THE FACTORISATION OF FINITE ABELIAN GROUPS

by

A.D. SANDS. M.Sc.

A famous conjecture of Minkowski, concerning the columnation of space-filling lattices, was first proved by Hajós in 1941 by translating the problem into one involving finite abelian groups. The problem solved by Hajós was one concerning a special type of factorisation of finite abelian groups. In the general problem considered in the thesis no restriction is placed on the nature of the factors. It was originally conjectured by Hajós that, in any factorisation, one of the factors must possess a non-trivial subgroup as a factor. However, Hajós himself soon found that not all finite abelian groups possess this property. Those which do were called "good" and those which do not were called "bad".

Further contributions to determining those groups which are good and those which are bad were made by Rédei and de Bruijn. But for groups of many types the problem was left undecided. In this thesis the problem is solved completely for finite abelian groups. A special case of this problem for cyclic groups was shown by de Bruijn to be equivalent to a conjecture of his concerning bases for the sets of integers. This conjecture and a generalisation of it are also shown to be true.

It is shown first that a cyclotomic polynomial is

irreducible over certain fields of roots of unity. This extension of the well-known result that a cyclotomic polynomial is irreducible over the rational field is basic to the following work and is used frequently throughout the thesis.

A theorem, similar to the theorems of de Bruijn, showing that certain types of groups are bad is then proved. Then, in the main part of the thesis all the groups not shown to be bad by this theorem or one of the theorems of de Bruijn are shown to be good.

Hajós gave a method which, he claimed, would give all factorisations of a good group. However it is shown that a correction is needed in this method and the corrected method is then presented.

The final section is concerned with the extension of the results to certain types of infinite abelian groups. Under the restriction that one of the factors shall have only a finite number of elements, similar results to those proved for finite groups are obtained for the generalisations of these groups to the infinite cases.

Acta.Math.Acad.Sci.Hungar.,Vol. 8, 1957, pp 65-86

THE FACTORISATION OF FINITE ABELIAN GROUPS

A Thesis presented on application for the Degree

of Doctor of Philosophy in the

University of Glasgow

by

Arthur David Sands, M.Sc.

October 1957

ACKNOWLEDGMENT

The work of this thesis has been carried out in the Department of Mathematics in the University of Glasgow under the supervision of Professor R.A. Rankin, whom I would like to thank for his guidance, encouragement and general advice.

CONTENTS

INTRODUCTION

A famous conjecture of Minkowski concerning the columnation of space filling lattices was first proved by Hajós in 1941 by translating the problem into one involving finite abelian groups. The problem solved by Hajós was a special case of the problem of the factorisation of finite abelian groups. In this general problem no restriction is placed on the nature of the factors. It was originally conjectured by Hajós that in any factorisation one of the factors must possess a non-trivial subgroup as a factor. However, Hajós himself soon found that not all finite abelian groups satisfy this conjecture. Those which do were called "good" and the remaining groups which do not were called "bad". Further contributions to the problem of determining those groups which are good and those which are bad were made by Rédei and de Bruijn. But for many groups the problem was left undecided. A list of these groups is given by de Bruijn (1, p.259). In this thesis this problem is completely solved. De Bruijn also linked a special case of the problem with a problem concerning bases for the sets of integers. He put forward a conjecture concerning certain factorisations of finite cyclic groups equivalent to his conjecture concerning the integers. This conjecture, and a generalisation of it, are also shown to be true.

The scope of the thesis is now outlined.

Chapter I is an introductory chapter in which the fundamental definitions and notations are presented. Then certain preliminary results needed later in the thesis are proved. Of these Theorem 1.1

on the irreducibility of the cyclotomic polynomials over certain fields of roots of unity is basic to the following work and is used frequently throughout the remainder of the thesis. It enables us in many cases to substitute the use of a cyclotomic polynomial of order a power of a prime for more general cyclotomic polynomials.

In Chapter II the theorems of de Bruijn on bad groups are listed and one new theorem of a similar kind is added to them. This theorem shows that the groups of two of the types, listed by de Bruijn as undecided, are, in fact, bad.

In Chapter III the results on finite cyclic groups are presented. The generalisation of the conjecture of de Bruijn is proved in Theorem 3.2. Then it is shown that groups of the three remaining undecided types of finite cyclic groups are good.

Chapter IV deals with the non-cyclic groups. Here again it is shown, taking into account the results of Chapter II, that the groups of the remaining undecided types are good.

Hajós put forward a method which, he claimed, would give all factorisations of a good group. In Chapter V a necessary correction to this method is made. It is then shown that a similar method can be applied to certain special types of factorisation.

When he discovered that not all groups are good, Hajós put forward a more general conjecture concerning the quasi-periodicity of one of the factors. No general result concerning this conjecture has yet been proved. But in Chapter VI it is shown that the groups of one of the types, which have been shown to be bad in this thesis, do indeed satisfy the conjecture.

Certain generalisations to infinite abelian groups are made in Chapter VII. It is shown in many of the cases where a group of type $\{p^{\lambda}\}$ has occurred earlier in the thesis that it can be replaced by a group of type $\{p^{\infty}\}$. But the restriction is made in all cases that one of the factors shall have a finite number of elements.

Except for some preliminary remarks at the beginnings of Chapters I and VII all the work in the thesis is claimed as original. Of the formally stated results, Lemma 1.2, Lemma 5.2 and Theorem 6.1 would appear to be known to previous contributors to the subject but are given as they do not seem to have been formally proved before. Theorem 5.3 is a correction of a very similar theorem by Hajós. All other theorems and lemmas are claimed to be original.

CHAPTER I

Introduction

In Chapter I the problem of the factorisation of abelian groups is stated and the fundamental notations and definitions to be used throughout the thesis are given. It is then shown that the problem can be stated in terms of polynomials and of complex numbers. These interpretations of the problem are due to Hajós and to Rédei.

Certain preliminary results, which are to be used later in the thesis, are then obtained. Theorem 1.1 is an extension of a well known theorem on cyclotomic polynomials. Lemmas 1.2 and 1.3 are developments of results due to de Bruijn and Lemma 1.4, Lemma 1.5 and Lemma 1.6 are further results concerning products of cyclotomic polynomials.

Preliminaries

Unless otherwise stated the word group shall mean finite abelian group throughout the thesis. Groups and subgroups will be denoted by letters like G, H and K; subsets of groups by A, B, C, etc.; elements of groups by a, b, g, h, etc.; e will be used to denote the unit element. If A and B are subsets of a group G, the product AB is defined to be the set of all elements of the form ab, where a is in A and b is in B. If every element of AB is expressible in only one way as ab the product is said to be direct. If every element of G occurs in a direct product

AB then $G = AB$ and this is called a factorisation of G: the subsets A and B are called the factors of G.

A subset A of a group G is said to be periodic if there exists an element g of G, $g \neq e$, such that $gA = A$. The element g is called a period of A.

If A and B are subsets of a group G, then $A \circ B$ is used to denote any one of the subsets* $\sum_{i=1}^{n} a_i b_i$, where the elements of A are $a_1, a_2, \dots, a_n$ and the elements b_i are arbitrary elements of B. By an expression of the form $A_1 \circ A_2 \cdot A_3 \circ A_4 \cdot \dots \circ A_n$ is meant any one of the subsets obtained by bracketing the above expression with n-2 brackets to the left of A_1 and brackets after $A_2, A_3, \dots, A_{n-1}$, i.e., by bracketing from the left.

