RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

ZVI ARAD
GIDEON EHRLICH
OTTO H. KEGEL
JOHN C. LENNOX

An application of Ramsey's theory to partitions in groups - I

Rendiconti del Seminario Matematico della Università di Padova, tome 84 (1990), p. 143-157

<http://www.numdam.org/item?id=RSMUP_1990__84__143_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 84 (1990)

An Application of Ramsey's Theory to Partitions in Groups - I.

ZVI ARAD - GIDEON EHRLICH - OTTO H. KEGEL - JOHN C. LENNOX (*)

1. Introduction.

Ramsey theory is a branch of combinatorics which deals with structures which are preserved under partitions, for background details see [3]. The ideas and techniques of Ramsey theory have found broad applications in set theory, probability theory, analysis, and even theoretical computer science. Our aim in this paper is to take one of the earliest results of « Ramsey type » and apply it in group theory.

In 1916, in connection with his work on the Fermat Conjecture, I. Schur [9] proved the following result:

THEOREM. In every finite colouring of the positive integers $\mathbb{N}$ there exists a monochrome solution to the equation $x + y = z$.

For interest's sake we mention that 1927 van der Waerden [11] answered a conjecture of Schur [10] by proving a related result on subsets of $\mathbb{N}$:

(*) Indirizzo degli AA.: Z. ARAD and G. EHRLICH: Department of Mathematics and Computer Science, Bar-Ilan University, Ramat-Gan, Israel; O. H. KEGEL: Mathematisches Institut, Albert-Ludwigs-Universität, D-7800 Freiburg i. Br., West Germany; J. C. LENNOX: Department of Pure Mathematics, University College Cardiff, Cardiff CF1 1XL, England.

The work on this paper was supported by a grant of the German-Israeli Foundation.

THEOREM. If N is partitioned into finitely many subsets, then at least one of these subsets contains arbitrarily long arithmetic progressions.

This, of course, means that if N is 2-coloured, then there is a monochrome solution to the equation $x + y = z$. Both of these theorems have been generalised in [3].

Our objective here is to prove a version of Schur's Theorem for arbitrary groups. We treat the case of infinite and finite groups separately.

THEOREM A. For any n-colouring of an infinite group there exists a monochrome solution to the equation $xy = z$, where x, y, and z are distinct non-identity elements.

THEOREM B. For any n-colouring of a finite group of order at least $R(2, 8, (n^2 - n)/2) + 1$ there exists a monochrome solution to the equation $xy = z$, where x, y, and z are distinct non-identity elements.

The numbers $R(a, b, c)$ appearing here are the Ramsey numbers (see [3] and below). They are extremely large—in fact they have not yet been computed. (However, see [8] for another approach to such numbers.)

In the special cases $n = 2$ and $n = 3$ we use Theorem A to prove.

THEOREM C. *a*) If G is a 2-coloured group of order greater than 7 which is not elementary abelian of order 9 then there is a monochrome solution of the equation $xy = z$, where x, y, and z are distinct non-identity elements.

b) If G is a 3-coloured group of order 17 or greater than 18 then there is a monochrome solution of the equation $xy = z$, where x, y, and z are distinct non-identity elements.

The bounds on the group orders appearing in Theorems B and C will become smaller if we do not require the elements x, y, and z to be distinct. Indeed, if $f(t)$ denotes the largest n such that $[n] := \{1, 2, \ldots, n\} \subset \mathbb{N}$ can be t-coloured in such a way that there is no monochrome solution to the equation $x + y = z$, then according to ([5], p. 88) one has $f(1) = 1$, $f(2) = 4$, $f(3) = 13$, $f(4) = 44$. The evaluation of $f(5)$ appears to be a difficult combinatorial problem [5]. If $f^*(t)$ is defined in the same way as $f(t)$, except that we insist that

there be no monochrome solution to $x + y = z$ for distinct x, y, and z, then $f^*(1) = 2$, $f^*(2) = 8$, $f^*(3) = 23$.

PROOFS OF THEOREM A AND B. Ramsey's Theorem states that for every infinite set S, for every pair k, r of natural numbers, and for every partition (colouring) $\chi: \begin{bmatrix} S \\ k \end{bmatrix} \to [r]$ of the set $\begin{bmatrix} S \\ k \end{bmatrix}$ of all (unordered) k-element subsets of S into r (disjoint) subsets $C_i := := \chi^{-1}(i)$, $i = 1, \ldots, r$, there exists an infinite subset T of S such that all the k-element subsets of T belong to the same C_i.

