ISRAEL JOURNAL OF MATHEMATICS, Vol. 31, No. 1, 1978

CONJUGACY CLASSES IN FINITE GROUPS

BY
AVINOAM MANN

ABSTRACT

In the first part of this note, we give new proofs of known results regarding the class number of finite groups, adding a few related results. In the second part, we improve a result of Ito concerning a special class of p-groups.

1. Let G be a finite group having g elements and $r = r(G)$ conjugacy classes. Then the number of (ordered) commuting pairs of elements of G is gr [2]. Therefore the number of non-commuting pairs is $g^2 - gr$.

For a group H, let $\varphi_2(H)$ be the number of pairs, $a, b \in H$, such that $H = \langle a, b\rangle$. Counting pairs by the subgroups they generate, we get

$$g^2 - gr = \sum \varphi_2(H) \qquad (H \text{ is a non-abelian subgroup of } G). \tag{1}$$

From here to the end of Section 1, let G be a p-group. If H is a non-abelian 2-generator subgroup of G, then $H/\Phi(H)$ is of order p^2 and has $(p^2-1)(p^2-p)$ pairs of generators, so $\varphi_2(H) = (p^2-1)(p^2-p)|\Phi(H)|^2$. Substituting this in (1), we find $g^2 \equiv gr((p^2-1)(p-1))$, hence

$$g \equiv r((p^2-1)(p-1)). \tag{2}$$

The congruence (2) is the main step in proving the following result of P. Hall [4, V.15.2].

Let G be a group of order p^{2n+e}, $e = 0$ or 1, then for some non-negative integer k:

$$r = p^e + (p^2-1)(n + k(p-1)). \tag{3}$$

To prove (3), one notes first that

Received December 4, 1977

$$p^{2n+e} = p^e + (p^{2n}-1)p^e = p^e + (p^2-1)(p^{2n-2}+\cdots+p^2+1)(p^e-1+1)$$
$$\equiv p^e + (p^2-1)(p^{2n-2}+\cdots+p^2+1) \equiv p^e + (p^2-1)n \ \ ((p^2-1)(p-1)).$$

Thus (2) implies (3) with k an integer. To show that $k \geqq 0$ we first check that $k = 0$ for $g = p$. Next, for $g > p$, let N be a minimal normal subgroup of G. Then each class of G maps onto a class of G/N, so $r(G) \geqq r(G/N)$. Writing formula (3) for G and for G/N, we see that if $k(G) < k(G/N)$, then $r(G) < r(G/N)$. Hence $k(G) \geqq k(G/N)$, so $k(G) \geqq 0$ by induction.

Our proof of (2) is a simplification of one by Poland [7]. We present now a different proof, which was suggested in [10]. We first prove:

Let χ be a non-principal irreducible character of G. The number of algebraic conjugates of χ is divisible by $p-1$.

Indeed, we may assume that χ is faithful. Let z be a central element of order p in G. Then $\chi(z) = \chi(1)\varepsilon$, for some primitive p-root of unity ε. For each $0 < i < p$, the number of algebraic conjugates φ of χ such that $\chi(z) = \varphi(1)\varepsilon^i$ is independent of i, hence our claim (this is also proved in the course of proving (3) in [4, V.15]).

Now write

$$g = \sum_1^r \chi(1)^2 \tag{4}$$

summing over all irreducible characters of G. If $\chi(\neq 1_G)$ has $t = (p-1)s$ conjugates, the contribution of these conjugates is $(p-1)s\chi(1)^2 = (p-1)sp^{2m} \equiv (p-1)s((p^2-1)(p-1))$ so summing in (4) by families of conjugate characters yields (2).

The equality (1) can yield more information. Let n_3 be the number of non-abelian subgroups of order p^3 of G. Each of those contributes $(p^2-1)(p-1)p^3$ to the right hand side of (1). For the other terms in (1), $|\Phi(H)| \geqq p^2$ and $p^5 | \varphi_2(H)$. If $g \geqq p^5$, we divide (1) by p^3 and get:

The number of non-abelian subgroups of order p^3 of a p-group of order $\geqq p^5$ is divisible by p^2.