If $A = \sum_{i=1}^{n} a_i$ and $B = \sum_{i=1}^{m} b_i$ are subsets of a group G then $AB = (\sum_{i=1}^{n} a_i)(\sum_{i=1}^{m} b_i)$ where the multiplication is carried out as though $\sum$ meant addition and the distributive laws held. Clearly the number of elements in a direct product is the product of the number of elements in each term. Thus the number of elements in a factor of a group G is a divisor of the order of G. If $G = AB$ then $G = (gA)(hB)$ where g and h are any elements of G. Hence it may be assumed that e is in A and e is in B since any other factorisation may be obtained from such a factorisation by the above method. This assumption is made throughout the thesis.

* $\sum$ is used with group elements to mean set theoretic union.

Let G be a cyclic group of order n and A and B subsets such that $AB = G$. Then if g is a generator of G, $A = \sum_{i=1}^{m} g^{\alpha_i}$ and $B = \sum_{i=1}^{n/m} g^{\beta_i}$, $AB = (\sum_{i=1}^{m} g^{\alpha_i})(\sum_{i=1}^{n/m} g^{\beta_i}) = \sum_{i=0}^{n-1} g^{i}$ and the multiplication is carried out by adding the indices modulo n. This relationship remains true if g is replaced by any number ρ, provided $\rho^{n} = 1$. Thus, if ρ is an n^{th} root of unity $(\sum_{i=1}^{m} \rho^{\alpha_i})(\sum_{i=1}^{n/m} \rho^{\beta_i}) = \sum_{i=0}^{n-1} \rho^{i}$, where $\sum$ now is used to mean addition. If $\rho \neq 1$ then $\sum_{i=0}^{n-1} \rho^{i} = 0$ and it follows that $\sum_{i=1}^{m} \rho^{\alpha_i} = 0$ or $\sum_{i=1}^{n/m} \rho^{\beta_i} = 0$. A similar replacement can be made in terms of polynomials. Since $x^{i_1} \equiv x^{i_2} (\mathrm{mod}\ (x^{n} - 1))$ if and only if $i_1 \equiv i_2 \pmod{n}$, it follows that $A(x) \cdot B(x) \equiv 1 + x + x^{2} + \dots + x^{n-1} \quad (\mathrm{mod}\ (x^{n} - 1))$ where $A(x) = \sum_{i=1}^{m} x^{\alpha_i}$ and $B(x) = \sum_{i=1}^{n/m} x^{\beta_i}$.

If elements $g_1, g_2, \dots, g_k$ of orders $n_1, n_2, \dots, n_k$ respectively are an independent set of generators of a group G, then any subsets A and B of G can be expressed in the form

$$A = \sum_{i=1}^{m} g_1^{\alpha_{1i}} \dots g_k^{\alpha_{ki}}, \quad B = \sum_{i=1}^{n/m} g_1^{\beta_{1i}} \dots g_k^{\beta_{ki}}$$

and the multiplication of A by B is carried out by adding the exponents of each g_j modulo n_j. Thus each g_j can be replaced by a root of unity of suitable order. It will be found convenient to replace one generating element, say g_1, by x and to replace the remaining generators by roots of unity of suitable orders, thus obtaining equations involving polynomials in x, whose coefficients are complex numbers, multiplication of the polynomials being carried out modulo $(x^{n_1} - 1)$.

It will be clear, from the above discussion involving roots of unity and relationships of the form

$$A(x) \quad B(x) \equiv 1 + x + \qquad + x^{n-1} \quad (\text{mod } (x^n - 1)),$$

that the cyclotomic polynomials will play an important part in this treatment of the problem. Throughout the thesis $F_n(x)$ will denote the n^{th} cyclotomic polynomial. It is well known that the cyclotomic polynomials are irreducible, to the extent of a constant factor, over the rational field.[*] The following extension of this result is now proved.

THEOREM 1.1 If n and m are relatively prime, the n^{th} cyclotomic polynomial $F_n(x)$ is irreducible, to the extent of a constant factor, over the field of the m^{th} roots of unity.

Proof: Let ρ and σ be primitive roots of unity of orders n and m respectively. Let $A(x)$ be a polynomial with coefficients from the field of the m^{th} roots of unity such that $A(\rho) = 0$. To prove the theorem it is sufficient to show that $A(\rho^d) = 0$ for all integers d relatively prime to n. It may be assumed, by multiplying throughout by a constant if necessary, that $A(x) = \sum_r a_r x^r$ where $a_r = \sum_s b_{r,s} \sigma^s$ and the coefficients $b_{r,s}$ are integers. Then

$$A(\rho) = \sum_r a_r \rho^r = \sum_r \sum_s b_{r,s} \sigma^s \rho^r = 0.$$

For each pair of integers r and s let $t_{r,s}$ be the unique integer such that $o \leq t_{r,s} < n\,m$, $t_{r,s} \equiv s \pmod{m}$ and

[*] See, for example, Van der Waarden, Modern Algebra, Vol.I, pp. 156-158.

$t_{r,s} \equiv r \pmod{n}$. Then $o = A(\rho) = \sum_{r,s} b_{r,s} (\rho\sigma)^{t_{r,s}}$. But $\rho\sigma$ is an nm^{th} primitive root of unity and the nm^{th} cyclotomic polynomial is irreducible, to the extent of a constant factor, over the rational field. It follows that $\sum_{r,s} b_{r,s}((\rho\sigma)^d)^{t_{r,s}} = o$ for all integers d relatively prime to nm.

Consider the set of n numbers $1, 1 + m, \ldots, 1 + (n-1)m$. These form a complete set of residues modulo n. Hence among these are $\varphi(n)$[*] numbers incongruent modulo n and prime to n. Let $d = 1 + cm$ be any such number. Then, since d and n are relatively prime and d and m are relatively prime, it follows that d and nm are relatively prime. Thus

$$\begin{aligned} O &= \sum_{r,s} b_{r,s} ((\rho\sigma)^d)^{t_{r,s}} = \sum_{r,s} b_{r,s} (\sigma^{1+cm} \rho^d)^{t_{r,s}} \\ &= \sum_{r,s} b_{r,s} (\sigma\rho^d)^{t_{r,s}} = \sum_{r,s} b_{r,s} \sigma^s (\rho^d)^r \\ &= \sum_{r} a_r (\rho^d)^r = A(\rho^d). \end{aligned}$$

This completes the proof.

COROLLARY. If the greatest common divisor of m and n is 2, then $F_n(x)$ is irreducible, to the extent of a constant factor, over the field of the m^{th} roots of unity.

Proof. Let n be equal to $2k$ and m be equal to $2l$. Then k and l are relatively prime and so k or l is odd.

If l is odd, then n and l are relatively prime. Therefore, by the theorem, $F_n(x)$ is irreducible over the field of the l^{th}

[*] $\varphi(n)$ denotes Euler's φ function.

roots of unity. But, since $m = 2l$ and l is odd, this is also the field of the m^{th} roots of unity.

Suppose that l is not odd. Then k is odd. Let ρ be a primitive n^{th} root of unity. Let $A(x)$ be a polynomial with coefficients from the field of the m^{th} roots of unity with $A(\rho) = 0$. Then, as before, it is sufficient to show that $A(\rho^d) = 0$ for all integers d relatively prime to n. Such integers d are odd. Let $B(x) = A(-x)$. Then $B(-\rho) = A(\rho) = 0$. Now $-\rho$ is a k^{th} primitive root of unity. For $\rho^{2k} = 1$ and $\rho^k \neq 1$. Therefore $\rho^k = -1$ and $(-\rho)^k = -\rho^k = 1$. Further $(-\rho)^{l} = 1$ implies $\rho^{2l} = 1$ and so that $2k$ is a divisor of $2l$. Hence, since k and m are relatively prime, $B((-\rho)^d) = 0$ for all integers d relatively prime to k. Let d be relatively prime to n. Then d is also relatively prime to k. Thus $A(\rho^d) = A(-(-\rho)^d) = B((-\rho)^d) = 0$.

This completes the proof.