The compactness theorem yields a remarkable finite version of Ramsey's

THEOREM. There exists a (smallest) natural number $R(k, l, r)$ such that for every finite set S with at least $R(k, l, r)$ elements and any partition $\chi: \begin{bmatrix} S \\ k \end{bmatrix} \to [r]$ of the set of k-element subsets of S into r subsets C_i, $i = 1, \ldots, r$, there exists a subset T of S containing at least l elements and such that $\begin{bmatrix} T \\ k \end{bmatrix} \subseteq C_i$ for some $i \in [r]$.

Let S_n denote the commutative partial semigroup on the set $[n] := \{1, 2, \ldots, n\} \subseteq (\mathbb{N}, +)$ defined by the restriction of the usual addition of natural numbers to $[n]$: The sum $a + b$ is defined for $a, b \in S_n$ if and only if $a + b \in [n]$. Essentially Schur's proof now yields

THEOREM 1. If the natural number n is at least as large as $R(2, 4, r)$, then for every partition $\chi: \begin{bmatrix} S_n \\ 1 \end{bmatrix} \to [r]$ of S_n into r (disjoint) subsets C_i, $i = 1, \ldots, r$, there exist two distinct elements $a, b \in S_n$ such that a, b, and $a + b$ belong to some subset C_i of S_n.

PROOF. Define a partition χ^* of $\begin{bmatrix} S_n \\ 2 \end{bmatrix}$ into r subsets by $\chi^*(x, y) = = \chi(|x - y|)$. By the finite version of Ramsey's Theorem and the choice of $n \geqslant R(2, 4, r)$ there exists a 4-element subset $T = \{w, x, y, z\}$, $w < x < y < z$, of S_n such that $\chi^*(g, h) = i$ for some $i \in [r]$ and all $g, h \in T$ with $g \neq h$. But that means $\chi(x - w) = \chi(y - x) = \chi(y - w)$, and $y - w = (x - w) + (y - x) \in S_n$.

Putting $a = (x - w)$ and $b = (y - x)$ we shall have proved our assertion if $a \neq b$. But if $(x - w) = (y - x)$, put $a = (x - w)$ and $b = (z - x)$ to prove the theorem. □

REMARK. If the set $[n]$ is embedded in such a way into a commutative (and additively written) partial semigroup S that the addition of S induces on $[n]$ an addition that extends that of S_n, then —if $n \geqslant R(2, 4, r)$—for every partition of S into r subsets one has the statement of the theorem for S (actually, for the restriction of S to $[n]$). An important example of this sort of embedding will be the natural map of $[n]$ into the cyclic group $C_m \cong Z/mZ$, where m is any integer $m \geqslant n$.

The order of the element s of the partial semigroup S is the smallest natural number n such that either s^{n+1} is not defined or $s^{n+1} = s^m$ for some m with $1 \leqslant m \leqslant n$. If no such n exists s has infinite order. The partial semigroup S is called periodic if every element of S is of finite order. With this definition one has the following consequence of the theorem and the remark:

COROLLARY. If the partial semigroup S admits a partition into r subsets C_i, $i = 1, \ldots, r$, such that for none of these subsets C_i the product of any two distinct elements of C_i is again in C_i, then S is periodic and the order of every element of S is bounded by $R(2, 4, r)$.

PROOF. For $s \in S$ assume that the elements $s, s^2, \ldots, s^n$ are all defined and pairwise distinct, then there is an injection of the partial semigroup S_n into the partial subsemigroup $\langle s \rangle$ of S generated by s, such that $1 \to s$. If now $n > R(2, 4, r)$ the remark yields a contradiction to the assumption. Hence one has of necessity $n \leqq R(2, 4, r)$.

In the same vein as Theorem 1 we now prove

THEOREM 2. Let G be any group with at least

$$R(2, 8, (r^2 - r)2^{-1}) + 1$$

elements. For every partition $\chi: G^{\times\times} \to [r]$ of $G^{\times\times} = G \setminus \{1\}$ into r pairwise disjoint subsets $C_i = \chi^{-1}(i)$, $i \in [r]$, there is at least one such subset C_i of G containing two distinct elements a, b as well as their product ab.

