PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 6, June 2008, Pages 1961–1966
S 0002-9939(08)09380-5
Article electronically published on February 14, 2008

ON A CONGRUENCE OF BLICHFELDT CONCERNING THE ORDER OF FINITE GROUPS

DAVID CHILLAG

(Communicated by Jonathan I. Hall)

ABSTRACT. We show that if G is a finite group, C a conjugacy class of G and $d = |C|$, $d_2, d_3, \ldots, d_m$ are the distinct elements in the multiset $\left\{ \frac{|C|\chi(C)}{\chi(1)} \mid \chi \in \mathrm{Irr}(G) \right\}$ (here $\chi(C)$ is the value of χ on any element of C), then

$$|G/\langle C \rangle| \cdot (d - d_2)(d - d_3) \cdots (d - d_m) \equiv 0 \mod |G|.$$

This is a dual to a generalization of a theorem of Blichfeldt stating that if G is a finite group, θ a generalized character and $d = \theta(1), d_2, d_3, \ldots, d_m$ are the distinct values of θ, then

$$|\ker(\theta)|(d - d_2)(d - d_3) \cdots (d - d_m) \equiv 0 \mod |G|.$$

We also observe that $d = \theta(1)$ in Blichfeldt's congruence can be replaced, with a minor adjustment, by any rational value of θ. A similar change can be done to the first congruence above.

1. Introduction

The following result was proved for a permutation character θ by Blichfeldt ([2]), rediscovered by Kiyota ([7]) and proved for characters and generalized characters by the author ([4]) and independently by Cameron and Kiyota ([3]):

Theorem 1. *Let G be a finite group, θ a generalized character of G, and $d = \theta(1), d_2, d_3, \ldots, d_m$ the distinct values of θ. Then*

$$|\ker(\theta)|(d - d_2)(d - d_3) \cdots (d - d_m) \equiv 0 \mod |G|.$$

First we show that a dual congruence is true as well, namely:

Theorem 2. *Let G be a finite group, C a conjugacy class of G, and $d = |C|, d_2, d_3, \ldots, d_m$ the distinct elements in the multiset $\left\{ \frac{|C|\chi(C)}{\chi(1)} \mid \chi \in \mathrm{Irr}(G) \right\}$ (here $\chi(C)$ is the value of χ on any element of C). Then*

$$|G/\langle C \rangle| \cdot (d - d_2)(d - d_3) \cdots (d - d_m) \equiv 0 \mod |G|.$$

Next, we observe that $d = \theta(1)$ in Theorem 1 can be replaced by any rational value of θ, namely:

Received by the editors April 17, 2007.
2000 *Mathematics Subject Classification.* Primary 20G15.

Theorem 3. *Let G be a finite group, θ a generalized character of G, and $d, d_2, d_3, \ldots, d_m$ the distinct values of θ, where d is rational. Set $V_d(\theta) = \{x \in G \mid \theta(x) = d\}$. Then*

$$|V_d(\theta)|\,(d-d_2)\,(d-d_3)\cdots(d-d_m) \equiv 0 \mod |G|\,.$$

Since $V_{\theta(1)}(\theta) = \ker(\theta)$, Theorem 1 follows from Theorem 3. For a permutation character θ, this was already proved in [2].

A similar adjustment can be done in Theorem 2; the exact statement is Corollary 6(2) in the next section.

The proofs are very similar to the proof of Theorem 1 in [4]. In fact all the above theorems can be deduced as special cases of a congruence in a general setup (see Section 2).

Equality in Theorem 2, which is $(d-d_2)\,(d-d_3)\cdots(d-d_m) = |\langle C\rangle|$, can occur.