It is well-known that the n^{th} cyclotomic polynomial $F_n(x)$ can be expressed as $F_n(x) = \prod_{d/n} (x^{n/d} - 1)^{\mu(d)}$, where the product is taken over all divisors d of n and $\mu(d)$ is the möbius function.*

LEMMA 1.2. If $N = mn$, where $m = p^\lambda$ and p is a prime not dividing n then

$$\prod_{d/n} F_{md}(x) = \frac{x^N - 1}{x^{N/p} - 1}$$

* See Van der Waarden, Modern Algebra, Vol. I, pp. 108.

Proof. $$\prod_{d|n} F_{md}(x) = \prod_{d|N} F_d(x) \Big/ \prod_{d|\frac{N}{p}} F_d(x)$$
$$= \frac{x^N - 1}{x^{N/p} - 1}$$

De Bruijn proves in Theorem 2 (2, p.374) that if $A(x)$ is a polynomial with non-negative integral coefficients of degree less than n, where $n = p^\lambda q^\mu$ and p and q are distinct primes, and if $F_n(x) \mid A(x)$, then $A(x)$ can be expressed as

$$A(x) = P(x)(x^n - 1)/(x^{n/p} - 1) + Q(x)(x^n - 1)/(x^{n/q} - 1)$$

where $P(x)$ and $Q(x)$ are polynomials with non-negative integral coefficients. The following extension of this theorem is now proved.

LEMMA 1.3. If $N = p^\lambda q^\mu M$, where $p^\lambda = n$, $q^\mu = m$ and p and q are distinct primes not dividing M, $A(x)$ is a polynomial of degree less than N with non-negative integral coefficients and $F_{nmd}(x)$ divides $A(x)$ for all divisors d of M then $A(x)$ can be expressed as

$$A(x) = \frac{x^N - 1}{x^{N/p} - 1} A_p(x) + \frac{x^N - 1}{x^{N/q} - 1} A_q(x)$$

where $A_p(x)$ and $A_q(x)$ are polynomials with non-negative integral coefficients.

Proof. Repeated use is made of Theorem 1 of (2, p.372) to show that such a representation exists with polynomials with integral coefficients. Let $M = \prod_{i=1}^{k} r_i^{\nu_i}$, where the numbers r_i are distinct primes. Then, since $F_N(x) \mid A(x)$ it follows by Theorem 1 of (2) that

$$(1) \quad A(x) = \frac{x^N - 1}{x^{N/p} - 1} B_p(x) + \frac{x^N - 1}{x^{N/q} - 1} B_q(x) + \sum_{i=1}^{k} \frac{x^N - 1}{x^{N/r_i} - 1} B_{r_i}(x) .$$

Now if s is a prime dividing N, then by Lemma 1.2, $F_{N/r_k}(x)$ divides $(x^N - 1)/(x^{N/s} - 1)$ if and only if $s \neq r_k$. Therefore, since $F_{N/r_k}(x) \mid A(x)$, it follows from (1) that $F_{N/r_k}(x) \mid B_{r_k}(x)$. Hence, by Theorem 1 of (2),

$$B_{r_k}(x) = \frac{x^{N/r_k} - 1}{x^{N/pr_k} - 1} B_p{}^1(x) + \frac{x^{N/r_k} - 1}{x^{N/qr_k} - 1} B_q{}^1(x) + \sum_{i=1}^{k-1} \frac{x^{N/r_i} - 1}{x^{N/r_i r_k} - 1} B_{r_i}{}^1(x)$$

$$+ \frac{x^{N/r_k} - 1}{x^{N/r_k 2} - 1} B_{r_k}{}^1(x),$$

the last term only occurring if r_k divides N/r_k, i.e. if $v_k \geqslant 2$. When this expression for $B_{r_k}(x)$ is substituted into (1) and

$\dfrac{x^N - 1}{x^{N/r_k} - 1} \cdot \dfrac{x^{N/r_k} - 1}{x^{N/pr_k} - 1}$ is written as $\dfrac{x^N - 1}{x^{N/p} - 1} \cdot \dfrac{x^{N/p} - 1}{x^{N/pr_k} - 1}$

with similar changes for q and for r_i, the following expression for $A(x)$ is obtained:-

$$A(x) = \frac{x^N - 1}{x^{N/p} - 1} B_p''(x) + \frac{x^N - 1}{x^{N/q} - 1} B_q''(x) + \sum_{i=1}^{k-1} \frac{x^N - 1}{x^{N/r_i} - 1} B_{r_i}''(x)$$

$$+ \frac{x^N - 1}{x^{N/r_k^2} - 1} B_{r_k}''(x),$$

the last term only occurring if $v_k \geqslant 2$. Continuing, step by step, in this way using $F_{N/r_k 2}(x), \ldots, F_{N/r_k v_k}(x)$,

$F_{N/r_{k-1} r_k^{v_k}}(x), \ldots, F_{N/M}(x)$ the following expression for $A(x)$

is finally obtained:

$$A(x) = \frac{x^N - 1}{x^{N/p} - 1} B^*_p (x) + \frac{x^N - 1}{x^{N/q} - 1} B^*_q (x),$$

where $B^*_p(x)$ and $B^*_q(x)$ have integral coefficients.

Now the method of proof of Theorem 2 of (2, p.374) with $v = N/pq$ can be used to show that $A_p(x)$ and $A_q(x)$ can be found with non-negative integral coefficients such that

$$A(x) = \frac{x^N - 1}{x^{N/p} - 1} A_p (x) + \frac{x^N - 1}{x^{N/q} - 1} A_q (x).$$

This completes the proof.

LEMMA 1.4. If n and m are relatively prime then $\prod_{d/m} F_{nd}(x) = F_n(x^m)$.

Proof. The proof is by induction on the number of distinct prime divisors of m. Let $m = q^\lambda$ where q is a prime. Then

$$\begin{aligned}\prod_{d/m} F_{nd}(x) &= F_n(x) . F_{nq}(x) \, F_{nq^2}(x) \dots F_{nq^\lambda}(x) \\ &= \Big(\prod_{d/n} (x^{n/d} - 1)^{\mu(d)}\Big)\Big(\prod_{d/n} (x^{nq/d} - 1)^{\mu(d)} \prod_{d/n} (x^{n/d} - 1)^{\mu(dq)}\Big) \\ &\quad \Big(\prod_{d/n} (x^{nq^2/d} - 1)^{\mu(d)} \prod_{d/n} (x^{nq/d} - 1)^{\mu(dq)} \prod_{d/n} (x^{n/d} - 1)^{\mu(dq^2)}\Big) \\ &\quad \dots \Big(\prod_{d/n} (x^{nq^\lambda/d} - 1)^{\mu(d)} \prod_{d/n} (x^{nq^{\lambda-1}/d} - 1)^{\mu(dq)} \dots \\ &\quad \prod_{d/n} (x^{n/d} - 1)^{\mu(dq^\lambda)}\Big).\end{aligned}$$

Since $\mu(c) = 0$ if c is not square free only those divisors d of n, and the corresponding numbers dq, such that d is square free, need be considered. In this case $\mu(dq) = - \mu(d)$. Then

$$\begin{aligned}\prod_{d|m} F_{nd}(x) &= \prod_{d|n}(x^{n/d}-1)^{\mu(d)} \prod_{d|n}(x^{n/d}-1)^{-\mu(d)} \prod_{d|n}(x^{nq/d}-1)^{\mu(d)} \\ &\qquad \prod_{d|n}(x^{nq/d}-1)^{-\mu(d)} \cdots \prod_{d|n}(x^{nq^{\lambda}/d}-1)^{\mu(d)} \\ &= \prod_{d|n}\left((x^{q^{\lambda}})^{n/d}-1\right)^{\mu(d)} \\ &= F_n(x^{q^{\lambda}})\end{aligned}$$

Suppose that the lemma is true for numbers m with $k - 1$ prime divisors. Let q be a prime not dividing m or n.