PROOF. Starting from the partition χ of $G^{\times\times}$ define a partition χ^* of $\begin{bmatrix} G \\ 2 \end{bmatrix}$ into $(r^2 - r)/2$ subsets by

$$\chi^*(g, h) = (\chi(gh^{-1}), \chi(hg^{-1})) .$$

The group G is chosen large enough to apply the finite version of Ramsey's Theorem: There exists an 8-element subset T of $G^{\times\times}$ such that χ^* restricts to a constant function on $\begin{bmatrix} T \\ 2 \end{bmatrix}$, i.e. χ^* associates with every pair of distinct elements of T the same pair of numbers from $[r]$, $(1, 1')$, say. Let v be any element of T; then there exist at least four further elements $w, x, y, z \in T$ such that $\chi(vw^{-1}) = \chi(vx^{-1}) = \chi(vy^{-1}) = \chi(vz^{-1})$ $(= 1$, say). Assume, without loss of generality, that also $\chi(wx^{-1}) = 1$; then one has $(vw^{-1})(wx^{-1}) = vx^{-1}$, and the two factors on the left have the desired property, unless $vw^{-1} = wx^{-1}$.

Thus we may assume that among the quotients gh^{-1} of distinct elements in T there are no two having the desired property: For every such triple $f, g, h \in T$ with $\chi(fg^{-1}) = \chi(gh^{-1})$ the equation

$$(fg^{-1})(gh^{-1}) = fh^{-1} \quad \text{entails } fg^{-1} = gh^{-1} .$$

Consider the case $\chi(wy^{-1}) = 1$. Then $(vw^{-1})(wy^{-1}) = vy^{-1}$, so that $vw^{-1} = wy^{-1}$. But this leads to $wx^{-1} = wy^{-1}$ and $x = y$, a contradiction. So one must have $\chi(yw^{-1}) = 1 (\neq 1')$. By the same argument we obtain $\chi(xy^{-1}) = 1$ and also $\chi(wz^{-1}) = 1$. But now the equations

$$(vw^{-1})(wx^{-1}) = vx^{-1} \quad \text{and } (vw^{-1})(wz^{-1}) = vz^{-1}$$

together with our assumption lead to $x = z$, a contradiction! Thus, the assumption cannot be correct on T, and a pair with the desired properties must exist. □

This completes the proof of Theorems A and B.

2. Generalities.

Having obtained that the class $\boldsymbol{rP}$ of groups G admitting a partition into disjoint subsets $\{1\}, C_1, \ldots, C_r$ such that for every $i \in [r]$

and every choice of distinct elements $x, y \in C_i$ the product $xy \notin C_i$ is a class of groups of bounded order, one would like to determine the finitely many isomorphism types of groups in this class $\boldsymbol{rP}$. Exploiting the group structure of $\boldsymbol{rP}$-groups one hopes to get much sharper bounds on order and exponent of $\boldsymbol{rP}$-groups than those given by the Ramsey numbers in Theorem B or the Corollary to Theorem A. But, as long as one has only an essentially combinatorial approach, such an enterprise seems to be feasible only for very small values of r. We shall treat here only the cases $r = 2$ and $r = 3$.

The case $r = 2$ may be approached directly by easy combinatorial trickery.

PROOF OF THEOREM C. *a*) Let $G \in \boldsymbol{2P}$, that is $G = \{1\} \cup A \cup B$ with the product of any two distinct elements of A (resp. B) being in $B \cup \{1\}$ (resp. $A \cup \{1\}$). We shall show $|G| \leqslant 9$.

Suppose $|A| \geqslant |B|$, and $|A| \geqslant 5$. Then of the four distinct elements $a_1 a_i$, $i = 2, 3, 4, 5$, at least three lie in B; hence $|B| \geqslant 3$.

Choose $x_1 \in A$. There is an element $x_2 \in A \setminus \{x_1, x_1^{-1}\}$; so one has $x_1 x_2 \in B$.

If the $|A|$ elements $(x_1 x_2)a$, $a \in A$, all belonged to A, then one would have $|B \setminus \{x_1 x_2\}| = 1$ since $(x_1 x_2)b \in A \cup \{1\}$ for all $b \in B \setminus \{x_1 x_2\}$. Thus there exists an element $x_3 \in A$ with $(x_1 x_2)x_3 \in B$.

There exists an element $x_4 \in A \setminus \{x_3, x_3^{-1}, (x_1 x_2 x_3)^{-1}\}$ with $x_3 x_4 \in B$ and $x_3 x_4 \neq x_1 x_2$: Hence $(x_1 x_2)(x_3 x_4) \in A$. Now there exists an element $x_5 \in A \setminus \{x_4, x_4^{-1}, x_4^{-1} x_1 x_2 x_3, (x_1 x_2 x_3 x_4)^{-1}\}$. (We owe this choice of x_5 to a suggestion of M. J. Tomkinson, Glasgow.) One has then $x_4 x_5 \in B$, $x_4 x_5 \neq x_1 x_2 x_3$ or $(x_1 x_2 x_3)^{-1}$ Hence we get $x_1 x_2 x_3 x_4 x_5 \in A$. If $x_5 \neq \neq x_1 x_2 x_3 x_4 \in A$, then $(x_1 x_2 x_3 x_4) x_5 \in B$, a contradiction. Thus we must have $x_5 = x_1 x_2 x_3 x_4$ and $A = \{x_4, x_4^{-1}, x_4^{-1} x_1 x_2 x_3, (x_1 x_2 x_3 x_4)^{-1}, x_5\}$. Now $x_5^2 = (x_1 x_2 x_3)(x_4 x_5) \in A$, as $x_1 x_2 x_3 \neq x_4 x_5$.

