BOOLEAN POWERS OF SIMPLE GROUPS

B. H. NEUMANN and SADAYUKI YAMAMURO

(Received 12 August 1964)

We prove that factor groups of cartesian powers of finite non-abelian simple groups cannot be countably infinite. This is not our main result, but it had been our original aim. The proof is based on a similar fact concerning σ-complete Boolean algebras, and on a representation of certain subcartesian powers of a group in its group ring over a Boolean ring. This representation, to which we give the name "Boolean power", will be our central theme, and we begin with it.

1. Boolean powers

Let G be a group (with unit element e) and R a Boolean ring (with unit element 1). In the group ring of G over R we consider those finite sums

$$p = \sum \rho_a a \quad (\rho_a \in R, a \in G)$$

that satisfy

$$\rho_a \rho_b = 0 \quad \text{if} \quad a \neq b, \quad \sum \rho_a = 1.$$

They form a group, which we call a *Boolean power* [1] of G and denote by

$$P = \mathrm{BP}(G, R).$$

It is generated by the elements $\rho a + (1-\rho)e$, with ρ and a ranging over R and G, respectively; for fixed ρ these elements form an isomorphic copy of G, which in the special case $\rho = 1$ is called the *diagonal* of P. We define the *support* of $p \in P$ by

$$\sigma(p) = \sum_{a \neq e} \rho_a = 1 - \rho_e.$$

Instead of Boolean rings we could have used arbitrary rings, and we have allowed for this by writing $1-\rho$ for $1+\rho$; but the resulting gain in generality is illusory.

A more important generalization is obtained if G and R are infinite and infinite sums $\sum \rho_a a$ are admitted; this requires that the Boolean ring be complete, or at least $\mathfrak{m}$-complete [2] if sums with $\mathfrak{m}$ terms are to be given a

[1] See addendum at end.

[2] Our notation is that of Sikorski [4].

meaning. The group so obtained will be called an $\mathfrak{m}$-complete Boolean power, and denoted by

$$P^* = \mathrm{BP}^*(G, R);$$

the cardinal $\mathfrak{m}$ will usually be the order $|G|$ of G, unless differently specified.

An important illustration is provided by $R^* = \mathrm{GF}(2)^I$, where I is an arbitrary index set; thus R^* is the Boolean ring that corresponds to the Boolean algebra $\mathscr{P}(I)$ of all subsets of I. As R^* is complete, we can form P^*, whatever the group G; and P^* is isomorphic to the cartesian power G^I. If G or I is finite, then P^* and P coincide; but if G and I are both infinite, then P is a proper subgroup of P^*, namely that which in the natural isomorphism between P^* and G^I corresponds to the "bounded" subgroup of G^I, consisting of those functions on I to G that take only finitely many values.

The Boolean powers $\mathrm{BP}(G, R)$ will be called *finitary* if it is necessary to distinguish them from complete or $\mathfrak{m}$-complete ones. We shall concentrate mainly on the finitary Boolean powers, and treat the others only sketchily.

A representation, similar to ours, of the normal subgroups of G^I that correspond to ideals of R^* has been studied by Teh [5].

2. Ideals and normal subgroups

If φ is a homomorphism of the Boolean ring R into a Boolean ring S such that φ maps $1 \in R$ on $1 \in S$, then φ induces a homomorphism ψ of $P = \mathrm{BP}(G, R)$ into $Q = \mathrm{BP}(G, S)$ by

$$(\sum \rho_a a)\psi = \sum (\rho_a \varphi) a. \tag{1}$$

Let J denote the kernel of φ and N the kernel of ψ. Then

$$N = \{p \in P \mid \sigma(p) \in J\}; \tag{2}$$

thus to every ideal J of R there corresponds a normal subgroup

$$N = J\nu \tag{3}$$

of P; and ν then maps the lattice $\mathfrak{J}$ of all ideals of R into the lattice $\mathfrak{N}$ of all normal subgroups of P. In fact ν is a lattice monomorphism, as can be easily verified; but ν is not in general an epimorphism.