For example, let G be a group containing a central cyclic subgroup $A = \langle a\rangle$ of order m. Let C be the conjugacy class of a. Then $|C| = 1$ and $|\langle C\rangle| = m$. Let $\epsilon = e^{\frac{2\pi i}{m}}$. Then for every $j = 0, 1, \ldots, m-1$ there exists a linear character λ_j of A such that $\lambda_j(a) = \epsilon^j$. For every such j let $\chi_j \in \mathrm{Irr}(G)$ be such that $\left((\chi_j)_A, \lambda_j\right) \neq 0$. Then $(\chi_j)_A = \chi_j(1)\lambda_j$ so that $\chi_j(a) = \chi_j(1)\epsilon^j$. Since $\mathrm{Irr}(A) = \{\lambda_j \mid 0 \leq j \leq m-1\}$, every $\chi \in \mathrm{Irr}(G)$ satisfies $\chi_A = \chi(1)\lambda_j$ and $\chi(a) = \chi(1)\epsilon^j$ for some $j = 0, 1, \ldots, m-1$. It follows that $d = 1$ and the other distinct elements in the multiset $\left\{\frac{|C|\chi(C)}{\chi(1)} | \chi \in \mathrm{Irr}(G)\right\}$ are the ϵ^j, $j = 0, 1, \ldots, m-1$. Consequently

$$(d-d_2)\,(d-d_3)\cdots(d-d_m) = (1-\epsilon)\left(1-\epsilon^2\right)\cdots\left(1-\epsilon^{m-1}\right).$$

It is easy to see that this product is equal to $m = |\langle C\rangle|$.

Another example is a Frobenius group G of order $p^n(p^n-1)$ with an abelian Frobenius kernel G' of order p^n. Let $g \in G' - \{1\}$ and let C be its conjugacy class. Then $|C| = p^n - 1$ and $|\langle C\rangle| = p^n$. It is known that $\mathrm{Irr}(G)$ contains exactly one nonlinear character χ, $\chi(1) = p^n - 1$ and $\chi(g) = -1$. Thus $m = 2$, $d = p^n - 1$ and $d_2 = \frac{|C|\chi(C)}{\chi(1)} = \frac{(p^n-1)(-1)}{p^n-1} = -1$. It follows that $p^n = |\langle C\rangle| = (d-d_2)$.

It may be of interest to study when equality occurs as a "dual" study to sharp groups (these are groups in which equality occurs in the Blichfeldt's congruence (Theorem 1)). Many cases of sharp groups were studied, by Kiyota, Cameron and others. The last example is such a dual "sharp" example for the case $|\langle C\rangle| = (d-d_2)$. It is not hard to see (Proposition 7) that this equality holds if and only if $\langle C\rangle = C \cup \{1\}$ is a minimal normal elementary abelian p-subgroup for some prime p.

Equality can occur in Theorem 3 for $d \neq \theta(1)$ as well.

Proofs can be found in the next section. Our notation is standard and taken mainly from [6].

2. Proofs

Let $\mathbb{F}$ be any subfield of the real number field $\mathbb{R}$ and let A be a semi-simple, finite-dimensional commutative $\mathbb{F}$-algebra. The identity element of A (which is known to exist) will be denoted by 1_A.

Let $\mathfrak{B} = \{b_1 = 1_{\mathbf{A}}, b_2, \ldots, b_n\}$ be a basis of A. For every $a \in A$, define a matrix $M(a, \mathfrak{B}) = (m_{ij}(a, \mathfrak{B}))$ by $ab_i = \sum_{j=1}^{n} m_{ij}(a, \mathfrak{B})b_j$. It is known that each $M(a, \mathfrak{B})$ is diagonalizable over the field of complex numbers (see [5], Lemma 2.1).

Definition 4. Let $\mathbb{F}$ be any subfield of the real number field $\mathbb{R}$ and let A be a semi-simple, n-dimensional commutative $\mathbb{F}$-algebra. Let $\mathfrak{B}$ be a basis of A with $1_A \in \mathfrak{B}$. Let $a \in A$ and $a(1), a(2), \ldots, a(n)$ be the eigenvalues of $M(a, \mathfrak{B})$. Define $K_d(a) = \{i \mid a(i) = d\}$.