If $x_5^2 \neq x_5^{-1} = (x_1 x_2 x_3 x_4)^{-1} \in A$, then $x_5 = x_5^2 x_5^{-1} \in B$, a contradiction. So $x_5^3 = 1$.

From $5 = |A| \geqslant |B|$ it follows that $|G| = 9, 10$, or 11. But the group G has order divisible by 3. Hence $|G| \leqslant 9$.

If $|G| = 8$ or $G \cong C_9$ then one checks that $G \notin \boldsymbol{2P}$. On the other hand, it is not difficult to choose subsets A and B in $G \cong C_3 \times C_3$ showing that $G \in \boldsymbol{2P}$. □

For $r > 2$ we shall need some helpful organisation.

3. The computer programme CP.

In order to decide constructively whether a set of n elements has an r-partition, i.e. a partition into r disjoint subsets, that fulfills some property P, one can generate all such partitions and check whether there is one with this peroperty P. An algorithm for this is given in [1]; it generates each new r-partition from its predecessor by moving a single element from one subset to another. The number of r-partitions of a set of n elements is known as the Stirling number of the second kind $S(n, r)$, it is given by the recursive formula (see [1]):

$$\begin{aligned} S(n, r) &= S(n-1, r-1) + r \cdot S(n-1, r) && n > r \\ S(n, r) &= 1 && n = r \\ S(n, r) &= 0 && n < r\,. \end{aligned}$$

Solving this, one obtains

$$S(n, r) = \frac{1}{r!} \sum_{i=0}^{r} (-1)^i \binom{n}{i} (r-i)^n\,.$$

One can see that

$$S(n, r) > r^{n-r}\,.$$

This relation shows that generating all partitions is practical only for small n and r. The sizes of some of the groups we have to check are larger than 40, and the present super computers need more than a life time to deal with them! We can generate all t-partitions, $\leqslant r$, of n elements as follows:

0) Start with the partition of the empty set.

1) Once we have a t-partition p of the first $k < n$ elements, we get from it $\min(t+1, r)$ partitions p' of the first $k+1$ elements by adding the $(k+1)$-st element to each of the subsets of p or, if $t < r$, as a set by itself.

Let T be a directed graph the nodes of which are all the t-partitions of the first k-elements of a given set of n elements, $t \leqslant r$, $k \leqslant n$; the edge $p \to p'$ exists in T if and only if p' is generated from p by adding a single element to a subset of p.

T is a tree with root the empty partition; its leaves are all the t-partitions of the n elements.

A backtrack algorithm is a general method of generating all the nodes of similar trees, where the nodes are combinatorial items. We start by generating the root and then we generate all the nodes of subtrees—branches—rooted on the sons of the root, by the same method, subtree after subtree. Examples of backtrack algorithms, both recursive and iterative, are given in [6].

The value of backtrack algorithms in our context lies in the fact that they facilitate pruning a tree. Once we know that a subtree does not have a « good » leaf, we prune the whole subtree; after generating the root of such a subtree, we do not generate any of its sons, but pass immediately to its next brother, if it has any. We do not dispose of any magic rule to decide whether a subtree has a good leaf. Otherwise we could apply that magic rule to the root and would know immediately whether a given group is in $\boldsymbol{rP}$.

We prune the tree in two cases:

1) if the $(k+1)$-st element violates the property P, i.e. in our case if in the subset to which it was added there now is a triple of elements one of which is the product of the others.

2) If among the elements not in any subset of p there is an element that cannot be added to p withoug violating the property P.

4. The algorithm.

In order to use one algorithm for all cases each group is transformed to the following standard representation:

The n elements are the integers $0, \ldots, n-1$ where 0 represents the unit element.

The group operation $\cdot$ is an $n \times n$ integer matrix MULT: MULT $(i, j) = i \cdot j \cdot$MULT is used just for building another $n \times n$ set matrix UNFIT:

$$\text{UNFIT}\,(i, j) = \{i \cdot j, j \cdot i, i \cdot j^{-1}, i^{-1} \cdot j, j \cdot i^{-1}, j^{-1} \cdot \text{i}\}\,.$$

A partition of $\{1, \ldots, k\}$ is kept in two ways: as an array showing for each j, $1 \leqslant j \leqslant k$, to which of the subsets $1, \ldots, r$ it belongs, and as an array of r stacks each holding one of the subsets.