If R is $\mathfrak{m}$-complete and the $\mathfrak{m}$-complete Boolean power $P^* = \mathrm{BP}^*(G, R)$ is considered, the analogue of equation (1) may be devoid of meaning, unless S is also $\mathfrak{m}$-complete; but in analogy to (2), (3) we can define a mapping ν^* by

$$N^* = J\nu^* = \{p \in P^* \mid \sigma(p) \in J\};$$

and N^* will be a normal subgroup of P^*. It is again easy to verify that ν^*

is a lattice monomorphism of $\mathfrak{J}$ into the lattice $\mathfrak{N}^*$ of all normal subgroups of P^*.

Next let N be a normal subgroup of $P = \mathrm{BP}(G, R)$ and put

$$J = N\mu = \{\sigma(p) | p \in N\}. \tag{4}$$

Then J will be subset of R, but not in general an ideal.

LEMMA 1. *If the centre of G is trivial then $J = N\mu$ is an ideal of R; in this case, for all ideals J of R,*

$$J\nu\mu = J,$$

and for all normal subgroups N of P,

$$N \leqq N\mu\nu.$$

PROOF. Let $\sigma, \tau \in J = N\mu$ and $\rho \in R$. We have to show that $\sigma+\tau \in J$ and $\sigma\rho \in J$. We begin with the latter. There is an element

$$p = \sum \rho_a a \in N$$

such that $\sigma(p) = \sigma$. To each $a \neq e$ that occurs with coefficient $\rho_a \neq 0$ in p, we choose an element $b(a) \in G$ that does not commute with a: this is possible because the centre of G is assumed trivial. Put

$$r = \sum_{a \neq e} \rho_a \rho b(a) + (1-\sigma\rho)e;$$

it is easy to verify that $r \in P$. Also the commutator $[p, r]$ is given by

$$[p, r] = \sum_{a \neq e} \rho_a \rho [a, b(a)] + (1-\sigma\rho)e;$$

this is an element of N because N is normal; and $\sigma([p, r]) = \sigma\rho$; hence $\sigma\rho \in J$. It now follows that both $\sigma_1 = \sigma(1-\tau)$ and $\tau_1 = (1+\sigma)\tau$ belong to J; thus there are elements $p_1, q_1 \in N$ with $\sigma(p_1) = \sigma_1$, $\sigma(q_1) = \tau_1$. Then also $p_1 q_1 \in N$. One readily verifies that $\sigma_1\tau_1 = 0$ and that, therefore,

$$\sigma(p_1 q_1) = \sigma_1 + \tau_1 = \sigma + \tau.$$

Hence also $\sigma+\tau \in J$, and J is an ideal, as claimed. The relations $J\nu\mu = J$ and $N \leqq N\mu\nu$ follow at once from the definitions, and the lemma is proved.

If G has trivial centre, then μ maps the lattice $\mathfrak{N}$ of normal subgroups of P onto the lattice $\mathfrak{J}$ of ideals of R: but μ is in general neither a homomorphism nor one-to-one.

If the $\mathfrak{m}$-complete Boolean power $P^* = \mathrm{BP}^*(G, R)$ is defined, one can use (4) to define a mapping μ^* from the lattice $\mathfrak{N}^*$ of normal subgroups of P^* to $\mathfrak{J}$, provided that G has trivial centre; and again

$$J\nu^*\mu^* = J$$

for all $J \in \mathfrak{J}$, and

$$N^* \leqq N^*\mu^*\nu^*$$

for all $N^* \in \mathfrak{N}^*$. We omit the proof.

3. The main result

We now investigate when μ and ν can be mutually inverse isomorphisms. Leaving aside the trivial cases that G or R have a single element only, we see at once that this can be the case only if G is a non-abelian simple group. Our main result is that this obviously necessary condition is also sufficient.

