Remark on the multiplicity of a partition of a group into cosets*

by

Marc A. Berger, Alexander Felzenbaum and Aviezri Fraenkel (Rehovot)

1. Abstract. We find a lower bound for the multiplicity of a coset partition of a group. This proves the conjectures of Burshtein and Herzog–Schönheim in a special group setting. Our result applies to finite groups which satisfy a chain condition similar to solvability.

We shall concern ourselves with finite groups G which contain a chain of subgroups

(1) $$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G$$

with

(2) $$[G_{k-1}\colon G_k] = p(|G_{k-1}|), \quad 1 \leqslant k \leqslant n,$$

where $p(m)$ denotes the least prime factor of m. Such groups will be called *pyramidal.* It is well known that the condition (2) implies that $G_k \lhd G_{k-1}$, (e.g. [5, Exer. 3.43]), so (1) is a composition series for G, and G is necessarily solvable. Any supersolvable group is pyramidal. Our main result is

THEOREM. *Assume $K_1, \ldots, K_t$ are subgroups of and $a_1, \ldots, a_t$ elements of a pyramidal group G, such that $(C_i = a_i K_i\colon 1 \leqslant i \leqslant t)$ disjointly partition G. If $t > 1$ then at least*

(3) $$x = \left[\frac{P(l)\varphi(l)}{l}\right] + 1$$

of the K_i have the same order, where

(4) $$l = \frac{|G|}{\text{g.c.d.}(|K_i|\colon 1 \leqslant i \leqslant t)}.$$

Here $P(m)$ denotes the greatest prime factor of m, φ is the Euler totient function and $[\cdot]$ denotes the greatest integer function. Note that $x \geqslant 2$, so this Theorem proves

* Research supported by United States–Israel Binational Science Foundation Grant No. 85-00368 (all three authors).

the conjectures of Burshtein [2] and Herzog–Schönheim [4] for pyramidal groups. In [1] we proved this result for finite nilpotent groups.

The Herzog-Schönheim conjecture asserts that if the cosets $(a_iK_i\colon 1\leqslant i\leqslant t)$, $t>1$, disjointly partition a (finite or infinite) group G then at least two indices $[G\colon K_i]$ coincide. (It is known that these indices are necessarily all finite, and there are examples where the K_i themselves are all distinct. See [4].) The Burshtein conjecture concerns disjoint covering systems of residue classes of integers — equivalently, disjoint coset partitions of cyclic groups — but it readily extends to the general finite group setting. It concerns the case where g.c.d. $(|K_i|\colon 1\leqslant i\leqslant t) = 1$. It states that none of the prime divisors of $|G|$ exceed $q_{\varkappa(M)-1}$, where $2 = q_1, q_2, \ldots$ is the consecutive enumeration of all the primes, M is the largest number of the K_i all having the same order, and

$$\varkappa(M) = \min\Big(k\in N\colon (q_k-1)\prod_{i=1}^{k-1}(1-q_i^{-1})\geqslant M\Big).$$

Thus, for example, $M=1$ is impossible, if $M=2$ then $P(|G|)\leqslant 7$ and if $M=3$ then $P(|G|)\leqslant 13$. See [2] for a brief discussion of this function $\varkappa$. This (extension of the) Burshtein conjecture can be considered a strengthening of the Herzog–Schönheim conjecture for finite groups.

We need several lemmas.

LEMMA I. *Let K, L be subgroups of a finite group G, and let $a, b\in G$. Then $aK\cap bL$ is either empty or a coset of $K\cap L$, in which case*

$$|aK\cap bL| = |K\cap L|. \tag{5}$$

Proof. If $c\in aK\cap bL$ then $aK = cK$, $bL = cL$. Thus $aK\cap bL = cK\cap cL = c(K\cap L)$. ■

LEMMA II. *Let G be a finite group with a subgroup G_1 of index $p(|G|)$. For any subgroup $K\subset G$ and any $a\in G$, either*

$$aK\subset aG_1 \ \text{ or } \ aK\cap bG_1\neq\emptyset, \quad \text{for all } b\in G. \tag{6}$$

Proof. Let aK intersect precisely r distinct left cosets of G_1. By Lemma I

$$|K| = |aK| = r|K\cap G_1|. \tag{7}$$

Thus $r\,\big|\,|G|$. Since $r\leqslant p(|G|)$ we must have $r=1$ or $r = p(|G|)$. ■

LEMMA III. *Every pyramidal group G contains a unique Sylow $P(|G|)$-subgroup (which is therefore normal).*

Proof. We use induction on $|G|$. The case $|G| = 1$ is trivial, so we proceed to the induction step. If G is a p-group then G is its only Sylow subgroup, so we may assume

$$p(|G|)<P(|G|). \tag{8}$$

Let G have the chain (1). By the induction hypothesis G_1, being pyramidal, contains a unique Sylow $P(|G_1|) = P(|G|)$-subgroup S. Since $G_1\lhd G$ and (Sylow's theorem) any two Sylow $P(|G|)$-subgroups are conjugate, it follows that S is the only Sylow $P(|G|)$-subgroup of G. ■