Once an element k is added to a subset t we build a set

$$\mathrm{CAN}\,(k) = \mathrm{CAN}\left(\mathrm{stack}\,(t, \mathrm{top}\,(t))\right) \setminus \sum \mathrm{UNFIT}\,(k, i); \qquad i \in \mathrm{stack}_i\,.$$

(The stacks are not treated as pure stacks.)

Using CAN (k) helps us perform prunings of the first kind. This type of prunine along was found to be powerful enough; just one to ten minutes were needed for checking each of the groups on a P.C. using Turbo-Pascal.

For the second pruning we check whether

$$\mathrm{CAN}\left(\mathrm{stack}\,(t, \mathrm{top}\,(t))\right) = \{k+1, \ldots, n\}\,.$$

The input to the algorithm is: a list of generators and relations and a list of group elements.

The output of the algorithm is: all r-partitions of the elements $\neq 1$ as groups in $\boldsymbol{rP}$ or a note that this group does not belong to $\boldsymbol{rP}$.

We shall refer to these computer programmes as CP.

Proof of Theorem C. *b*) The situation for $\mathbf{3P}$ being much more complicated than for $\mathbf{2P}$, we resort to the intensive use of our CP.

Lemma 1. For the cyclic group C_n of order n one has $C_n \in \mathbf{3P}$ if and only if $4 \leqslant n \leqslant 15$.

Proof. It is easy to check that $C_n \in \mathbf{3P}$ if $4 \leqslant n \leqslant 15$. By our CP we proved

a) $C_n \notin \mathbf{3P}$ for $16 \leqslant n \leqslant 30$, and

b) the partial semigroup $S_{24} \subseteq \{\mathbb{N}, +\}$ may not be 3-coloured such that the sum of any two elements of the same colour has a different colour.

Therefore $C_n \notin \mathbf{3P}$ for $n \geqslant 16$.

Remark. The partial semigroup $S_{23} \subseteq \{\mathbb{N}, +\}$ has exactly the following three partitions such that in the corresponding colourings the sum of any two distinct elements of the same colour has a different

colour:

1) $A_1 = \{9, 10, 12, 13, 14, 15, 16, 17, 18, 20\}$
   $A_2 = \{1, 2, 4, 8, 11, 22\}$
   $A_3 = \{3, 5, 6, 7, 19, 21, 23\}$
2) $A_1 = \{9, 10, 12, 13, 14, 15, 16, 18, 20\}$
   $A_2 = \{1, 2, 4, 8, 11, 17, 22\}$
   $A_3 = \{3, 5, 6, 7, 19, 21, 23\}$
3) $A_1 = \{9, 10, 12, 13, 14, 15, 17, 18, 20\}$
   $A_2 = \{1, 2, 4, 8, 11, 16, 22\}$
   $A_3 = \{3, 5, 7, 19, 21, 23\}$

LEMMA 2. Abelian groups of orders $2^5, 3^3, 5^2, 7^2, 11^2, 13^2, 2^2 \cdot 5$, $2^2 \cdot 7$, $3^2 \cdot 5$, $2^3 \cdot 3$, and $2^2 \cdot 3^2$ do not belong to $\mathbf{3P}$. If the abelian group A has order 16 and belongs to $\mathbf{3P}$ then it is elementary abelian or a direct product of two cyclic groups of order 4.

PROOF. This was checked by our CP. Of the given orders > 16 there exist 31 isomorphism types of abelian groups none of which belongs to $\mathbf{3P}$. The direct product of the cyclic group of order 8 with the group of order 2 does not belong to $\mathbf{3P}$.

LEMMA 3. For the abelian group $A \in \mathbf{3P}$ one has $|A| \leqslant 18$ and $|A| \neq 17$.

PROOF. By Lemma 1 the set $\pi(A)$ of prime divisors of $|A|$ is contained in the set $\{2, 3, 5, 7, 11, 13\}$. Thus, if $|A| > 18$, the group A would have a subgroup A_0 of one of the orders > 16 discussed in Lemma 2. But the colouring of $A \in \mathbf{3P}$ would induce such a colouring of A_0. However, Lemma 2 gives $A_0 \notin \mathbf{3P}$. Thus $|A| \leqslant 18$.