LEMMA 2. *Let G be a non-abelian simple group; then to every pair of elements a, b of G with $a \neq e$ there is a positive integer n and a sequence of $2n$ elements $c_1, d_1, c_2, d_2, \cdots, c_n, d_n$ of G such that*

$$c_1^{-1}a^{-1}c_1d_1^{-1}adc_2^{-1}a^{-1}c_2 \cdots d_n^{-1}ad_n = b.$$

PROOF. If F denotes the set of all

$$f(c, d) = c^{-1}a^{-1}cd^{-1}ad$$

as c, d range over G, then F is clearly self-conjugate in G and self-inverse, and contains the unit element e but not only e. Hence

$$F \subseteqq F^2 \subseteqq F^3 \subseteqq \cdots \text{ and } \bigcup F^n = G,$$

as G is simple; thus there is an integer n such that $b \in F^n$, and the lemma follows.

We remark that if G is finite, then n can be taken equal to the order of G, whatever the pair a, b; and probably much smaller. On the other hand, one can also choose n arbitrarily larger than necessary by adding factors $f(e, e) = e$ *ad libitum*. Thus we obtain the following apparent extension of Lemma 2, which is what will in fact be used later.

COROLLARY 3. *Let A, B be finite subsets of the non-abelian simple group G, and assume $e \notin A$. Then there is a positive integer n and a family of elements $c_i(a, b)$, $d_i(a, b)$ with $i = 1, 2, \cdots, n$ and $a \in A$, $b \in B$ such that, for all such a and b,*

$$\prod_{i=1}^{n} c_i(a, b)^{-1}a^{-1}c_i(a, b)d_i(a, b)^{-1}ad_i(a, b) = b.$$

One only needs to choose n large enough to suffice for all pairs $a \in A$, $b \in B$ simultaneously.

LEMMA 4. *Let G be a non-abelian simple group, R a Boolean ring, and*

$$p = \sum \rho_a a, \quad q = \sum \sigma_a a$$

https://doi.org/10.1017/S1446788700027749 Published online by Cambridge University Press

two elements of $P = \mathrm{BP}(G, R)$. *Then* q *lies in the normal closure* N_p *of* p *in* P *if, and only if,*

$$\rho_e \sigma(q) = 0.$$

PROOF. The annihilator of ρ_e in R,

$$J = \{\sigma \in R \mid \rho_e \sigma = 0\},$$

is an ideal of R, and the corresponding normal subgroup of P is

$$Jv = N = \{q \in P \mid \rho_e \sigma(q) = 0\}.$$

We have to show that $N = N_p$. As $p \in N$, clearly $N_p \leqq N$, and only the reverse inclusion remains to be proved. Let $q \in N$. Put

$$A = \{a \in G \mid a \neq e \text{ and } \rho_a \neq 0\}; \quad B = \{b \in G \mid \sigma_b \neq 0\}.$$

These are finite subsets of G, and $e \notin A$. Thus we can apply Corollary 3 and find n and $c_i(a, b)$, $d_i(a, b)$ accordingly. Put, for $i = 1, 2, \cdots, n$,

$$s_i = \sum_{(a,b) \neq (e,b)} \rho_a \sigma_b c_i(a, b) + \rho_e e,$$

$$t_i = \sum_{(a,b) \neq (e,b)} \rho_a \sigma_b d_i(a, b) + \rho_e e.$$

The coefficient in s_i of an element $c \in G$ is 0 or a sum of products $\rho_a \sigma_b$, with an additional ρ_e if $c = e$. These products are mutually orthogonal, and orthogonal to ρ_e; hence the coefficients of different elements $c \in G$ in s_i are orthogonal. Their sum is

$$\sum_{(a,b) \neq (e,b)} \rho_a \sigma_b + \rho_e = \sum_{a \neq e} \rho_a \sum_b \sigma_b + \rho_e = \sum_{a \neq e} \rho_a + \rho_e = 1.$$

Thus $s_i \in P$, and similarly $t_i \in P$. By a tedious, but not difficult computation, which we omit, one verifies that

$$\prod_{i=1}^{n} s_i^{-1} p^{-1} s_i t_i^{-1} p t_i = \sum_{(a,b) \neq (e,b)} \rho_a \sigma_b b + \rho_e e. \tag{5}$$