Theorem 5. *Let $\mathbb{F}$ be any subfield of the real number field and let A be a semi-simple, n-dimensional commutative $\mathbb{F}$-algebra. Let $\mathfrak{B}$ be a basis of A with $1_A \in \mathfrak{B}$. Let $a \in A$. Let $d = a(1), a(2), \ldots, a(k), a(k+1), \ldots, a(n)$ be the eigenvalues of $M(a, \mathfrak{B})$, where $a(1), a(2), \ldots, a(k)$ are all the distinct eigenvalues. Let $(\alpha_1, \alpha_2, \ldots \alpha_n)$ be an n-tuple of positive integers and let $a = \sum_{i=1}^{n} \alpha_i$. Assume that*

(1) *The matrix $M(a, \mathfrak{B})$ has integral entries.*
(2) *d is an integer.*
(3) *$\sum_{j=1}^{n} \alpha_j \left(a(j)\right)^i$ is a positive integral multiple of α for all $i = 1, 2, \ldots, k$.*

Then

$$(d - a(2))\,(d - a(3)) \cdots (d - a(k)) \cdot \sum_{i \in K_d(a)} \alpha_i \equiv 0 \,(\mathrm{mod}\, \alpha)\,.$$

Proof. As the entries of the matrix $M(a, \mathfrak{B})$ are all integers, all the eigenvalues are algebraic integers. Also the minimal polynomial $m(x)$ of $M(a, \mathfrak{B})$ has rational coefficients. Since $M(a, \mathfrak{B})$ is diagonalizable (see [5], Lemma 2.1),

$$m(x) = (x - a(1))(x - a(2)) \cdots (x - a(k)).$$

By assumption $a(1)$ is an integer, so the polynomial

$$f(x) = (x - a(2))(x - a(3)) \cdots (x - a(k))$$

also has rational coefficients.

As all the coefficients of $f(x)$ are algebraic integers, the coefficients of $f(x)$ are integers.

Note that if s is such that $a(s) \neq d$, then $f(a(s)) = 0$, while

$$f(a(s)) = (d - a(2))(d - a(3)) \cdots (d - a(k))$$

whenever s is such that $a(s) = d$, that is, whenever $s \in K_d(a)$.

Set $f(x) = \sum_{i=0}^{k-1} n_i x^i$ where the n_i's are integers. We compute $\sum_{j=1}^{n} \alpha_j \cdot f\left(a(j)\right)$ in two ways. First, the previous paragraph shows that

$$\sum_{j=1}^{n} \alpha_j \cdot f\left(a(j)\right) = (d - a(2))(d - a(3)) \cdots (d - a(k)) \sum_{j \in K_d(a)} \alpha_j.$$

Next

$$\sum_{j=1}^{n} \alpha_j \cdot f\left(a(j)\right) = \sum_{j=1}^{n} \alpha_j \left(\sum_{i=0}^{k-1} n_i \cdot a(j)^i \right) = \sum_{i=0}^{k-1} n_i \sum_{j=1}^{n} \alpha_j \cdot a(j)^i.$$

By assumption, each $\sum_{j=1}^{n} \alpha_j \cdot a(j)^i$ is an integral multiple of α. Also the n_i's are integers, so $\sum_{j=1}^{n} \alpha_j \cdot f\left(a_j\right)$ is a multiple of α. This ends the proof. □

Corollary 6. 1. *(Theorem 3). Let G be a finite group, θ a generalized character of G, and $d, d_2, d_3, \ldots, d_m$ the distinct values of θ, where d is rational. Set $V_d(\theta) = \{x \in G \mid \theta(x) = d\}$. Then*

$$|V_d(\theta)|\,(d - d_2)\,(d - d_3) \cdots (d - d_m) \equiv 0 \mod |G|\,.$$

2. *(Generalization of Theorem 2). Let G be a finite group, C a conjugacy class of G and $d, d_2, d_3, \ldots, d_m$ the distinct elements in the multiset $\left\{ \frac{|C|\chi(C)}{\chi(1)} \mid \chi \in \mathrm{Irr}(G) \right\}$. Assume that d is an integer and set*

$$I_d(C) = \left\{ \chi \in \mathrm{Irr}(G) \mid \frac{|C|\,\chi(C)}{\chi(1)} = d \right\}.$$

Then

$$\left(\sum_{\chi \in I_d(C)} \chi^2(1) \right) \cdot (d - d_2)\,(d - d_3) \cdots (d - d_m) \equiv 0 \mod |G|.$$

Proof. Set $class(G) = \{C_1, C_2, \ldots, C_n\}$ to be the collection of conjugacy classes of G, and $\mathrm{Irr}(G) = \{\chi_1, \chi_2, \ldots, \chi_n\}$.

