数理解析研究所講究録
1140 巻 2000 年 136-139

The number of subgroups of a finite p-group

Yugen Takegahara
竹ヶ原 裕元
Muroran Institute of Technology
室蘭工業大学

1 The main result

For a finitely generated group A, $m_A(d)$ denotes the number of subgroups of index d in A. Let p be a prime. We say that a finitely generated group A admits $\mathrm{CP}(p^s)$, where s is a positive integer, if the following conditions hold:

(1) For any integer i with $1 \leq i \leq [(s+1)/2]$, where $[(s+1)/2]$ is the greatest integer $\leq (s+1)/2$,

$$m_A(p^{i-1}) \equiv m_A(p^i) \bmod p^i.$$

(2) Moreover

$$m_A\left(p^{\left[\frac{s+1}{2}\right]}\right) \equiv m_A\left(p^{\left[\frac{s+1}{2}\right]+1}\right) \bmod p^{\left[\frac{s}{2}\right]}.$$

For a finite group A, let A' be the commutator subgroup of A, $|A|$ the order of A, and $\exp A$ the exponent of A. Hereafter, we will mainly treat the results for p-groups. Butler proved the following [3]:

Proposition 1 *Any finite abelian p-group P admits* $\mathrm{CP}(|P|)$.

Question 2 What p-groups P admit $\mathrm{CP}(|P:P'|)$?

A finite p-group P admits $\mathrm{CP}(p)$, because

$$m_P(p) = m_{P/\Phi(P)}(p) \equiv 1 = m_P(1) \bmod p,$$

where $\Phi(P)$ denotes the Frattini subgroup of P. Also, for any finite p-group P such that $|P/\Phi(P)| = p^s$,

$$m_P(p^i) \equiv m_{P/\Phi(P)}(p^i) \bmod p^{s-i+1}$$

by [4, Theorem 1.61]. This result, together with Proposition 1, implies that any finite p-group P admits $\mathrm{CP}(|P:\Phi(P)|)$ [8, Theorem 1.1]. So if the factor group P/P' of a finite p-group P by P' is elementary abelian, then P admits $\mathrm{CP}(|P:P'|)$. As a generalization of this fact, we have the following main result of this report.

Theorem 3 *If P/P' is the direct product of a cyclic group and an elementary abelian group, then P admits* $\mathrm{CP}(|P:P'|)$.

2 Related results

For a finitely generated group A and for a finite group G, Hom(A,G) denotes the number of homomorphisms from A to G. Let S_n be the symmetric group of degree n. In [9] Wohlfahrt proved that for a finitely generated group A,

$$1+\sum_{n=1}^{\infty}\frac{\sharp\mathrm{Hom}(A,S_n)}{n!}X^n=\exp\left(\sum_{B\leq A}\frac{1}{|A:B|}X^{|A:B|}\right)$$

where the summation $\sum_{B\leq A}$ runs over all subgroups B of A with the factor groups A/B are finite groups. Using this formula we can prove the following.

Proposition 4 *If a finite p-group P admits* CP(p^s), *then*

$$\sharp\mathrm{Hom}(P,S_n)\equiv 0 \bmod \gcd(p^s,n!).$$

This proposition is a special case of [7, Theorem 1.2]. Combining Proposition 4 with Proposition 1 and 3, we have the following.

Corollary 5 *Let P be a finite p-group.*

(1) *If P is abelian, then* $\sharp\mathrm{Hom}(P,S_n)\equiv 0 \bmod \gcd(|P|,n!)$.

(2) *If P/P' is the direct product of a cyclic group and an elementary abelian group, then* $\sharp\mathrm{Hom}(P,S_n)\equiv 0\,\gcd(|P:P'|,n!)$.

The assertions of Corollary 5 are special cases of these results.

Theorem 6 ([10]) *For a finite abelian group A and for a finite group G,*

$$\sharp\mathrm{Hom}(A,G)\equiv 0 \bmod \gcd(|A|,|G|).$$

Theorem 7 ([1, 2]) *For a finite groups A and G, if a Sylow p-subgroup of A/A' is either a cyclic group or the direct product of a cyclic group and an elementary abelian group for each prime p dividing $|A/A'|$, then*

$$\sharp\mathrm{Hom}(A,G)\equiv 0 \bmod \gcd(|A/A'|,|G|).$$

The above Theorem 6 due to Yoshida is a generalization of the following Frobenius' theorem:

Theorem 8 *The number of solutions of $x^n=1$ in a finite group H is a multiple of* $\gcd(n,|H|)$.