As $q \in N$ and thus $\rho_e \sigma_b = 0$, the coefficient of an element $b \neq e$ in (5) is

$$\sum_{a \neq e} \rho_a \sigma_b = \sum_{a \neq e} \rho_a \sigma_b + \rho_e \sigma_b = \sigma_b;$$

but then the coefficient of e must be σ_e, as we know that the coefficients are mutually orthogonal and add up to 1. Hence

$$\sum_{(a,b) \neq (e,b)} \rho_a \sigma_b b + \rho_e e = \sum_b \sigma_b b = q,$$

and thus $q \in N_p$. This completes the proof of the lemma.

We are now ready to prove our main result.

THEOREM 5. *Let G be a non-abelian simple group and R a Boolean ring. Then $\nu : \mathfrak{J} \to \mathfrak{N}$ and $\mu : \mathfrak{N} \to \mathfrak{J}$ are mutually inverse lattice isomorphisms between the lattices of ideals of R and of normal subgroups of the Boolean power* $\mathrm{BP}(G, R)$.

PROOF. It suffices, by Lemma 1, to show that $N\mu\nu \leqq N$ for every $N \in \mathfrak{N}$. Let then $q \in N\mu\nu$; then $\sigma(q) \in N\mu$, that is to say, there is an element $p \in N$ such that $\sigma(q) = \sigma(p)$. By Lemma 4 then $q \in N_p \leqq N$, and it follows that $N\mu\nu \leqq N$, as required. This completes the proof of the theorem.

COROLLARY 6. *If G is a non-abelian simple group then every epimorphic image of a Boolean power of G is again a Boolean power of G. Specifically, if R is a Boolean ring, $P = \mathrm{BP}(G, R)$ the Boolean power of G, and $\psi : P \to Q$ an epimorphism, then there is an epimorphism $\varphi : R \to S$ such that* $Q \cong \mathrm{BP}(G, S)$.

4. A result on Boolean rings

We now turn to the Boolean rings themselves; the following theorem naturally applies to Boolean algebras, too.[3]

THEOREM 7. *The epimorphic images of σ-complete Boolean rings are finite or uncountable.*

Sikorski ([4], § 20 E) remarks that σ-complete Boolean algebras are themselves finite or uncountable; and he bases this on the fact that every infinite Boolean algebra contains an infinite set of disjoint elements. As we need this — apparently well-known — fact, too, but know of no convenient reference to its proof, we sketch our proof of it, or rather of its ring counterpart.

LEMMA 8. *Every infinite Boolean ring contains an infinite set of mutually orthogonal elements.*

PROOF. Let R be an infinite Boolean ring. If R contains infinitely many prime elements, say $\pi_1, \pi_2, \pi_3, \cdots$, then $1+\pi_1, 1+\pi_2, 1+\pi_3, \cdots$ are infinitely many mutually orthogonal elements. If R has only a finite set of prime elements, let their product be π; then $\pi \neq 0$, as R is infinite; and $1+\pi$ has no prime divisors. We can then form an infinite sequence

$$1+\pi = \rho_1, \rho_2, \rho_3, \cdots$$

of elements of R, each a proper factor of its predecessors, so that for all $i, k > 0$

$$\rho_i \neq \rho_{i+k} \quad \text{and} \quad \rho_i = \rho_i \rho_{i+k}.$$

[3] See addendum at end.

Then $\rho_1+\rho_2, \rho_2+\rho_3, \rho_3+\rho_4, \cdots$ form an infinite set of mutually orthogonal elements, and the lemma follows.