1. Clearly we can rearrange $class(G)$ such that

$$d = \theta(C_1), d_2 = \theta(C_2), \ldots, d_m = \theta(C_m), d_{m+1} = \theta(C_{m+1}), \ldots, d_n = \theta(C_n).$$

Let $A = \mathbb{Q}(\mathrm{Irr}(G))$ be the algebra generated by $\mathfrak{B} = \mathrm{Irr}(G)$ over the rationals $\mathbb{Q}$. Then A is a semi-simple, n-dimensional commutative $\mathbb{Q}$-algebra and $\theta \in A$. By the orthogonality relations $M(\theta, \mathfrak{B})$ consists of integer entries; also d is rational by assumption, hence an integer. Furthermore, $M(\theta, \mathfrak{B})$ is diagonalized by the character table and its eigenvalues are $\theta(C_1) = d, \theta(C_2), \ldots, \theta(C_n)$ (see [4]). Let $(\alpha_1, \alpha_2, \ldots, \alpha_n) = (|C_1|, |C_2|, \ldots, |C_n|)$. Then

$$\sum_{j=1}^{n} \alpha_j \left(\theta(j)\right)^i = \sum_{j=1}^{n} |C_j|\,\theta(C_j)^i = \sum_{g \in G} \theta(g)^i = |G| \left(\theta^i, 1_G\right).$$

As $\left(\theta^i, 1_G\right)$ is an integer, we can apply Theorem 5 to get

$$(d - d_2)\,(d - d_3) \cdots (d - d_m) \cdot \sum_{i \in K_d(\theta)} \alpha_i \equiv 0 \,(\mathrm{mod}\, \alpha).$$

Note that $K_d(\theta) = \{i \mid \theta(C_i) = d\}$ so that $\sum_{i \in K_d(\theta)} \alpha_i = \sum_{\theta(C_i) = d} |C_i| = |V_d(\theta)|$. Also, $\alpha = \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} |C_i| = |G|$. The result follows.

2. Let $A = Z(\mathbb{Q}\mathbb{G})$, the center of the group algebra of G over $\mathbb{Q}$. For every $D \in class(G)$ let $\overline{D} = \sum_{x \in D} x$. Then $\mathfrak{B} = \left\{\overline{C}_i \mid i = 1, 2, \ldots, n\right\}$ is a basis of A. Moreover, A is a semi-simple, n-dimensional commutative $\mathbb{Q}$-algebra and $\overline{C} \in A$. It is well known ([6], p. 15) that $M(\overline{C}, \mathfrak{B})$ consists of integer entries, it can be diagonalized and its eigenvalues (e.g. [5], p. 155) are the numbers $\overline{C}(i) = \frac{|C|\chi_i(C)}{\chi_i(1)}$ for $i = 1, 2, \ldots, n$.

Clearly we can rearrange $\mathrm{Irr}(G)$ such that

$$d = \frac{|C|\,\chi_1(C)}{\chi_1(1)}, d_2 = \frac{|C|\,\chi_2(C)}{\chi_2(1)}, \ldots, d_m = \frac{|C|\,\chi_m(C)}{\chi_m(1)},$$
$$d_{m+1} = \frac{|C|\,\chi_{m+1}(C)}{\chi_{m+1}(1)}, \ldots, d_n = \frac{|C|\,\chi_n(C)}{\chi_n(1)}.$$

By assumption d is an integer.