The number of all subgroups of order p^3 is generally $\equiv 1 + p(p^2)$ [4, III, 8.8] so, by subtracting:

The number of abelian subgroups of order p^3 of a non-cyclic p-group of order at least p^5, p odd, is congruent to $p+1 (\mathrm{mod}\, p^2)$.

(The fact that this number is $\equiv 1(p)$ was established in [6].)

Next, let n_4 be the number of non-abelian 2-generator subgroups of G of order p^4. For these subgroups $\varphi_2(H)=(p^2-1)(p-1)p^5$, while for subgroups of higher order, $p^7 \mid \varphi_2(H)$. Dividing again (1) by p^3, we now see that, provided $g \geqq p^7$, the number $n_3+p^2n_4$ is divisible by p^4. Generally, let n_k be the number of non-abelian 2-generator subgroups of G, of order p^k, then the same method yields:

If $g \geqq p^{2k-1}$, *then* $n_3+p^2n_4+\cdots+p^{2k-6}n_k$ *is divisible by* p^{2k-4}.

Finally, we derive a relative version of (2). Thus, let $N \lhd G$, and let N contain exactly s classes of G. Let $n=|N|$, and denote by $\varphi_{2,N}(H)$, for $H \subseteq G$, the number of pairs of generators a, b of H with $a \in N$. Then, analogously to (1), we have

(5) $$gn-gs=\sum \varphi_{2,N}(H) \qquad (H \text{ a non-abelian subgroup of } G).$$

Let $N_1=N\cap H$. If $H=N_1$, then $\varphi_{2,N}(H)=\varphi_2(H)$. If $N_1 \subseteq \Phi(H)$, then $\varphi_{2,N}(H)=0$. Finally, if $H \neq N_1 \nsubseteq \Phi(H)$, then

$$|H: N_1\Phi(H)|=|N: N_1\cap\Phi(H)|=p$$

and we are interested in pairs (a,b) with $a\in N_1-N_1\cap\Phi(H)$, $b\in H-N_1\Phi(H)$, the number of such pairs being

$$\begin{aligned}\varphi_{2,N}(H)&=(|N_1|-|N_1\cap\Phi(H)|)(|H|-|N_1\Phi(H)|)\\&=(p-1)^2|N_1\cap\Phi(H_1)|\,|N_1\Phi(H)|(=(p-1)^2|N_1|\,|\Phi(H)|).\end{aligned}$$

Substituting these values in (5) yields

(6) $$n \equiv s \ \ ((p-1)^2).$$

2. We now pass to arbitrary finite groups. Recall P. Hall's definition of the Möbius function $\mu_G(H)$ [1]. This is

(7) $$\mu_G(G)=1, \quad \sum_{K\supseteq H}\mu_G(K)=0 \qquad (H \text{ a proper subgroup of } G).$$

Hall shows in [1] that if $f(H)$ is a function defined on the subgroups of G, then letting

(8) $$g(H)=\sum_{K\subseteq H} f(K)$$

one has

$$f(H) = \sum_{K \subseteq H} \mu_H(K) g(K) \tag{9}$$

and in particular

$$\varphi_2(H) = \sum_{K \subseteq H} \mu_H(K) |K|^2, \tag{10}$$

$$\sum_{K \subseteq H} \mu_H(K) |K| = 0 \qquad (H \text{ non-cyclic}). \tag{11}$$

The last equation expresses the fact that H has no one-element generating sets.

Adding (10), (11) and the second equation in (7), we see that for a non-cyclic H, and arbitrary numbers a, b

$$\varphi_2(H) = \sum_{K \subseteq H} \mu_H(K)(|K|^2 + a|K| + b). \tag{12}$$

Therefore, if $(d, g) = 1$, and $d \mid |K|^2 + a|K| + b$ for all $K \subseteq H$, then (1) shows that $g \equiv r(d)$. Let $p_1, \cdots, p_u$ be the primes dividing g. Since

$$kl - 1 = k(l-1) + k - 1$$

we see that if $d \mid p_i - 1$ for all i, then $d \mid |K| - 1$ for all K, and $d^2 \mid (|K| - 1)^2$. Similarly, if $d \mid p_i^2 - 1$ for all i, $d \mid |K|^2 - 1$. Hence

(13) $g \equiv r$ *(modulo the* gcd *of* $(p_i^2 - 1)$, *and also modulo the* gcd *of* $(p_i - 1)^2$).