Checking through the well-known groups of order 16 our CP provides us with the useful

LEMMA 4. There are precisely two non-abelian groups of order 16 that belong to $\mathbf{3P}$:

$$G_1 = \langle x, y, z, w;\ x^2 = y^2 = w^2 = 1,\ z^2 = w,\ zy = yzw\ ,$$
$$[x, y] = [x, z] = [y, x] = [z, w] = 1\rangle$$

$$G_2 = \langle x, y, z, w;\ x^2 = y^2 = w^2 = 1,\ y^2 = z,\ yx = xyw,$$
$$[x, z] = [y, z] = [y, w] = [z, w] = 1\rangle\ .$$

In both these groups the subgroup $\langle x, z, w\rangle$ is a characteristic subgroup of order 8.

LEMMA 5. The soluble groups of orders $2\cdot11$, $2\cdot13$, $3\cdot7$, $3\cdot13$, $5\cdot11$, $2\cdot3\cdot5$, $2^2\cdot5$, $2^2\cdot7$, $2^3\cdot5$, $2^3\cdot7$, 3^3, $2^3\cdot3^2$, $2^4\cdot3$, $2^4\cdot5$, $2^4\cdot7$, 2^5 are not in $\mathbf{3P}$.

PROOF. The following non-abelian groups were checked by our CP; none of them belongs to $\mathbf{3P}$. We arrange them in a table:

Order of the non-abelian soluble group	$2\cdot11$	$2\cdot13$	$3\cdot7$	$3\cdot13$	$5\cdot11$	$2\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot5$	3^3	$2^3\cdot3$	$2^2\cdot3^2$
number of isomorphism types	1	1	1	1	1	3	2	3	2	9	10

a) The soluble non-abelian group of orders $2^3\cdot5$ and $2^2\cdot3\cdot5$ are not in $\mathbf{3P}$: By Sylow's theorem and its generalisation by P. Hall any such group G contains a subgroup H of order $2^2\cdot5$. By Lemma 3 and the result reported in the preceding table, $H \notin \mathbf{3P}$. But then G cannot belong to $\mathbf{3P}$, for otherwise any $\mathbf{3P}$-colouring of G would induce such a colouring in H.

b) A group of order $2^3\cdot7$ does not belong to $\mathbf{3P}$: A group G of this order has a normal subgroup H of prime index p. If $p = 2$, then $|H| = 2^2\cdot7$. By Lemma 3 and the above table $H \notin \mathbf{3P}$. Hence we may assume $p = 7$ and H is an elementary abelian 2-subgroup of order 8; G is a Frobenius group of order $2^3\cdot7$. Using our CP we checked that this Frobenius group does not belong to $\mathbf{3P}$.

c) A group of order $2^3 \cdot 3^2$ does not belong to **3P**: A group G of this order contains a normal subgroup H of prime index p. If $p = 2$, then H has order $2^2 \cdot 3^2$. Lemma 3 and the table yield that $H \notin \mathbf{3P}$. Hence we may assume that $p = 3$ and $|H| = 2^3 \cdot 3$. Again Lemma 3 and the table yield $H \notin \mathbf{3P}$. Thus $G \notin \mathbf{3P}$.

d) A group of order $2^4 \cdot 3$, $2^4 \cdot 5$, or $2^4 \cdot 7$ does not belong to **3P**: In each case, such a group contains a normal subgroup H of prime index p. If $p = 2$, then the possible orders for H are $2^3 \cdot 3$, $2^3 \cdot 5$ or $2^3 \cdot 7$, respectively. By the table, Lemma 3, and the result in step *b*) we obtain $H \notin \mathbf{3P}$. Thus we may assume that p is odd and H is a normal subgroup of order 16. If H is abelian, Lemma 2 yields that H is either elementary abelian or a direct product of two cyclic groups of order 4. Assume $H \cong C_4 \times C_4$, then H contains a characteristic elementary abelian subgroup V of order 4. Thus G contains a subgroup K on order $4 \cdot p$. If $p = 5$ or 7 then Lemma 3 and the table imply $K \notin \mathbf{3P}$. If $p = 3$, and a Sylow 3-subgroup T of G normalises a subgroup E of order 8, then Lemma 3 and the table yield that $K = TE \notin \mathbf{3P}$. Up to isomorphism there is only one group G of order $2^4 \cdot 3$ with normal subgroup $H \cong C_4 \times C_4$ and such that no subgroup of order 8 is normal in G. Our CP checked that this group is not in **3P**.