Let $(\alpha_1, \alpha_2, \ldots, \alpha_n) = \left(\chi_1^2(1), \chi_2^2(1), \ldots, \chi_n^2(1)\right)$. Then:

$$\sum_{j=1}^{n} \alpha_j \left(a(j)\right)^i = \sum_{j=1}^{n} \chi_j^2(1) \left(\overline{C}(j)\right)^i = \sum_{j=1}^{n} \chi_j^2(1) \left(\frac{|C|\,\chi_j(C)}{\chi_j(1)}\right)^i$$
$$= |C|^i \sum_{j=1}^{n} \frac{\left(\chi_j(C)\right)^i}{\chi_j^{i-2}(1)} = |G| \cdot \frac{|C|^i}{|G|} \sum_{j=1}^{n} \frac{\left(\chi_j(C)\right)^i \chi_j(1)}{\chi_j^{i-1}(1)}.$$

Next,

$$\frac{|C|^i}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C)^i \cdot \chi(1)}{\chi(1)^{i-1}}$$

is an integer for every i. It is the coefficient of 1 in the expansion $\overline{C}^i = \sum \alpha_j \overline{C}_j$, so it is the number of times that 1 can be written as a product of exactly i elements of C (see [1], Lemma 10.1, pp. 43-44).

Note that $\alpha = \sum_{i=1}^{n} \chi_i^2(1) = |G|$ and that

$$\sum_{i \in K_d(\overline{C})} \alpha_i = \sum_{|C|\frac{\chi(C)}{\chi(1)} = d} \chi^2(1) = \sum_{\chi \in I_d(C)} \chi^2(1).$$

Now the result follows from Theorem 5. □

If we chose $d = |C|$ in part 2 of the corollary, then

$$\sum_{\chi \in I_d(C)} \chi^2(1) = \sum_{\chi(C) = \chi(1)} \chi^2(1) = \sum_{C \subset \ker(\chi)} \chi^2(1) = \sum_{\langle C \rangle \subset \ker(\chi)} \chi^2(1)$$
$$= \sum_{\chi \in \mathrm{Irr}\left(\frac{G}{\langle C \rangle}\right)} \chi^2(1) = |G/\langle C \rangle|.$$

Thus, Theorem 2 follows from part 2 of the corollary.

We finish with a description of groups for which $|\langle C \rangle| = (|C| - d_2)$.

Proposition 7. *Let G be a finite group and C a conjugacy class of G. Let $d = |C|, d_2, d_3, \ldots, d_m$ be the distinct elements in the multiset $\left\{ \frac{|C|\chi(C)}{\chi(1)} \mid \chi \in \mathrm{Irr}(G) \right\}$. Then $m = 2$ and $|\langle C \rangle| = (d - d_2)$ if and only if $\langle C \rangle = C \cup \{1\}$ is a minimal normal elementary abelian p-subgroup for some prime p.*

Proof. Let $\mathrm{Irr}(G/\langle C \rangle) = \{\chi_1, \chi_2, \ldots, \chi_r\}$ and

$$\mathrm{Irr}(G) = \{\chi_1, \chi_2, \ldots, \chi_r, \chi_{r+1}, \ldots, \chi_k\}.$$

Assume first that $m = 2$ and $|\langle C \rangle| = (d - d_2)$. Then there exists an $\alpha \neq 1$ such that

$$\frac{\chi_i(C)}{\chi_i(1)} = \begin{cases} 1 & \text{for } 1 \leq i \leq r, \\ \alpha & \text{for } r+1 \leq i \leq k. \end{cases}$$

As $d_2 = |C|\,\alpha$, $d = |C|$ and $|\langle C \rangle| = (d - d_2)$ we get that $\alpha \neq 0$.

Let $x \in \langle C\rangle - \{1\}$. We wish to show that $x \in C$. Suppose the contrary. Then $\sum_{i=1}^{k} \chi_i(C)\overline{\chi_i(x)} = 0$. Let $y \in C$. Then