These congruences are proved in [2] and [7], respectively. In [2] Hirsch also proves that, for odd g, $g \equiv r(\operatorname{mod} 2 \gcd(p_i^2 - 1))$. A different proof was given by van der Waall [10].

To get a relative version of (13), we first point out that, the notation being as in (5) and (6),

$$\sum_{K \subseteq H} \varphi_{2,N}(K) = |N \cap H| |H| \tag{14}$$

and that, if H is not a cyclic subgroup of N,

$$\sum_{K \subseteq H} \mu_H(K) |K \cap N| = 0, \tag{15}$$

so for such H

$$\varphi_{2,N}(H) = \sum_{K \subseteq H} \mu_H(K)(|K||K \cap N| + a|K| + b|K \cap N| + c),$$

(16) $n \equiv s$ *(modulo the* gcd *of* $(p_i - 1)^2$).

Let $p_1, \cdots, p_v$ be those primes dividing n, let $d = \gcd(p_1 - 1, \cdots, p_u - 1)$, $e = \gcd(p_i - 1, \cdots, p_v - 1)$, and let f be the part of e that is prime to g. Then (16) can be improved slightly to

$$n \equiv s(df). \tag{17}$$

We note one final formula. Denote

$$\psi_2(H) = \{\text{number of commuting pairs of elements generating } H\},$$

then $\Sigma_{H \subseteq G} \psi_2(H) = gr$, the total number of commuting pairs. For G non-abelian, $\psi_2(G) = 0$, so by (9)

$$\text{If } G \text{ is non-abelian: } \sum_{H \subsetneq G} \mu_G(H)|H|r(H) = 0. \tag{18}$$

This relation can be regarded as a recurrence formula for $r(G)$.

3. In [5] Ito defines an F-group to be a group in which $C_G(a) \subseteq C_G(b)$ only if $b \in Z(G)$ or $C_G(a) = C_G(b)$. A special class of F-groups are $(n, 1)$-groups, which are the groups in which each class has size 1 or n. The F-groups which are not p-groups have been determined by Rebmann [8]. Let G be an F-group which is a p-group. Then Ito proves the existence of a normal abelian subgroup A, such that G/A has exponent p. Here we show

THEOREM. *Let G be a p-group and an F-group. Then either G has an abelian maximal group, or $G/Z(G)$ has exponent p.*

PROOF. We take G to be non-abelian. For each $a \in G - Z(G)$, let $Z(a) = Z(C_G(a))$. Then, by [8, 4.1], the subgroups $Z(a)/Z$ form a partition of G/Z ($Z = Z(G)$). Assume that G/Z has exponent greater than p. By [5], all elements of order greater than p in G/Z belong to the same component, $Z(u)/Z$ say, of the partition, and $Z(u)/Z$ is the unique normal component of the partition.

Suppose that $Z(u) \neq C(u)$. Pick a $z \in Z(u)$ and $a \in C(u) - Z(u)$ such that z has order greater than p in G/Z. Since $a, az \notin Z(u)$ we have $a^p, (az)^p \in Z$, hence $z^p \in Z$, a contradiction. Thus $Z(u) = C(u)$ is abelian. Since $Z(u) \lhd G$, there exists an $a \in Z(u)$ such that $a \in Z_2(G) - Z(G)$. Then $C(u) = C(a) \supseteq G'$, so $G/C(u)$ is abelian and G is metabelian. But then, $C(u)$ containing all elements of order greater than p in G/Z, [3] implies $|G : C(u)| = p$, and $C(u)$ is an abelian maximal subgroup.

A special class of F-groups, those in which all proper centralizers are abelian, is discussed by Rocke [9]. Our result implies theorem 3.13 (b) of that paper.

Now let G be an $(n, 1)$-group. Let $|G| = p^m$, $|Z| = p^z$, $n = p^t$. Then the class number of G is

$$r = p^z + \frac{p^m - p^z}{p^t} = p^z + p^{m-t} - p^{z-t}.$$

Substitute this value in (2). Thus

$$p^m \equiv p^z + p^{m-t} - p^{z-t} \quad ((p^2-1)(p-1)),$$

$$(19) \qquad p^{z-t}(p^{m-z}-1)(p^t-1) \equiv 0 \quad ((p^2-1)(p-1)),$$

$$(p^{m-z}-1)(p^t-1) \equiv 0 \quad ((p^2-1)(p-1)).$$

But $p^{2k+1} - 1 = (p^{2k}-1)p + p - 1 \equiv (p-1)\ (p^2-1)$, so if both $m - z$ and t are odd, the left-hand side of (19) is $\equiv (p-1)^2 \not\equiv 0\ (p^2-1)$, hence

Either $m - z$ or t is even.