3 Key results

For a finite group H and for a finite group C that acts on H, let $z(C, H)$ denote the number of all complements of H in the semidirect product CH with respect to a fixed action of C on H, i.e.,

$$z(C,H) = \sharp\{D \leq CH | D \cap H = \{1\}, DH = CH\},$$

which is equal to the number of all crossed homomorphisms from C to H. The following proposition is due to Asai and Yoshida [2, Proposition 3.3]:

Proposition 9 *Let H be a finite p-group and C a cyclic p-group that acts on H. Then $z(C, H) \equiv 0 \bmod \gcd(|C|, |H|)$.*

This result is a special case of the following theorem due to P. Hall [5, Theorem 1.6]:

Theorem 10 *For a finite group H and for an automorphism θ of H with $\theta^n = 1$, the number of elements x of H that satisfy the equation*

$$x \cdot x^{\theta} \cdot x^{\theta^2} \cdots x^{\theta^{n-1}} = 1$$

is a multiple of $\gcd(n, |H|)$.

This theorem is also a generalization of Theorem 8. Proposition 9 played an important role in the proof of Theorem 7. For the proof of Theorem 3, we need another type of result concerning $z(C, H)$. The following theorem is due to P.Hall [4, 6]:

Theorem 11 *Let x and y be any elements of a finite group G. Then there exist elements $c_2, c_3, \ldots, c_n$ of $\langle x, y\rangle$ such that c_i is an element of $C_i(\langle x, y\rangle)$ for each i and*

$$x^n y^n = (xy)^n c_2^{e_2} c_3^{e_3} \cdots c_n^{e_n}$$

where $e_i = n(n-1)\cdots(n-i+1)/i!$ for each i.

Using Theorem 11, we obtain the following.

Proposition 12 *Let H be a finite p-group and C a cyclic p-group that acts on H. If $\exp H \leq |C|$ and $|[CH, H]| < |C|$, then $z(C, H) = |H|$.*

To prove Theorem 3, we use this fact and the following result [8, Proposition 2.2]:

Proposition 13 *Let L be a finite group and H a normal subgroup of L such that L/H is a cyclic p-group. Let C be a cyclic p-subgroup of L with $C \cap H = \{1\}$. If $L \neq CH$ and $z(C, H) = |H|$, then $\{\tilde{C} \leq L | \tilde{C} \cap H = \{1\}, |\tilde{C}| = p|C|\}$ is not empty.*

4 Further results

The following proposition is a special case of [8, Theorem 1.2].

Theorem 14 *Let P be a finite p-group such that* $\exp P/P' = p^{\lambda_1}$. *Then*

$$m_P(p^{i-1}) \equiv m_P(p^i) \bmod p^i$$

for any integer i with $1 \leq i \leq \lambda_1$.

Corollary 15 *Under the hypothesis of Theorem 14, P admits* $\mathrm{CP}(p^s)$ *if* $2\lambda_1 \geq s+2$.

A sequence $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r, 0, \ldots)$ of nonnegative integers in weekly decreasing order is called the type of a finite abelian p-group isomorphic to

$$\mathbb{Z}/p^{\lambda_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\lambda_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\lambda_r}\mathbb{Z}.$$

Question 16 Does a finite p-group P such that the type $\lambda = (\lambda_1, \lambda_2, \ldots)$ of P/P' satisfies $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$ admit $\mathrm{CP}(|P : P'|)$?

As an answer of the Question 16, we have the following.

Theorem 17 *Let P be a finite p-group, and let $\lambda = (\lambda_1, \lambda_2, \ldots)$ be the type of P/P'. If $\lambda_2 \leq 2$, $\lambda_3 \leq 1$ and $\lambda_1 \geq \lambda_2 + \lambda_3 + \cdots$, then P admits* $\mathrm{CP}(|P : P'|)$.

References

[1] T. Asai and Y. Takegahara, On the number of crossed homomorphisms, *Hokkaido Math. J.*, to appear.

[2] T. Asai and T. Yoshida, $|\mathrm{Hom}(A, G)|$, II, *J. Algebra* **160** (1993), 273–285.

[3] L. M. Butler, A unimodality result in the enumeration of subgroups of a finite abelian group, *Proc. Amer. Math. Soc.* **101** (1987), 771–775.

[4] P. Hall, A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.*(2) **36** (1933), 29–95.

[5] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.*(2) **40** (1935), 468–501.

[6] M. Suzuki, Group Theory II, Springer–Verlag, New York, 1986.

[7] Y. Takegahara, On the Frobenius numbers of symmetric groups, *J. Algebra*, to appear.

[8] Y. Takegahara, The number of subgroups of a finite group, submitted to *J. Algebra.*

[9] K. Wohlfahrt, Über einen Satz von Dey und die Modulgruppe, *Arch. Math. (Basel)* **29** (1977), 455–457.

[10] T. Yoshida, $|\mathrm{Hom}(A, G)|$, *J. Algebra* **156** (1993), 125–156.