We turn to the proof of Theorem 7. Let R be a σ-complete Boolean ring and $\varphi : R \to S$ an epimorphism. We may assume that S is infinite, and have to prove it uncountable. Let $\sigma_1, \sigma_2, \sigma_3, \cdots$ be a sequence of (non-zero) mutually orthogonal elements of S, and let $\rho_1', \rho_2', \rho_3', \cdots$ be counter-images in R: thus

$$\rho_i'\varphi = \sigma_i \qquad (i = 1, 2, 3, \cdots).$$

Put $\rho_1 = \rho_1'$, and inductively

$$\rho_{i+1} = \rho_{i+1}'(1+\rho_1+\rho_2+\cdots+\rho_i).$$

Then $\rho_1, \rho_2, \rho_3, \cdots$ form a sequence of mutually orthogonal elements of R, and

$$\rho_i\varphi = \sigma_i \qquad (i = 1, 2, 3, \cdots).$$

If K is a set of positive integers, put

$$\rho_K = \sum_{i \in K} \rho_i;$$

this exists because R is σ-complete. Then using the distributive law which is the ring analogue of that of Sikorski ([4], § 19 (9)), we have

$$\rho_i\rho_K = \rho_i \quad \text{if} \quad i \in K,$$
$$\rho_i\rho_K = 0 \quad \text{if} \quad i \notin K.$$

Thus, putting $\rho_K\varphi = \sigma_K$ and applying φ, we get

$$\sigma_i\sigma_K = \sigma_i \quad \text{if} \quad i \in K,$$
$$\sigma_i\sigma_K = 0 \quad \text{if} \quad i \notin K.$$

This shows that if K and L are distinct sets of positive integers, then σ_K and σ_L are distinct elements of S, and it follows that S is uncountable. This completes the proof of the theorem.

COROLLARY 9. *Let G be a finite non-abelian simple group, and let R be a σ-complete Boolean ring. Then every epimorphic image of $P = \mathrm{BP}(G, R)$ is either finite or uncountable. In particular the factor groups of cartesian powers G^I are finite or uncountable.*

5. A counterexample

Our main result, Theorem 5, deals with finitary Boolean powers only; the finiteness conditions enter the proof through Corollary 3 and so through the crucial Lemma 4. To show that these finiteness conditions are not just

an accident of the proof method, but an essential feature of the situation, we show that the analogue of Theorem 5 for $\mathrm{BP}^*(G, R)$ and μ^* and ν^* is not in general valid. To do this we specify an infinite simple group G and a normal subgroup N^* of $P^* = \mathrm{BP}^*(G, R)$, where R is an arbitrary infinite σ-complete Boolean ring, such that

$$N^* \neq N^*\mu^*\nu^*.$$

Let G be the finitary alternating group on $Z = \{1, 2, 3, \cdots\}$, that is the group of even permutations of Z that move only finitely many elements of Z; this group is well known to be simple. The Boolean ring R is to be infinite and σ-complete, but otherwise arbitrary; in $P^* = \mathrm{BP}^*(G, R)$ we consider the diagonal D, which consists of all elements $1a$ with $a \in G$; denote its normal closure in P^* by N^*. By the extension of Lemma 1 mentioned at the end of § 2 then $N^*\mu^* = R$, and so $N^*\mu^*\nu^* = P^*$. We have to show that

$$N^* \neq P^*. \tag{6}$$

Let us first remark that the normal closure of D in $P = \mathrm{BP}(G, R)$ is the whole of P, by Lemma 4; hence $P \leqq N^*$. However, as we shall see later, also

$$P \neq N^*. \tag{7}$$

We define the *degree* $\delta(a)$ of a permutation $a \in G$ to be the number of elements of Z that are actually moved by a. The definition of G implies that this is always finite. Next, if $p = \sum \rho_a a$, we define the *bound* $\beta(p)$ by

$$\beta(p) = \text{l.u.b. } \{\delta(a) \mid \rho_a \neq 0\}.$$

This is clearly finite for all $p \in P$, but infinite for some $p^* \in P^*$; for if we choose a sequence $a_1, a_2, a_3, \cdots$ of elements of G of strictly increasing degrees and a sequence $\rho_1, \rho_2, \rho_3, \cdots$ of mutually orthogonal non-zero elements of R, and then put

$$p^* = \sum \rho_i a_i + (1 - \sum \rho_i)e,$$

then clearly $\beta(p^*) = \infty$. On the other hand, there are also elements with finite bound in $P^* - P$: we only have to take $a_1, a_2, a_3, \cdots$ to be distinct transpositions, and form the same sum p^*: then $\beta(p^*) = 2$. Hence (6) and (7) will follow from:

LEMMA 10. *N^* consists precisely of the elements $p \in P^*$ with finite bound $\beta(p)$.*

PROOF. Firstly let $p = \sum \rho_a a$ have finite bound $\beta(p)$. To each element $a \in G$ we can choose an element $b(a)$ such that $a' = b(a)^{-1}ab(a)$ moves only the numbers $1, 2, \cdots, \delta(a)$ and leaves the rest of Z fixed. Put

$$t = \sum \rho_a b(a);$$

then

$$p' = t^{-1}pt = \sum \rho_a a'.$$

Now each a' moves $1, 2, \cdots, \beta(p)$ at most, and leaves the rest of Z fixed; hence there are only finitely many distinct a', and it follows that $p' \in P$. Thus every element with finite bound is conjugate to an element of P. As we have already remarked that $P \leqq N^*$, this shows that every element with finite bound lies in N^*, and also that $P \neq N^*$. Next we remark that

$$\beta(p^{-1}) = \beta(p) \quad \text{and} \quad \beta(pq) \leqq \beta(p)+\beta(q),$$

so that the elements with finite bound form a subgroup: this follows from the obvious relations

$$\delta(a^{-1}) = \delta(a) \quad \text{and} \quad \delta(ab) \leqq \delta(a)+\delta(b).$$

Finally, using the equally obvious relation

$$\delta(b^{-1}ab) = \delta(a),$$

one readily verifies that

$$\beta(t^{-1}pt) = \beta(p);$$

here a, b range over G and p, t over P^*. It follows that the set of elements with finite bounds is self-conjugate in P^*; thus it must coincide with N^*, and the lemma is proved.

Finally we remark that there are infinite simple groups for which the analogue of Theorem 5 for complete Boolean powers and μ^* and ν^* is valid: examples are the algebraically closed groups of Scott [3], the group C of P. Hall [1], and the infinite groups with only two classes of conjugate elements [2]; for in all these groups the number n of Lemma 2 does not have to depend on the pair a, b — in fact in all these groups $n = 1$ will do —, so that in these groups a strengthened form of Corollary 3, for infinite sets A and B and still with $n = 1$, is valid.

Addendum (19 February, 1965). Aspirant I. E. Burmistrovič, of the Department of Higher Algebra, Moscow State University, has kindly drawn our attention to some pertinent references. The definition of Boolean powers, not just of groups, but of arbitrarily general algebraic systems, is to be found in Foster [0]. Our Theorem 7 is Theorem 4.4 of Smith and Tarski [4½].

References

[0] Alfred L. Foster, Functional completeness in the small. *Math. Ann.* **143**, 29—58 (1961).
[1] P. Hall, Some constructions for locally finite groups. *J. London Math. Soc.* **34**, 305—319 (1959).

[2] Graham Higman, B. H. Neumann, and Hanna Neumann, Embedding theorems for groups. *J. London Math. Soc.* **24**, 247–254 (1949).
[3] W. R. Scott, Algebraically closed groups. *Proc. Amer., Math. Soc.* **2**, 118–121 (1951).
[4] Roman Sikorski, *Boolean algebras*. Springer-Verlag, Berlin-Göttingen-Heidelberg 1960.
[4½] E. C. Smith, Jr, and Alfred Tarski, Higher degrees of distributivity and completeness in Boolean algebras. *Trans. Amer. Math. Soc.* **84**, 230–257 (1957).
[5] H. H. Teh, On ideal coverings of a set and some directed products of groups. *Bull. Math. Soc. Nanyang Univ.* 1962, 1–7.

The Australian National University
Canberra