Then $$\begin{aligned}\prod_{d|mq^{\lambda}} F_{nd}(x) &= \prod_{d|m} F_{nd}(x) \prod_{d|m} F_{nqd}(x) \cdots \prod_{d|m} F_{nq^{\lambda}d}(x) \\ &= F_n(x^m) \cdot F_{nq}(x^m) \cdots F_{nq^{\lambda}}(x^m) \\ &= F_n(x^{mq^{\lambda}}).\end{aligned}$$

The first step follows by the inductive hypothesis and the second by the argument already used.

This completes the proof.

LEMMA 1.5. If every prime divisor of m is a divisor of n then $F_n(x^m) = F_{nm}(x)$.

Proof. The square free divisors of n and of nm are the same.

Therefore $$\begin{aligned}F_n(x^m) &= \prod_{d|n}(x^{mn/d}-1)^{\mu(d)} \\ &= \prod_{d|nm}(x^{nm/d}-1)^{\mu(d)} = F_{nm}(x).\end{aligned}$$

LEMMA 1.6. If $m = n_1 n_2$ where every prime divisor of n_1 is a divisor of n and no prime divisor of n_2 is a divisor of n then

$$F_n(x^m) = \prod_{d|n_2} F_{nn_1 d}(x).$$

Proof.

$$\begin{aligned} F_n(x^m) &= F_n((x^{n_2})^{n_1}) \\ &= F_{nn_1}(x^{n_2}) \quad , \text{ by Lemma 1.5} \\ &= \prod_{d|n_2} F_{nn_1 d}(x) \quad , \text{ by Lemma 1.4.} \end{aligned}$$

CHAPTER II

Introduction

It was conjectured by Hajós that in every factorisation of a group G involving two factors, at least one of the factors was periodic. However, Hajós himself showed that this is not the case. He called a group possessing this property "good" and groups admitting of factorisations AB= G with neither A nor B periodic he called "bad". De Bruijn improved on Hajós' results concerning bad groups. In this chapter a sufficient condition for a group to be bad is given, the theorems of de Bruijn on bad groups are stated and one new theorem of a similar type is then proved. As a consequence of this theorem it is shown that groups of two of the types listed by de Bruijn as unsolved cases are bad.

THEOREM 2.1. If a group G possesses a proper subgroup H and H admits of factorisations $H = AB = AC$, where A is non-periodic and B and C have no period in common then G is bad.

Proof. Let $k_1, k_2, \dots, k_n$ be a set of coset representatives for G by H. Let $D = Bk_1 + C(k_2 + k_3 + \dots + k_n)$. Then $AD = AB\,k_1 + AC\,(k_2 + \dots + k_n) = Hk_1 + H(k_2 + \dots + k_n) = G$. Now A is non-periodic. Let g be a period of D. Then $g = h\,k_i$ for some i, $1 \leqslant i \leqslant n$, where h is an element of H. Consider $h\,k_i\,B\,k_1$. Now $k_i\,k_1 = h_1\,k_j$ for some j, $1 \leqslant j \leqslant n$, and some element h_1 in H. Thus $h\,k_i\,b\,k_1 = h\,b\,h_1\,k_j = h_2\,k_j$, where b is in B and h_2 is in H. It follows that, for some fixed j, $h\,k_i\,B\,k_1 \subseteq H\,k_j$. But $h\,k_i\,D = D$. Therefore $h\,k_i\,B\,k_1 \subseteq B\,k_1 + Ck_2 + \dots + C\,k_n$. Thus if $j = 1$ then $h\,k_i\,B\,k_1 = B\,k_1$ and if $j > 1$ $=$ $h\,k_i\,B\,k_1 = C\,k_j$. ?

In the second case it follows that $C = h\,k_i\,k_1\,k_j^{-1}\,B$ and thus that any period of B is also a period of C. Since B and C have no period in common it follows that B and C must be non-periodic. Thus H is bad and it follows by the result of de Bruijn that subgroups of good groups are good, Theorem 4 (1, p. 263), that G is also bad. In the first case $h\,k_i\,B\,k_1 = B\,k_1$ and therefore $h\,k_i\,B = B$. Since B is contained in the subgroup H it follows that $h\,k_i$ is in H. Therefore $h\,k_i\,C\,k_2$ is contained in $H\,k_2$. But $h\,k_i\,C\,k_2$ is contained in $B\,k_1 + C\,k_2 + \cdots + C\,k_n$. It follows that $h\, k_i\, C\, k_2 = C\, k_2$ and hence that $h\, k_i\, C = C$. Therefore $h\, k_i$ is a period of both B and C. But this is not possible. Therefore, in this case, D is non-periodic and $AD = G$ is a factorisation of G with both factors non-periodic. Thus G is bad.

This completes the proof.

It will be shown later that this is also a necessary condition for a group to be bad, but no direct proof of this has been discovered and it is not proved until the problem of deciding whether or not a group is good or bad has been completely solved.

All the groups shown to be bad by de Bruijn do have this property. Indeed, it is the property used by de Bruijn to construct his non-periodic factorisation.

The following is the set of results obtained by de Bruijn on bad groups.[*]

(1) If G possesses a subgroup H which is a direct product of subgroups H_1 and H_2 of composite order and not of type $\{2,2\}$ then G is bad.

(2) If G possesses a proper subgroup H which is a direct product of cyclic subgroups H_1 and H_2 of the same order and this order is greater than three, then G is bad.

(3) If G possesses a proper subgroup K and K a proper subgroup H of type $\{3,3\}$ then G is bad.

(4) If G possesses a proper subgroup K and K a proper subgroup H which is a direct product of two subgroups of type $\{2,2\}$

[*] See de Bruijn (1).

then G is bad.

The following theorem, which is similar to those listed above, is now proved.

THEOREM 2.2. If a group G possesses a proper subgroup K and K a proper subgroup H which is the direct sum of a subgroup L of composite order and a subgroup of type $\{2,2\}$ then G is bad.

prod.

Proof. It may be assumed that L is not of type $\{2,2\}$ since de Bruijn has already shown that the theorem is true in this case. Then, by Lemma 1 of (1, p. 259) L contains a proper subgroup M, of order greater than 1, with a set of coset representatives $l_1, l_2, \ldots, l_k$ of L by M which is not periodic. Let $k_1, k_2, \ldots, k_n$ be any set of coset representatives for K by H. Let b and c be elements of order 2 generating the subgroup.of type $\{2,2\}$.

Let $A = \{k_2, \ldots, k_n\}.\{(e, bc) + (b, c).(M-e)\} + k_1.M.(e, l_2 bc)$, where l_2 is an element of L but not of M and $M - e$ indicates all elements of M except e. Let

$B = (e, b).(l_1, l_2, \ldots, l_k)$

and $C = (e, c).(l_1, l_2, \ldots, l_k)$.

