M \otimes \mathbf{F}_{q^n}$ which belong to some regular G-orbit is exactly $P(\mathcal{S}, M, q^n)$.

PROOF. If H is any subgroup of G then

$$C_{M \otimes \mathbf{F}_{q^n}}(H) = C_M(H) \otimes \mathbf{F}_{q^n}.$$

Since $d(H) = \dim(C_M(H))$,

$$\phi_H(M \otimes \mathbf{F}_{q^n}) = q^{nd(H)}$$

follows. The second part follows from this and Lemma 1.

Let $\mathcal{X}$ be a set of subgroups of G closed under conjugation. We denote by $e_{\mathcal{X}}$ the element of $\mathbf{Z}^{C(G)}$ defined by

$$e_{\mathcal{X}}((H)) = \begin{cases} 0 & \text{if } H \notin \mathcal{X}, \\ 1 & \text{if } H \in \mathcal{X}. \end{cases}$$

Then, from an earlier remark, $|G|e_{\mathcal{X}} \in \phi(\Omega)$. We define $m(\mathcal{X})$ to be the smallest positive integer such that $m(\mathcal{X})e_{\mathcal{X}} \in \phi(\Omega)$. If m is any integer such that $me_{\mathcal{X}} \in \phi(\Omega)$, then $m(\mathcal{X})$ divides m. In particular, $m(\mathcal{X})$ divides $|G|$.

LEMMA 3. *Let m be a positive integer divisor of $|G|$ and let $\mathcal{M}$ be the set of subgroups of G of order dividing m, let $\mathcal{M}^*$ be the set of solvable groups in $\mathcal{M}$ and let $\mathcal{C}$ be the set of cyclic subgroups of G.*

Then $m(\mathcal{M}) = |G|/m = m(\mathcal{M}^*)$ and $m(\mathcal{C}) = m(G)$.

PROOF. $m(\mathcal{M}) = |G|/m$ is Theorem 3.1 in [**7**]. $m(\mathcal{C}) = m(G)$ is Proposition 2.5 in [**7**]. Let $\mathcal{A}$ be the collection of solvable subgroups of G. Then, it follows from Proposition 2.1 in [**7**] that $m(\mathcal{A}) = 1$. Hence $e_{\mathcal{A}} \in \phi(\Omega)$. From $e_{\mathcal{M}^*} = e_{\mathcal{A}}e_{\mathcal{M}}$ and ϕ a ring homomorphism follows that $m(\mathcal{M})e_{\mathcal{M}^*} \in \phi(\Omega)$, i.e., that $m(\mathcal{M}^*)$ divides $m(\mathcal{M})$. Since $\gcd\{|G : S| : S \in \mathcal{M}^*\} = |G|/m$, Proposition 2.7 in [**7**] implies that $|G|/m$ divides $m(\mathcal{M}^*)$. Hence $m(\mathcal{M}^*) = |G|/m$. This concludes the proof of the lemma.

THEOREM 4. *Let M be an $\mathbf{F}_q$ G-module, $\mathscr{X}$ any subset of $\mathscr{S}$ closed under conjugation and $n \geq 0$.*

Then $|G|/m(\mathscr{X})$ divides $P(\mathscr{X}, M, q^n)$.

PROOF. Consider $M \otimes \mathbf{F}_{q^n}$ as a G-set (as the G-set with one element if $n = 0$). Then $m(\mathscr{X})e_{\mathscr{X}}\phi(M \otimes \mathbf{F}_{q^n}) \in \phi(\Omega)$ and

$$[m(\mathscr{X})e_{\mathscr{X}}\phi(M \otimes \mathbf{F}_{q^n})]\,((H)) = \begin{cases} 0 & \text{if } H \notin \mathscr{X}, \\ m(\mathscr{X})q^{nd(H)} & \text{if } H \in \mathscr{X}, \end{cases}$$

by Lemma 2. Now Lemma 1 implies that $|G|$ divides $\sum_{H \in \mathscr{X}} m(\mathscr{X})\mu(H)q^{nd(H)}$. It follows, since $m(\mathscr{X})$ divides $|G|$, that $|G|/m(\mathscr{X})$ divides $P(\mathscr{X}, M, q^n)$. The theorem follows.

THEOREM 5. *Let χ be a character of G and assume that χ is p-rational for every prime divisor p of $|G|/m(\mathscr{X})$. Let n be an integer with $(n, |G|/m(\mathscr{X})) = 1$. Then $|G|/m(\mathscr{X})$ divides $P(\mathscr{X}, \chi, n)$.*

In particular $x^{p-1} - 1$ divides $P(\mathscr{X}, \chi, x)$ in $\mathbf{F}_p[x]$ for every prime divisor p of $|G|/m(\mathscr{X})$.