Hence we may assume that $H \lhd G$ and H is elementary abelian. If $p = 7$, then G is not a Frobenius group since $7 \nmid (2^4 - 1)$. Thus $14 \| C_G(S) \|$, where S is a Sylow 7-subgroup of G. In particular, S normalises a subgroup E of order 8 in H. But the subgroup $K = ES \notin \mathbf{3P}$ by step *b*).

If $p = 5$ then G must be a Frobenius group, since a group of order $2^2 \cdot 5$ or $2^3 \cdot 5$ cannot be in **3P**. Our CP checked that this Frobenius groups does not belong to **3P**.

If $p = 3$, then either G is a Frobenius group, or the Sylow 3-subgroup S of G has fixed-points $\neq 1$ in H. In the latter case S normalises a subgroup E or order 8 in H. As the subgroup $K = ES \notin \mathbf{3P}$ by the table, $G \notin \mathbf{3P}$. The case that G is a Frobenius group is ruled out by our CP.

If the normal subgroup H of order 16 is non-abelian and in **3P**, then by Lemma 4 there is a characteristic normal subgroup E of order 8 in H. Thus, if S is a Sylow p-subgroup of G the subgroup $K = ES \notin \mathbf{3P}$, by the previous results.

To complete the proof of Lemma 5, we only have to consider groups of order 2^5.

e) A group of order 2^5 does not belong to **3P**: If G is such a group in **3P** then by Lemma 3 G is non-abelian. By Lemmas 2 and 4 we know the possible structure of maximal subgroups of G.

Case 1. All maximal subgroups of G are abelian. Suppose G contains maximal subgroups $R \cong C_2 \times C_2 \times C_2 \times C_a$ and $S \cong C_4 \times C_4$. Then $|R \cap S| = 8$, this intersection is elementary abelian as subgroup of R and of exponent 4 as maximal subgroup of S, a contradiction. Thus maximal subgroups of G must be of the same type.

If all the maximal subgroups of G were of elementary abelian, then every non-trivial element of G would be an involution, and hence G would be abelian, a contradiction. Thus assume that every maximal subgroup of G is of type $C_4 \times C_4$. Let R and S be two distinct maximal subgroups of G, then $|R \cap S| = 8$ and $R \cap S$ is isomorphic to $C_4 \times C_2$. Clearly $R \cap S = Z(G)$, since G is non-abelian. For any $x \in G \setminus (R \cap S)$ the subgroup $(R \cap S)\langle x \rangle$ is abelian and thus proper. Thus this subgroup is of type $C_4 \times C_4$, and the element x has order 4. Therefore G contains exactly 3 involutions which form a subgroup $T \cong C_2 \times C_2$ inside $Z(G)$. For every element $y \in G$ of order 4, one has $y^2 \in T$. Hence G/T is elementary abelian. In particular, if y and z are elements of order 4 in G, the subgroup $\langle y, z \rangle$ is a proper subgroup of G contained in a subgroup isomorphic to $C_4 \times C_4$. Thus $yz = zy$, and G is abelian, a contradiction.

Case 2. G contains a non-abelian maximal subgroup H. By Lemma 4 the subgroup H is isomorphic to one of the two groups given there. Let $x \in G \setminus H$, $G = H\langle x \rangle$. Now we checked by our CP that the partial semigroup $T \leqslant \{G, \cdot\}$, $T = \{H^\# := H \setminus \{1\} \cup \{x\} \cup H^\# x\}$ of 31 elements of G does not admit a 3-colouring. Thus $G \notin \mathbf{3P}$. □

LEMMA 6. The non-abelian simple groups A_5, A_6, A_7, $PSL(2, 7)$, and $PSL(2, 8)$ do not belong to **3P**.

PROOF. Our CP showed that $A_5 \notin \mathbf{3P}$. Since $A_5 \subset A_6 \subset A_7$, the groups A_6 and A_7 cannot belong to **3P**. The groups $PSL(2, 7)$ and $PSL(2, 8)$ contain soluble subgroups of orders 21 and $2^3 \cdot 7$, respectively. By Lemma 5 these subgroups cannot belong to **3P**, neither can the containing group.

We now come to the final step in the proof of Theorem C ***b***):

LEMMA 7. If $G \in \mathbf{3P}$, then $|G| \leqslant 18$.