Then

$$\begin{aligned} AB &= \{k_2, \ldots, k_n\}.(e, bc).(e).(e, b).(l_1, \ldots, l_k) \\ &\quad + \{k_2, \ldots, k_n\}.(b, c).(M-e).(e, b).(l_1, \ldots, l_k) \\ &\quad + k_1.M.(e, l_2 bc).(e, b).(l_1, \ldots, l_k) \\ &= (k_2, \ldots, k_n).(e).(e, b, c, bc).(l_1, \ldots, l_k) \\ &\quad + (k_2, \ldots, k_n).(M-e).(e, b, c, bc).(l_1, \ldots, l_k) \\ &\quad + k_1.M.(e, b, l_2 c, l_2 bc)(l_1, \ldots, l_k) \end{aligned}$$

$$= (k_2, \ldots, k_n).(e, b, c, bc).(l_1, \ldots, l_k).M$$
$$+ k_1.L.(e, b, l_2 c, l_2 bc)$$
$$= (k_2, \ldots, k_n).L.(e, b, c, bc) + k_1.L.(e, b)$$
$$+ k_1 . l_2 L.(c, bc)$$
$$= (k_2, \ldots, k_n).L.(e, b, c, bc) + k_1.L.(e, b, c, bc)$$
$$= (k_1, k_2, \ldots, k_n).L$$
$$= K$$

Similarly, since $(e, c) . (e, bc) = (e, b, c, bc)$ also, it may be shown that $AC = K$.

Let g be a period of both B and C. Then, since B and C are contained in H, g is an element of H and so of one of the forms, l, lb, lc, lbc; where l is an element of L. Now if $g = l$ then it takes $(l_1, l_2, \ldots, l_k)$ into $(l_1, l_2, \ldots, l_k)$. But this set is not periodic and so this case is impossible. lb could be a period of B but could not be a period of C since l, lb is not in C. Similarly lc could be a period of C but is not a period of B. lbc is not a period of either B or C. Thus B and C can have no period in common.

Let f be a period of A. Then f is an element of K. Therefore multiplication by f will permute the cosets Hk_1, Hk_2, ..., Hk_n. If $f\,k_1 M.(e, l_2 bc) = k_1 M.(e, l_2 bc)$ then $f M.(e, l_2 bc) = M.(e, l_2 bc)$ and f is an element of H. Therefore f is of one of the forms l', $l'b$, $l'c$, $l'bc$ where l' is an element of L. Clearly f can only be of the first or last form. But, since f is in H, it must also take

$(e, bc) + (b, c).(M - e)$ into itself. l' cannot do this, unless $l' = e$, since it does not lie in this set. $l'bc$ only does this if $l' = c$. But bc is not a period of $M.(e, l_2\, bc)$ since l_2 is not in M. The remaining possibility is that f take $k_1 M.(e, l_2 bc)$ into $k_i\{(e, bc) + (b, c).(M - e)\}$. Now f is of the form $k_j l$, $k_j l b$, $k_j l c$ or $k_j l b c$, where l is an element of L.

Let $f_1 = k_j\, l$. Then both $f_1 k_1$ and $f_1 k_1 l_2$ lie in $k_i M$. Therefore $(f_1 k_1)^{-1} f_1 k_1 l_2$ lies in $k_i^{-1} k_i M$. Thus l_2 lies in M. But this is not the case. Therefore A is not periodic.

Hence, by Theorem 2.1, G is bad.

COROLLARY. Groups of type $\{p^{\lambda}, 2, 2\}$, including those of type $\{2^{\lambda}, 2, 2\}$, where p is a prime, are bad if $\lambda \geq 4$.

These are the only groups to which this theorem applies to which one of the theorems of de Bruijn, which are listed above, does not already apply.

CHAPTER III

Introduction

In this chapter a lemma is first proved which is applicable to all groups, dealing with factorisations in which one factor has two or three elements. But the remainder of the chapter is devoted entirely to cyclic groups. It is proved that if $AB = G$, where G is a cyclic group, and the number of elements in A is a power of a prime then A or B is periodic. This is a generalisation of a conjecture by deBruijn that the result held when the number of elements in A was a prime.* In the final part of the chapter it is shown that groups of type $\{p^2, q^2\}$, $\{p^2, q, r\}$ and $\{p, q, r, s\}$, where p, q, r and s are distinct primes, are good. This, together with the previous work of Rédei, Hajós and de Bruijn, completely solves the problem of deciding whether a finite cyclic group is good or bad.

Factorisations in which the number of elements in one factor is a power of a prime

LEMMA 3.1 If G is a group and $AB = G$ where A has two or three elements then either A or B is periodic.

Proof. (i) Let A have two elements e and a. Then $(e, a) B = G$. Therefore $a(e, a) B = (a, a^2) B = aG = G$.

* See de Bruijn (2, p. 371).

Comparing these two results it is seen that $(e, a)\, B = (a, a^2)\, B$. Therefore $e\, B = a^2 B$. It follows that B is periodic or that $a^2 = e$, in which case A is periodic.

(ii) Let A have three elements e, a and b. Then $(e, a, b)\, B = G$. Therefore $a\,(e, a, b)\, B = (a, a^2, ab)\, B = G$. It follows from these two results that $(e, b)\, B = (a^2, ab)\, B$. Now if bB and abB have an element in common, then eB and aB have an element in common, which contradicts $AB = G$. Therefore $bB = a^2 B$ and so $eB = abB$. It follows that B is periodic or that $b = a^2$ and $e = ab$ in which case a is a period of A.

This completes the proof.

THEOREM 3.2. If G is a finite cyclic group, $AB = G$ and A has p^{μ} elements, where p is a prime then either A or B is periodic.

Proof. Let the order of G be $N = p^{\lambda} n$, where $p^{\lambda} = m$, p does not divide n and $\lambda \geqslant \mu$. Let $p^{\mu - 1} = v$. Let a and b be generators of G of orders m and n respectively. Then $g = ab$ generates G and it may be supposed that

$$A = \sum_{i=1}^{pv} a^{\alpha_i} b^{\beta_i} = \sum_{i=1}^{pv} g^{\gamma_i} \qquad \text{and}$$

$$B = \sum_{i=1}^{N/pv} a^{\lambda_i} b^{\mu_i} = \sum_{i=1}^{N/pv} g^{\nu_i}$$

where $\alpha_1 = \beta_1 = \gamma_1 = \lambda_1 = \mu_1 = \nu_1 = 0$ and $0 \leqslant \alpha_i < m$, $0 \leqslant \beta_i < n$, $0 \leqslant \gamma_i < N$, $0 \leqslant \lambda_i < m$, $0 \leqslant \mu_i < n$ and $0 \leqslant \nu_i < N$. Then $\alpha_i \equiv \gamma_i \pmod{m}$, $\beta_i \equiv \gamma_i \pmod{n}$,

$\lambda_i \equiv V_i \pmod m$ and $\mu_i \equiv \nu_i \pmod n$. Let

$$A_a(x) = \sum_{i=1}^{p^{\nu}} x^{\alpha_i}, \quad B_a(x) = \sum_{i=1}^{N/p^{\nu}} x^{\lambda_i},$$
$$A(x) = \sum_{i=1}^{p^{\nu}} x^{\gamma_i}, \quad B(x) = \sum_{i=1}^{N/p^{\nu}} x^{\nu_i}.$$

Then, from AB = G, it follows that

$$A_a(x)\, B_a(x) \equiv n(1+x+\dots+x^{m-1}) (\mathrm{mod}\,(x^m-1)).$$

Therefore, for each divisor r of m, with $r>1$, $F_r(x) \mid A_a(x).B_a(x)$ and so $F_r(x) \mid A_a(x)$ or $F_r(x) \mid B_a(x)$. Since $F_r(1) = p$, $A_a(1) = p^{\mu}$ and $B_a(1) = p^{\lambda-\mu} n$, it follows that $F_r(x)$ divides A(x) for precisely μ such divisors r of m. Let these be $r_1, r_2, \dots, r_{\mu}$ with $r_1 > r_2 > \dots > r_{\mu}$.