PROOF. If the first part of Theorem 5 holds, then $P(\mathscr{X}, \chi, x) \pmod p$ has every nonzero value in $\mathbf{F}_p$ as a root, by the Chinese Remainder Theorem, and it follows that $x^{p-1} - 1$ divides $P(\mathscr{X}, \chi, x) \pmod p$. Hence we only need to show the first part. Let $m = |G|/m(\mathscr{X})$, let π be the set of prime divisors of m, and let $|G|_{\pi'}$ be the π'-part of $|G|$. Since $(|G|_{\pi'}, m) = 1$ and $(n, m) = 1$, there exists, by Dirichlet's Theorem, a prime p such that $p \equiv n \pmod m$ and $p \equiv 1 \pmod{|G|_{\pi'}}$.

Let $F = \mathbf{Q}(\varepsilon)$ where ε is a primitive $|G|_{\pi'}$th root of 1. Then $\chi(g) \in F$ for all $g \in G$, since χ is r-rational for every prime $r \in \pi$. Pick ψ any irreducible character contained in χ. Let α be the number of characters in χ which are Galois conjugate over F to ψ counting multiplicities. Then $[F(\psi) : F]$ is a divisor of α. If we identify the values of ψ with elements in some algebraic closure of $\mathbf{F}_p$, it follows from $p \nmid |G|$ and (9.14) Theorem in [**3**] that there exists an $\mathbf{F}_p(\psi)G$-module N with Brauer character ψ. Viewed as an $\mathbf{F}_pG$-module, N has as Brauer character the sum of $[\mathbf{F}_p(\psi) : \mathbf{F}_p]$ Galois conjugates of ψ. By, for example, Proposition 19 in [**6**], $[\mathbf{F}_p(\psi) : \mathbf{F}_p]$ divides $[F(\psi) : F]$, whence $[\mathbf{F}_p(\psi) : \mathbf{F}_p]$ also divides α. We take the direct sum of $\alpha/[\mathbf{F}_p(\psi) : \mathbf{F}_p]$ copies of N. We repeat this process for every Galois conjugacy class over F of characters in χ and we denote by M the $\mathbf{F}_pG$-module obtained by taking the direct sum of the modules thus obtained.

Let χ_0 be the Brauer character of M. We can establish a one-to-one correspondence between the irreducible characters of χ_0 (counting multiplicities) and the irreducible characters of χ (counting multiplicities) in such a way that corresponding characters are Galois conjugate over F. It then follows from the definition that $P(\mathscr{X}, \chi, x) = P(\mathscr{X}, \chi_0, x)$. Furthermore $P(\mathscr{X}, \chi_0, x) = P(\mathscr{X}, M, x)$. From Theorem 4 we obtain that m divides $P(\mathscr{X}, M, p)$, i.e., that $P(\mathscr{X}, \chi, p) \equiv 0 \pmod m$. Since $p \equiv n \pmod m$ and $P(\mathscr{X}, \chi, x)$ is a polynomial with integer coefficients, it follows that $P(\mathscr{X}, \chi, n) \equiv 0 \pmod m$. This concludes the proof of Theorem 5.

PROOF OF COROLLARY A. If P is a p-group and $\mu(P) \neq 0$, then P is elementary Abelian. This well-known fact appears, for example, as Proposition 2.4 in [**4**]. Hence $P(\mathscr{P}, \chi, x) = P(\mathscr{E}, \chi, x)$. The rest of the theorem follows from Theorem 5 and Lemma 3 by setting $m = |G|_p$, whence $\mathscr{M} = \mathscr{M}^* = \mathscr{P}$.

Corollaries B and C follow immediately from Theorem 5 and Lemma 3. Corollary D follows likewise from Theorem 4 and Lemma 3.

REFERENCES

1. K. Brown, *Euler characteristics of groups: the p-fractional part*, Invent. Math. **29** (1975), 1–5.
2. T. tom Dieck, *Transformation groups and representation theory*, Lecture Notes in Math., vol. 766, Springer-Verlag, Berlin and New York, 1979.
3. I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976.
4. C. Kratzer and J. Thévenaz, *Fonction de Möbius d'un groupe fini et anneau de Burnside*, Comment. Math. Helv. **59** (1984), 425–438.
5. T. Y. Lam, *Artin exponent of finite groups*, J. Algebra **9** (1968), 94–119.
6. J. P. Serre, *Corps locaux*, Hermann, Paris, 1962.
7. J. Thévenaz, *Idempotents de l'anneau de Burnside et caractéristqiue d'Euler*, Séminaire groupes finis III, Publ. Math. Univ. Paris VII, 1987.
8. A. Turull, *Hall-Higman type theorems for arbitrary groups, why and how*, Proc. 4th Int. Conf. on Representations of Algebras (Ottawa, August 1984), Carleton Lecture Notes.
9. ——, *Fixed point free action with regular orbits*, J. Reine Angew. Math. **371** (1986), 67–91.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF MIAMI, CORAL GABLES, FLORIDA 33124