PROOF. Assume this statement is false, and let G be a minimal (finite!) counter-example. Thus, proper subgroups of G will be in $\mathbf{3P}$ and hence be of order $\leqslant 18$. Further, by Lemma 1, the set $\pi(G)$ of prime divisors of $|G|$ is contained in $\{2, 3, 5, 7, 11, 13\}$. Assume H is a subgroup of prime order $p = 11$ or 13 of G. Then H cannot be contained properly in any proper subgroup of G; in particular, either $H = N_G(H)$ or H is normal in G of prime index. In the first case $H = N_G(H)$, by Burnside's theorem H has a normal complement K in G, which is a minimal normal subgroup of G. Since $|K| \leqslant 18$ the subgroup K is soluble, hence elementary abelian. By Lemmas 3 and 5 the subgroup K cannot be of prime order. So the only possibilities for $|K|$ are 2^i, $2 \leqslant i \leqslant 4$, and 3^3. As $H = N_G(H)$, one has $|K| = |G: N_G(H)|$ the number of Sylow p-subgroups of G. By Sylow's theorem this number is congruent to 1 mod p. But this is clearly not the case for $p = 11$ or 13 with $|K| = 4, 8, 16$, or 9. So this case cannot arise.

If H is normal in G, then $|G: H|$ is a prime. But then Lemmas 3 and 5 show that $G \notin \mathbf{3P}$, a contradiction. Therefore we may assume that neither 11 nor 13 divide $|G|$, i.e. $|G| \in \{3^3, 2^5$, divisor of $2^4 \cdot 3^2 \cdot 5 \cdot 7\}$.

If G is soluble, then $\{5, 7\} \not\subseteq \pi(G)$ and $3^2 \cdot 5 \nmid |G|$, since G cannot contain an abelian subgroup of order > 18. For G one therefore obtains one of the following orders: $2 \cdot 3 \cdot 5$, $2^2 \cdot 3 \cdot 5$, $2^2 \cdot 3^2$, $2^2 \cdot 5$, $2^2 \cdot 7$, $2^3 \cdot 3$, $2^3 \cdot 5$, 2^5, 3^3, $2^3 \cdot 7$, $2^3 \cdot 3^2$, $2^4 \cdot 3$, $2^4 \cdot 5$, $2^4 \cdot 7$, $3^2 \cdot 5$, or a product of two primes. But by Lemmas 3 and 5 groups of these orders do not belong to $\mathbf{3P}$.

There remains the case that G is non-soluble. A non-abelian composition factor of G must—for order reasons—be one of the simple groups considered in Lemma 6. If a minimal normal subgroup of G is non-soluble, it would be a direct product of isomorphic copies of the simple groups considered there. But these groups do not belong to $\mathbf{3P}$, so G could not belong to $\mathbf{3P}$. This contradiction shows that $S(G) \neq \langle 1 \rangle$, where $S(G)$ denotes the largest normal soluble subgroup of G. A minimal normal subgroup of $G/S(G)$ is a direct product of the simple groups considered in Lemma 6. As each of these simple groups contains a soluble subgroup of order $\geqslant 10$, the non-soluble group G contains a soluble subgroup K of order $K \geqslant 20$. This contradicts the minimality of G. □

This completes the proof of Theorem C ***b***).

REFERENCES

[1] G. EHRLICH, *Algorithm* **477**: *Generator of set-partitions to exactly R subsets* [G7], Communication of the ACM, **17**, no. 4 (1974), pp. 224-225.
[2] S. EVEN, *Algorithmic Combinatorics*, Mac Millan (1973), pp. 60-61.
[3] R. L. GRAHAM, *Rudiments of Ramsey theory*, CBMS Regional Conference Series in Mathematics, no. 45, American Math. Soc. (1981).
[4] R. L. GRAHAM - B. L. ROTSCHILD, *Ramsey's theorem for n-parameter sets*, Trans. Amer. Math. Soc., **159** (1971), pp. 257-292.
[5] R. L. GRAHAM - B. L. ROTHSCHILD - J. H. SPENCER, *Ramsey Theory*, Wiley-Interscience Series in Discrete Math. (1980).
[6] E. REINGOLD - J. NIVERGELT - N. DEO, *Combinatorial Algorithms*, Prentice-Hall (1977), pp. 106-112.
[7] J. SANDERS, *A Generalization of Schur's Theorem, dissertation*, Yale University (1969).
[8] S. SHELAH, *Primitive recursive bounds for van der Waerden numbers*, J. AMS, **1** (1988), pp. 683-697.
[9] I. SCHUR, *Über die Kongruenz* $x^m + y^m$ *congruent* $z^m \pmod p$, Iber, Deutsche Math. Verein., **25** (1916), pp. 114-116.
[10] I. SCHUR, *Gesammelte Abhandlungen*, Springer-Verlag, Berlin (1973).
[11] B. L. VAN DER WAERDEN, *Beweis einer Baudetschen Vermutung*, Nieuw. Arch. Wisk., **19** (1927), pp. 212-216.

Manoscritto pervenuto in redazione il 27 agosto 1989.