These results are now used to show that no two of the numbers α_i occurring among the exponents in $\sum_{i=1}^{p^{\nu}} x^{\alpha_i}$ are equal. Suppose that two such α_i are equal. Then there is a coefficient at least equal to two in $A_a(x)$. If $r_1 < m$, the exponents of $A_a(x)$ are reduced modulo r_1, i.e. $A_a(x)$ is reduced modulo $(x^{r_1} - 1)$, to give $A_a^1(x)$; then, since $F_{r_1}(x)$ divides $A_a(x)$ and $x^{r_1} - 1$ it divides $A_a^1(x)$ and the degree of $A_a^1(x)$ is less than r_1.
Therefore

$$A_a^{'}(x) = A_a^{2'}(x)\left(1 + x^{r_1/p} + \dots + x^{(p-1)r_1/p}\right).$$ (by lemma

The degree of $A_a^{2'}(x)$ is less than $r_1 - (p-1) r_1/p = r_1/p$.
Now $A_a^{'}(x)$ has non-negative coefficients of which one is at least two. It follows that $A_a^{2'}(x)$ has non-negative coefficients, one of

which is at least two. Since $F_{r_2}(x)$ divides $A_a(x)$ and $x^{r_1} - 1$ it follows that $F_{r_2}(x)$ divides $A_a^{1}(x)$ and thus that it divides $A_a^{2'}(x)$. If $r_2 < r_1 / p$ the exponents of $A_a^{2'}(x)$ are reduced modulo r_2, i.e. $A_a^{2'}(x)$ is reduced modulo $(x^{r_2} - 1)$, to give $A_a^{2}(x)$. Then $A_a^{2}(x)$ has non-negative integral coefficients of which one is at least 2 and it is divisible by $F_{r_2}(x)$. Therefore

$$A_a^{2}(x) = A_a^{3'}(x)\left(1 + x^{r_2/p} + \dots + x^{(p-1)r_2/p}\right).$$

It follows, as before, that the coefficients of $A_a^{3'}(x)$ are non-negative and that one of them is at least two. Continuing in this way using $F_{r_3}(x), \dots, F_{r_\mu}(x)$ the following result is finally obtained:-

$$A_a^{\mu}(x) = A_a^{(\mu+1)'}(x)\left(1 + x^{r_\mu/p} + \dots + x^{(p-1)r_\mu/p}\right)$$

where the coefficients of $A_a^{(\mu+1)'}(x)$ are non-negative and one of them is at least two. Thus the sum of the coefficients in $A_a^{\mu}(x)$ is at least 2p. Working back from this it is seen that the sum of the coefficients in $A^{1}_a(x)$, and so in $A_a(x)$, is at least 2 pv. But this sum is pv. It follows that the numbers α_i in $\sum_{i=1}^{pv} x^{\alpha_i}$ are all distinct.

From AB = G it follows that

$$A(x).B(x) \equiv (1 + x + \dots x^{N-1})(\mathrm{mod}\,(x^{N}-1)).$$

Therefore for each divisor d of N, with d > 1, $F_d(x) \mid A(x).B(x)$ and so $F_d(x) \mid A(x)$ or $F_d(x) \mid B(x)$.

If $F_{md}(x) \mid B(x)$ for each divisor d of n, then, by Lemma 1.2, $((x^{N}-1)/(x^{N/p}-1)) \mid B(x)$ and so $g^{N/p}$ is a period of B.

Thus it may be assumed that, for some divisor d of n, $F_{md}(x)$ divides $A(x)$. Let ρ and σ be primitive roots of unity of orders m and n respectively. Let $n = dk$. Then $\tau = \rho\sigma^{k}$ is an $(md)^{\text{th}}$ primitive root of unity. Therefore $F_{md}(\tau) = 0$. Hence $A(\tau) = 0$.

Thus $\sum_{i=1}^{pv} \tau^{\gamma_i} = \sum_{i=1}^{pv} \rho^{\alpha_i}\sigma^{k\beta_i} = 0$. It follows by the irreducibility of $F_m(x)$ over the field of the n^{th} roots of unity that $F_m(x) \mid \sum_{i=1}^{pv} x^{\alpha_i}\sigma^{k\beta_i}$. Therefore

$$\sum_{i=1}^{pv} x^{\alpha_i}\sigma^{k\beta_i} = C(x)\left(1 + x^{m/p} + \dots + x^{(p-1)m/p}\right).$$

Since $0 \leqslant \alpha_i < m$, it follows that the degree of $C(x)$ is less than $m - (p-1)m/p$, i.e. less than m/p, and therefore that the coefficients of $C(x)$ are powers of σ, no sums of powers of σ occurring, since no two exponents α_i are equal. Since there are pv terms on the left and p terms in $F_m(x)$ there must be v terms in $C(x)$. Let the exponents occurring in $C(x)$ be $t_1, t_2, \dots, t_v$ with $0 = t_1 < t_2 < \dots < t_v < m/p$. Thus the numbers α_i are $t_1, t_2, \dots, t_v, t_1 + m/p, \dots, t_v + m/p, t_1 + 2m/p, \dots, t_v + (p-1)m/p$ and the coefficients of $x^{t_j}, x^{t_j + m/p}, \dots, x^{t_j + (p-1)m/p}$ in $\sum_{i=1}^{pv} x^{\alpha_i}\sigma^{k\beta_i}$ are equal for each j, where $j = 0, 1, \dots, v$. It follows that the corresponding exponents $k\beta_i$ are equal modulo n, and so that the corresponding numbers β_i are equal modulo d. Conversely, if the exponents α_i are as above, and the corresponding numbers β_i are equal modulo d, where $d \mid n$, then $F_{md}(x) \mid A(x)$. It follows that if $F_{md}(x) \mid A(x)$ so does $F_{mc}(x)$ whenever $c \mid d$ and also that if $F_{md_1}(x) \mid A(x)$ and $F_{md_2}(x) \mid A(x)$ so does $F_{md}(x)$ where d is the lowest common multiple of d_1 and d_2, provided that d_1 and d_2 are divisors of n.

If $F_{mn}(x) \mid A(x)$ then, from the above results, $F_{md}(x) \mid A(x)$ for all divisors d of n. Hence, by Lemma 1.2, $((x^{N}-1)/(x^{N/p}-1)) \mid A(x)$ and $g^{N/p}$ is a period of A.

Let u be the greatest divisor of n such that $F_{mu}(x) \mid A(x)$ It may be assumed that $u < n$. Then, by the above results, if d divides n, $F_{md}(x) \mid A(x)$ if and only if $d \mid u$. The information about A(x) which was obtained above may be written as

$$A(x) = \sum_{i=1}^{v} \sum_{s=1}^{p} x^{t_i + sv + k_{i,s} m}$$

where, for each i and for each pair s_1 and s_2, $0 < s_1 \leq p$, $0 < s_2 \leq p$, $t_i + s_1 v + k_{i,s_1} m \equiv t_i + s_2 v + k_{i,s_2} m \pmod{u}$ and so $s_1 + k_{i,s_1} p \equiv s_2 + k_{i,s_2} p \pmod{u}$.