Introduce a measure μ on N through

$$\mu(\{m\}) = \varphi(m). \tag{9}$$

For any nonempty subset $R\subset N$ define

$$D(R) = \{d\in N\colon d\,|\,m \text{ for some } m\in R\}, \tag{10}$$

and set $D(\emptyset) = \emptyset$. Observe that

$$D(R_1\cup R_2) = D(R_1)\cup D(R_2), \tag{11}$$

and

$$R\subset D(R)\subset D(kR) \tag{12}$$

for any $k\in N$. From Gauss's identity ([3, p. 542])

$$\mu\big(D(\{m\})\big) = m \tag{13}$$

one can establish that for any $k\in N$

$$\mu\big(D(kR)\big) = k\mu\big(D(R)\big). \tag{14}$$

LEMMA IV. *Let G be a pyramidal group, let $K_1, \ldots, K_t\subset G$ be subgroups and let $a_1, \ldots, a_t\in G$. Then*

$$\Big|\bigcup_{i=1}^{t} a_iK_i\Big|\geqslant\mu\big(D(R)\big) \tag{15}$$

where

$$R = \{|K_i|\colon 1\leqslant i\leqslant t\}. \tag{16}$$

Proof. We use induction on $|G|$. The case $|G| = 1$ is trivial, so we proceed to the induction step. Let G have the chain (1), and let the distinct left cosets of G be $b_1G_1, \ldots, b_pG_1$ where $p = p(|G|)$. According to Lemma II each set a_iK_i either lies entirely within a single coset b_jG_1, or else intersects all p of them. Let

$$R_0 = \{|K_i|\colon a_iK_i\cap b_jG_1\neq\emptyset, \quad 1\leqslant j\leqslant p\}, \tag{17}$$

$$R_j = \{|K_i|\colon a_iK_i\subset b_jG_1\}, \quad 1\leqslant j\leqslant p. \tag{18}$$

Then

$$R = \bigcup_{j=0}^{p} R_j. \tag{19}$$

Since G_1 is pyramidal we can apply the induction hypothesis to each coset $b_j G_1$, obtaining

$$(20)\quad |\bigcup_{i=1}^{t} a_i K_i| \geqslant \sum_{j=1}^{p} \mu\left(D\left(\frac{1}{p} R_0 \cup R_j\right)\right) = \sum_{j=1}^{p} \mu\left(D\left(\frac{1}{p} R_0\right) \cup D(R_j)\right)$$

$$\geqslant (p-1)\mu\left(D\left(\frac{1}{p} R_0\right)\right) + \mu\left(D\left(\frac{1}{p} R_0\right) \cup \bigcup_{j=1}^{p} D(R_j)\right)$$

$$= p\mu\left(D\left(\frac{1}{p} R_0\right)\right) + \mu\left(\bigcup_{j=1}^{p} D(R_j)\right) - \mu\left(D\left(\frac{1}{p} R_0\right) \cap \bigcup_{j=1}^{p} D(R_j)\right)$$

$$\geqslant p\mu\left(D\left(\frac{1}{p} R_0\right)\right) + \mu\left(\bigcup_{j=1}^{p} D(R_j)\right) - \mu\left(D(R_0) \cap \bigcup_{j=1}^{p} D(R_j)\right).$$

We have used here (11), (12) and elementary properties of measures. Using (11), (14), (19) we now obtain (15). ■

Proof of Theorem: We first make an observation relating to x. If l has the prime factorization

$$(21)\quad l = \prod_{j=1}^{m} p_j^{t_j}, \quad p_1 < \ldots < p_m$$

then

$$(22)\quad y = \frac{P(l)\varphi(l)}{l} = (p_m - 1) \prod_{j=1}^{m-1} (1 - p_j^{-1}).$$

Thus for any $d \in N$ whose prime factors form a subset of $\{p_1, \ldots, p_{m-1}\}$

$$(23)\quad \varphi(d) \geqslant \frac{dy}{p_m - 1}.$$

We use induction on $|G|$. The case $|G| = 2$ is trivial, so we proceed to the induction step. Let $S \subset G$ be a Sylow $P(|G|)$-subgroup, and set

$$(24)\quad I = \{i\colon |S| \mid |K_i|\}.$$

It follows from Lemma III that if $j \notin I$ then

$$(25)\quad S \lhd K_j.$$

In particular $SC_j = C_j$ for $j \notin I$, and we conclude therefore that

$$(26)\quad \bigcup_{i \in I} C_i = \bigcup_{i \in I} SC_i.$$

If $I = \emptyset$ then we can apply the induction hypothesis to G/S. Indeed, according to Lemma III some $G_k = S$, and we have

$$(27)\quad \{1\} = G_k/S \subset G_{k-1}/S \subset \ldots \subset G/S,$$

showing that G/S is pyramidal. According to (25), $(a_i K_i/S\colon 1 \leqslant i \leqslant t)$ forms a coset partition of G/S. Furthermore the number l given by (4) does not change, since everything is divisible by $|S|$.