$$\begin{aligned} 0 &= \sum_{i=1}^{r} \chi_i(y)\overline{\chi_i(x)} + \sum_{i=r+1}^{k} \chi_i(C)\overline{\chi_i(x)} = \sum_{i=1}^{r} \chi_i(y\,\langle C\rangle)\overline{\chi_i(x\,\langle C\rangle)} \\ &\quad + \alpha \sum_{i=r+1}^{k} \chi_i(1)\overline{\chi_i(x)} = \sum_{i=1}^{r} \chi_i^2(1) + \alpha\left[\sum_{i=1}^{k} \chi_i(1)\overline{\chi_i(x)} - \sum_{i=1}^{r} \chi_i(1)\overline{\chi_i(x)}\right] \\ &= \frac{|G|}{|\langle C\rangle|} + \alpha\left[0 - \sum_{i=1}^{r} \chi_i(\langle C\rangle)\overline{\chi_i(x\,\langle C\rangle)}\right] = \frac{|G|}{|\langle C\rangle|} - \alpha\sum_{i=1}^{r} \chi_i^2(1) \\ &= \frac{|G|}{|\langle C\rangle|} - \alpha\frac{|G|}{|\langle C\rangle|}. \end{aligned}$$

This forces $\alpha = 1$, a contradiction. Hence $\langle C\rangle - \{1\}$ is a conjugacy class, and as $C \subset \langle C\rangle$ we get $\langle C\rangle = C \cup \{1\}$ as desired. Now $\langle C\rangle$ is a minimal normal subgroup in G, and all elements of $\langle C\rangle - \{1\}$ have the same order. So $\langle C\rangle$ is an elementary abelian p-subgroup for some prime p.

Conversely, assume that $\langle C\rangle = C \cup \{1\}$ is a minimal normal elementary abelian p-subgroup for some prime p. Then $\chi_i(C) = \chi_i(1)$ for $1 \le i \le r$ and $d = |C|$. Let $i > r$ and $\chi = \chi_i$. Then $C \nleq \ker(\chi)$ and so $\chi_{\langle C\rangle} = e(\lambda_1 + \lambda_2 + \cdots + \lambda_s)$ where $\lambda_i \in \mathrm{Irr}(\langle C\rangle)$. As $\langle C\rangle$ is abelian and all elements of $\langle C\rangle - \{1\}$ are conjugate, Brauer's Permutation lemma implies that $\{\lambda_1, \lambda_2, \ldots, \lambda_s\} = \mathrm{Irr}(\langle C\rangle) - \{1_{\langle C\rangle}\}$. So $\chi(a) = -e$ for all $a \in \langle C\rangle - \{1\}$. Also $\chi(1) = se$ and $s = |\langle C\rangle - \{1\}| = |C|$. It follows that $m = 2$ and

$$d_2 = \frac{|C|\,\chi(C)}{\chi(1)} = -\frac{|C|\,e}{se} = -\frac{|C|}{|C|} = -1.$$

Finally

$$d - d_2 = |C| - (-1) = |\langle C\rangle|\,. \qquad \square$$

References

[1] Arad, Z.; Stavi, J.; Herzog, M. Powers and products of conjugacy classes in groups. Products of Conjugacy Classes in Groups, Lecture Notes in Math., 1112 (1985) 6–51, Springer, Berlin. MR783068

[2] Blichfeldt, H. F., A theorem concerning the invariants of linear homogeneous groups, with some applications to substitution groups. Transactions of the American Mathematical Society 5 (1904), 461-466. MR1500684

[3] Cameron, P. J.; Kiyota, M. Sharp characters of finite groups. J. Algebra 115 (1988), 125–143. MR937604 (89b:20026)

[4] D. Chillag, Character values of finite groups as eigenvalues of nonnegative integer matrices, Proceedings of the American Math. Society, 97 (1986), 565-567. MR840647 (87f:20017)

[5] D. Chillag, Regular representations of semisimple algebras, separable field extensions, group characters, generalized circulants, and generalized cyclic codes, Linear Algebra and its Applications, 218 (1995), 147-183. MR1324056 (96d:16024)

[6] I. M. Isaacs, Character Theory of Finite Groups, Academic Press, 1976. MR0460423 (57:417)

[7] Kiyota, M. An inequality for finite permutation groups. J. Combin. Theory Ser. A 2, 1 (1979), 119. MR541348 (81f:20009)

Department of Mathematics, Technion, Israel Institute of Technology, Haifa, Israel
E-mail address: chillag@techunix.technion.ac.il