Let $q_1, q_2, \ldots, q_k$ be the set of prime numbers such that there is a power of q_1 dividing n which does not divide u. Let the greatest powers of q_i dividing u and n be respectively $q_i^{\phi_i}$ and $q_i^{\theta_i}$. Then $\phi_i < \theta_i$. For each ω_i, such that $\phi_i < \omega_i \leq \theta_i$, $F_{m q_i^{\omega_i} d}(x)$ divides B(x) for every divisor d of $N/m\, q_1^{\theta_i}$. Repeated use is now made of Lemma 1.3. From

$F_{mq_1^{\theta_1}d}(x) \mid B(x)$ for all divisors d of $N/mq_1^{\theta_1}$ it follows that

$$(1) \qquad B(x) = \frac{x^N - 1}{x^{N/p} - 1} B_p(x) + \frac{x^N - 1}{x^{N/q_1} - 1} B_{q_1}(x)$$

where $B_p(x)$ and $B_{q_1}(x)$ have non-negative integral coefficients. Let $B_p(x)$ be chosen to satisfy (1) so that the sum of its coefficients is a maximum. Now if $\theta_1 - \phi_1 \geqslant 2$, $F_{mq_1^{\theta_1 - 1}d}(x) \mid B(x)$ for all divisors d of $N/mq_1^{\theta_1}$. But, by Lemma 1.2, all these cyclotomic polynomials divide $(x^N - 1)/(x^{N/p} - 1)$ and do not divide $(x^N - 1)/(x^{N/q_1} - 1)$. Therefore, from (1), they divide $B_{q_1}(x)$ and, also from (1), the degree of $B_{q_1}(x)$ is less than N/q_1. Hence, by Lemma 1.3,

$$B_{q_1}(x) = \frac{x^{N/q_1} - 1}{x^{N/pq_1} - 1} B_p'(x) + \frac{x^{N/q_1} - 1}{x^{N/q_1^2} - 1} B_{q_1}'(x)$$

where $B_p^1(x)$ and $B_{q_1}^1(x)$ have non-negative integral coefficients. Substituting for $B_{q_1}(x)$ in (1) it is seen, from the maximality of $B_p(x)$, that $B_p^1(x) = 0$ and thus

$$B(x) = \frac{x^N - 1}{x^{N/p} - 1} B_p(x) + \frac{x^N - 1}{x^{N/q_1^2} - 1} B_{q_1}'(x)$$

Continuing in this way, using $\theta_1 - 2, \ldots, \phi_1 + 1$, the following formula for $B(x)$ is obtained:-

$$(2) \qquad B(x) = \frac{x^N - 1}{x^{N/p} - 1} B_p(x) + \frac{x^N - 1}{x^{N/q_1^{\theta_1 - \phi_1}} - 1} B_{q_1}^*(x)$$

Now $F_{m q_2^{\theta_2} d}(x)$ divides $B(x)$ for every divisor d of $N/m q_2^{\theta_2}$ and so for every divisor d of $N/m q_1^{\theta_1 - \phi_1} q_2^{\theta_2}$. Applying this to (2) it follows, by Lemma 1.2, that $F_{m q_2^{\theta_2} d}(x) \mid B_{q_1}^{*}(x)$ for every divisor d of $N/m q_1^{\theta_1 - \phi_1} q_2^{\theta_2}$. From (2) the degree of $B_{q_1}^{*}(x)$ is less than $N/q_1^{\theta_1 - \phi_1}$. Therefore, by Lemma 1.3,

$$B_{q_1}^{*}(x) = \frac{x^{N/q_1^{\theta_1-\phi_1}} - 1}{x^{N/p q_1^{\theta_1-\phi_1}} - 1} B_p''(x) + \frac{x^{N/q_1^{\theta_1-\phi_1}} - 1}{x^{N/q_2 q_1^{\theta_1-\phi_1}} - 1} B_{q_2}(x)$$

where $B_p''(x)$ and $B_{q_2}(x)$ have non-negative integral coefficients.

Substituting for $B_{q_1}^{*}(x)$ in (2) it is seen from the maximality of $B_p(x)$ that $B_p''(x) = 0$ and then

$$B(x) = \frac{x^N - 1}{x^{N/p} - 1} B_p(x) + \frac{x^N - 1}{x^{N/q_1^{\theta_1-\phi_1} q_2} - 1} B_{q_2}(x)$$

Continuing in this way, using $q_2, \ldots, q_k$ the following expression for $B(x)$ is finally obtained:-

$$B(x) = \frac{x^N - 1}{x^{N/p} - 1} B_p(x) + \frac{x^N - 1}{x^{Nu/n} - 1} B_u(x)$$

$$= \frac{x^N - 1}{x^{N/p} - 1} B_p(x) + \frac{x^N - 1}{x^{mu} - 1} B_u(x),$$

where the coefficients of $B_p(x)$ and $B_u(x)$ are non-negative integers.

Now, using the above expression for $B(x)$, consider the number of exponents in $A(x) . B(x)$ which are congruent modulo mu. If one arises from $A(x) \, B_u(x) \, . \, (x^N - 1) / (x^{mu} - 1)$ then all possible exponents congruent to it, modulo $m\,u$, arise from this term. But, as no term in $A(x) . B(x)$ occurs twice, the same must therefore be true for exponents arising from $A(x) \, B_p(x) \, (x^N - 1)/(x^{N/p} - 1)$.

Suppose that some coefficient in $B_p(x)$ is non-zero and so that terms do arise from it.

$$\frac{x^N - 1}{x^{N/p} - 1} = 1 + x^{N/p} + \dots + x^{(p-1)N/p}.$$

Now the numbers $0, N/p, 2N/p, \dots, (p-1)N/p$ are congruent to $0, m/p, \dots, (p-1)m/p$ (modulo m) in some order, since $0, n, 2n, \dots, (p-1)n$ are congruent to $0, 1, \dots, p-1$ (mod p) in some order. Let $h_j\, N/p$ be congruent to $j\, m/p$ (modulo m) for $j = 0, 1, 2, \dots, p-1$. Then $h_{j_1}\, N/p + t_i + s_1\, m/p + k_{i,s_1} m$ is congruent to $h_{j_2}\, N/p + t_i + s_2\, m/p + k_{i,s_2}\, m$ modulo mu if and only if $j_1 + s_1 \equiv j_2 + s_2$ (mod p). For if $j_1 + s_1 \equiv j_2 + s_2$ (mod p) then, since $h_j\, N/p = j_1\, m/p + w_{j_1}\, m$ and $h_{j_2}\, N/p = j_2\, m/p + w_{j_2}\, m$, the two numbers are clearly congruent modulo m. Further

$$(h_{j_1} N/p + t_i + s_1 m/p + k_{i,s_1} m) - (h_{j_2} N/p + t_i + s_2 m/p + k_{i,s_2} m)$$
$$= (h_{j_1} m/p - h_{j_2} m/p)\, n + (s_1 + k_{i,s_1} p - s_2 - k_{i,s_2} p)\, m/p$$

But $u \mid n$ and $s_1 + k_{i,s_1} p \equiv s_2 + k_{i,s_2} p$ (mod u). Therefore the two numbers are also congruent modulo u. Since p does not divide u it follows that the two numbers are congruent modulo m u. Conversely if the two numbers are congruent modulo m u then, a fortiori, they are congruent modulo m and hence, from

$$h_{j_1} N/p + s_1 m/p \equiv h_{j_2} N/p + s_2\, m/p \pmod{m},$$

it follows that $j_1 + s_1 \equiv j_2 + s_2$ (mod p). Now for any given number t, $0 \leq t < p$ there are p different pairs j_i, s_i such that $j_i + s_i \equiv t$ (mod p) where $0 \leq j_i < p$, $0 < s_i \leq p$.. Thus in the product $A(x)B_p(x)(x^N-1)/(x^{N/p}-1)$ if any exponent occurs, there are a multiple of p exponents congruent to it modulo mu. Thus the exact number of exponents in $A(x)B_p(x)(x^N-1)/(x^{N/p}-1)$ congruent to any given exponent modulo mu is a multiple of p. But the total number of such exponents is $N/mu = n/u$ which is not divisible by p.

It follows that $B_p(x) = 0$. Therefore $(x^N-1)/(x^{mu}-1)$ divides B(x). Hence g^{mu} is a period of B.

This completes the proof.

Certain consequences of this theorem concerning other work by Hajós and de Bruijn will be mentioned later in the thesis.

GOOD CYCLIC GROUPS

There remain three types of cyclic group which have not been shown to be good or bad. In each of these three cases Theorem 3.2 applies to all but one essential type of factorisation. The remaining types of factorisation are dealt with by direct application of Theorem 1.1 in the case of the groups of type $\{p^2, q, r\}$ and $\{p, q, r, s\}$. The group of type $\{p^2, q^2\}$ is considered first.