Assume then that $I \neq \emptyset$. This ensures that

$$(28)\quad P(|G|) = P(l) = p_m.$$

Let $H \subset G$ be a p_m-complement. (Its existence is ensured by Hall's Theorem since G is solvable.) Then G is the semidirect product of S by H (see [4, p. 136]), and

(i) $|SX| = |S|\,|SX \cap H|$ for any subset $X \subset G$.

(ii) $|H| = |S \cap X|\,|SX \cap H|$ for any subset $X \subset G$ with $S \cap X \neq \emptyset$.

Using (i), we obtain

$$(29)\quad |\bigcup_{i \in I} SC_i| = |S|\,|\bigcup_{i \in I} (SC_i \cap H)|.$$

Since $S \lhd G$ each $SC_i \cap H$ is a coset in H of the subgroup $SK_i \cap H$. So according to Lemma IV

$$(30)\quad |\bigcup_{I \in i} (SC_i \cap H)| \geqslant \mu(D(R))$$

where

$$(31)\quad R = \{|SK_i \cap H|\colon i \in I\}.$$

Each subgroup K_i has cardinality (using (ii) above)

$$(32)\quad |K_i| = p_m^k |SK_i \cap H|$$

for some $k \geqslant 0$, $p_m^k < |S|$. The prime divisors of $|SK_i \cap H|$ form a subset of $\{p_1, \ldots, p_{m-1}\}$, and so (23) applies to each $d \in R$. If the conclusion of the Theorem were false then no more than y subgroups K_i could have the same cardinality. It would then follow from (12), (23), (28), (32) that

$$(33)\quad \sum_{i \in I} |K_i| \leqslant y\left(1 + p_m + \ldots + \frac{|S|}{p_m}\right) \sum_{d \in R} d$$

$$= y\,\frac{|S| - 1}{p_m - 1} \sum_{d \in R} d \leqslant (|S| - 1) \sum_{d \in R} \varphi(d)$$

$$= (|S| - 1)\mu(R) \leqslant (|S| - 1)\mu(D(R)).$$

Together (26), (29), (30), (33) form a contradiction. ■

References

[1] M. A. Berger, A. Felzenbaum and A. S. Fraenkel, *The Herzog-Schönheim conjecture for finite nilpotent groups*, Canad. Math. Bull. 29 (3) (1986), 329–333.

[2] N. Burshtein, *On natural exactly covering systems of congruences having moduli occurring at most M times*, Discrete Math. 14 (1976), 205–214.

[3] G. Chrystal, *Textbook of Algebra, Part Two*, Dover, New York 1961.
[4] M. Herzog and J. Schönheim, *Research problem No. 9*, Canad. Math. Bull. 17 (1974), 150.
[5] J. J. Rotman, *The Theory of Groups*, Allyn and Bacon, Boston 1973.

DEPARTMENT OF MATHEMATICS
THE WEIZMANN INSTITUTE OF SCIENCE
Rehovot 76 100, Israel

Received 30 January 1985;
in revised form 2 May 1985

Forcing smooth square roots and integration

by

I. Moerdijk (Amsterdam), Ngo van Quê and G. E. Reyes (Montreal)

Abstract. This paper is concerned with models of Synthetic Differential Geometry (SDG, cf. Introduction).

We give affirmative answers to the following questions:

1) Is the existence of square roots of nonnegative (smooth) reals compatible with the axioms of SDG?

2) Does the integration axioms ("every functions from [0, 1] into R has a unique primitive vanishing at 0") hold in the generic (local) Archemedean C^∞-ring?

Introduction. This paper is a contribution to the study of models of Synthetic Differential Geometry (SDG). The aim of this theory is to give an intrinsic, naïve axiomatization of Differential Geometry as a foundation for the synthetic reasoning used by people like Darboux, Lie, Cartan (as well as physicists and engineers) in this field. Its basic notions are those of a commutative ring with 1, R ("the (smooth) reals") and its subset D of elements of square 0 ("infinitesimals of first order"). The basic assumption, the Kock-Lawvere axiom, asserts that D is large enough to make the map $\alpha\colon R\times R \to R^D$ invertible, where $\alpha(a, b)(h) = a+bh$, $\forall h \in D$. ("In the infinitely small, any curve is a line").

Since this axiom is incompatible with classical logic, no set-theoretical models exist for this theory. On the other hand, several topos-theoretical models have been constructed, showing the compatibility of SDG with intuitionistic logic. Many of these will be described in this paper.

Further developments of SDG require, naturally, more axioms on R. We shall assume that R is a local ring equipped with order relations $<$ and $\leqslant$ which are compatible with the ring structure and with each other i.e. we assume the following

Axioms (*):

$\neg 0 = 1$,

$\forall x \in R(x \text{ invertible} \vee (1-x) \text{ invertible})$,

$0 < 1$,

$\forall x, y \in R(0 < x \wedge 0 < y \to 0 < x+y \wedge 0 < x\cdot y)$,

$0 \leqslant 1$,