Added in proof, April 1978. The congruence (13) can be generalized, to include also Hirsch's result for odd groups, as well as (2). Namely

THEOREM. *Let $p_1, \cdots, p_u$ be the primes dividing the order g of the group G. Let $d = \gcd(p_1 - 1, \cdots, p_u - 1)$, $\delta = \gcd(p_1^2 - 1, \cdots, p_u^2 - 1)$. Then*

$$(20) \qquad g \equiv r \pmod{d\delta}.$$

PROOF. Let $g = p_1^{e_1} \cdots p_u^{e_u}$. Let k_i have order $d \pmod{p_i^{e_i}}$, then k_i has order d also $\pmod{p_i}$. There exists a number k, unique $\pmod g$, such that $k \equiv k_i \pmod{p_i^{e_i}}$ for all i. Then k has order d exactly modulo any divisor ($\neq 1$) of g. The map $a \to a^k$ of G induces a permutation on the conjugacy classes of G. If a and a^{k^n} are conjugate, by $b \in G$ say, then b induces on $\langle a \rangle$ an automorphism of order dividing d. But $(d, g) = 1$, so that b centralizes $\langle a \rangle$, $a = a^{k^n}$, so that $k^n \equiv 1$ $(|a|)$ and n is a multiple of d. Thus each orbit of this permutation of classes has length d (except for the orbit consisting of the identity element). Let $\chi_1, \cdots, \chi_u$ be the irreducible characters of G. Then $\chi \to \chi^{(k)}$, where $\chi^{(k)}(a) = \chi(a^k)$ is a permutation of the characters. By Brauer's lemma (e.g. [11, (12.1)]) this permutation has the same number of orbits as the previous one on classes. Moereover, one of these orbits has length 1 (the principal character) and the others' length is $\leqq d$. Hence they all have length d exactly. Thus the non-principal characters can be grouped in families, each family containing d characters of the same degree. If this common degree is m, then this family contributes to the right hand side of (4)

$$dm^2 \equiv d \pmod{d\delta}.$$

Summing in (4) by families, we get our result.

REMARK. This argument is a generalization of Burnside's [12, pp. 294/5]. It has been pointed out in [7] that one cannot generalize further to $g \equiv r(\bmod \gcd((p_i - 1)(p_i^2 - 1)))$.

REFERENCES

1. P. Hall, *The Eulerian functions of a group*, Quart. J. Math. **7** (1936), 134–151.
2. K. A. Hirsch, *On a theorem of Burnside*, Quart. J. Math (2) **1** (1950), 97–99.
3. G. T. Hogan and W. P. Kappe, *On the H_p-problem for finite p-groups*, Proc. Amer. Math. Soc. **20** (1969), 450–454.
4. B. Huppert, *Endliche Gruppen I*, Berlin, 1967.
5. N. Ito, *On finite groups with given conjugate types I*, Nagoya. Math. J. **6** (1953), 17–28.
6. M. Konvisser and D. Jonah, *Counting abelian subgroups of p-groups. A projective approach*, J. Algebra **34** (1975), 309–330.
7. J. Poland, *Two problems on finite groups with k conjugate classes*, J. Austral. Math. Soc. **8** (1968), 49–55.
8. J. Rebmann, *F-Gruppen*, Arch. Math. **22** (1971), 225–230.
9. D. M. Rocke, *p-groups with abelian centralizers*, Proc. London Math. Soc. (3) **30** (1975), 55–75.
10. R. W. van der Waall, *On a theorem of Burnside*, Elem. Math. **25** (1970), 136–137.
11. W. Feit, *Characters of Finite Groups*, New York, 1967.
12. W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., Dover, 1955.

THE HEBREW UNIVERSITY OF JERUSALEM
JERUSALEM, ISRAEL