THEOREM 3.3. If G is a group of type $\{p^2, q^2\}$, where p and q are distinct primes, then G is good.

Proof. Let AB = G. The essentially different cases which have to be considered are those in which A has p elements, p^2 elements and pq elements. The first two of these are covered by Theorem 3.2.

Let $p^2q^2 = n$. Let A have pq elements. Then B has pq elements. Let g be a generator of G. Let $A = \sum_{i=1}^{pq} g^{\alpha_i}$

and $B = \sum_{i=1}^{pq} g^{\beta_i}$. Let $A(x) = \sum_{i=1}^{pq} x^{\alpha_i}$ and $B(x) = \sum_{i=1}^{pq} x^{\beta_i}$. Then from AB = G it follows that

$$A(x).\,B(x) \equiv (1+x+\dots+x^{n-1})(\bmod\,(x^n-1)).$$

Therefore $F_n(x) \mid A(x).\,B(x)$ and so $F_n(x) \mid A(x)$ or $F_n(x) \mid B(x)$. Since A and B have the same number of elements it may be assumed, without loss of generality, that $F_n(x) \mid A(x)$. Then by Theorem 2 of (2, p.314) it follows that

$$A(x) = \frac{x^n-1}{x^{n/p}-1}\,A_p(x) + \frac{x^n-1}{x^{n/q}-1}\,A_q(x),$$

where $A_p(x)$ and $A_q(x)$ are polynomials with non-negative integral coefficients. Now $A(1) = pq = pA_p(1) + qA_q(1)$. Therefore either $A_p(1) = q$ and $A_q(1) = 0$ or $A_q(1) = p$ and $A_p(1) = 0$. In the first case $A_q(x) = 0$ and $((x^n-1)/(x^{n/p}-1)) \mid A(x)$, i.e. $g^{n/p}$ is a period of A. In the second case $A_p(x) = 0$ and $((x^n-1)/(x^{n/q}-1)) \mid A(x)$, i.e. $g^{n/q}$ is a period of A.

This completes the proof.

THEOREM 3.4. If a group G is of type $\{p^2, q, r\}$, where p, q and r are distinct primes, then G is good.

Proof. Let a, b and c be generators of G of orders p^2, q and r respectively. Let ρ, σ and τ be primitive roots of unity of orders p^2, q and r respectively.

Let AB = G. The essentially different cases which have to be considered are those in which A has p elements, p^2 elements, q elements and pq elements.

The first three of these are covered by Theorem 3.2.

Let A have pq elements. Then B has pr elements. Let

$A = \sum_{i=1}^{pq} a^{\alpha_i} b^{\beta_i} c^{\gamma_i}$ and $B = \sum_{i=1}^{pr} a^{\lambda_i} b^{\mu_i} c^{\nu_i}$. Then from $AB = G$ it follows that

$$\left(\sum_{i=1}^{pq} x^{\beta_i}\right)\left(\sum_{i=1}^{pr} x^{\mu_i}\right) \equiv p^2 r\,(1 + x + \ldots + x^{q-1}) (\mathrm{mod}\,(x^q - 1)).$$

Therefore $F_q(x)$ divides $\sum_{i=1}^{pq} x^{\beta_i}$ or $\sum_{i=1}^{pr} x^{\mu_i}$. But $F_q(1) = q$ and q does not divide pr. Therefore $F_q(x)$ can not divide $\sum_{i=1}^{pr} x^{\mu_i}$ and hence $F_q(x)$ divides $\sum_{i=1}^{pq} x^{\beta_i}$. It follows that the numbers β_i are $0, 1, \ldots, q-1$ and each of these must occur p times. Similarly it can be shown that the numbers ν_i are $0, 1, \ldots, r-1$, each occurring p times. Also from $AB = G$ it follows that

$$\left(\sum_{i=1}^{pq} x^{\alpha_i}\right)\left(\sum_{i=1}^{pr} x^{\lambda_i}\right) \equiv qr\,(1 + x + \ldots + x^{p^2-1}) (\mathrm{mod}\,(x^{p^2} - 1))$$

Therefore $F_{p^2}(x)$ and $F_p(x)$ divide $\left(\sum_{i=1}^{pq} x^{\alpha_i}\right).\left(\sum_{i=1}^{pr} x^{\lambda_i}\right)$. Since $F_{p^2}(1) = F_p(1) = p$, it follows that $F_p(x)$ divides either $\sum_{i=1}^{pq} x^{\alpha_i}$ or $\sum_{i=1}^{pr} x^{\lambda_i}$ and that $F_{p^2}(x)$ divides the other.

Replacing a, b and c by ρ, σ and τ respectively, it follows that $\left(\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i}\right).\left(\sum_{i=1}^{pr} \rho^{\lambda_i} \sigma^{\mu_i} \tau^{\nu_i}\right) = 0.$

Since q and r may be interchanged it may be assumed, without loss of generality, that $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} = 0$. Then it follows, by the irreducibility of $F_q(x)$ over the field of the $(p^2r)^{\text{th}}$ roots of unity, that $F_q(x)$ divides $\sum_{i=1}^{pq} \rho^{\alpha_i} \tau^{\gamma_i} x^{\beta_i}$ and so that

$$^{*} \sum_{i;\beta_i=0} \rho^{\alpha_i} \tau^{\gamma_i} = \sum_{i;\beta_i=1} \rho^{\alpha_i} \tau^{\gamma_i} = \ldots = \sum_{i;\beta_i=q-1} \rho^{\alpha_i} \tau^{\gamma_i}$$

From the results above each number β_i occurs precisely p times and so there are p elements in each sum.

[*] Where $\sum_{i;\beta_i=0}$ indicates that the summation is taken over those integers i for which $\beta_i = 0$.

Let $A_{k,h}(x) = \sum_{i;\beta_i=k} r^{\gamma_i} x^{\alpha_i} - \sum_{i;\beta_i=h} r^{\gamma_i} x^{\alpha_i}$, where $0 \leq k < q$ and $0 \leq h < q$. Then ρ is a root of the equation $A_{k,h}(x) = 0$ and so, by the irreducibility of $F_{p^2}(x)$ over the field of the r^{th} roots of unity, $F_{p^2}(x) \mid A_{k,h}(x)$. Since there are 2p terms in $A_{k,h}(x)$, either $A_{k,h}(x)$ is zero or else the exponents of x in $A_{k,h}(x)$ are $m, m+p, \ldots, m+p^2-p, n, n+p, \ldots, n+p^2-p$ where $0 \leq m < p$, $0 \leq n < p$ and m may be equal to n.

If for some pair k, h, $A_{k,h}(x) \neq 0$ and $m \neq n$, then the coefficient of $x^m, x^{m+p}, \ldots, x^{m+p^2-p}$ are equal, and the coefficients of $x^n, x^{n+p}, \ldots, x^{n+p^2-p}$ are equal.

If $r \neq 2$, then $r^{t_1} = -r^{t_2}$ is impossible and so $m, m+p, \ldots, m+p^2-p$ must occur as exponents in $\sum_{i;\beta_i=k} x^{\alpha_i}$ and $n, n+p, \ldots, n+p^2-p$ as exponents in $\sum_{i;\beta_i=h} x^{\alpha_i}$ or vice versa. Hence $\sum_{i;\beta_i=k} \rho^{\alpha_i} r^{\gamma_i} = 0$ and so $\sum_{i;\beta_i=t} \rho^{\alpha_i} r^{\gamma_i} = 0$ for $t = 0, 1, \ldots, q-1$.

If $r = 2$, then $r = -1$ and $r^{t_1} = -r^{t_2}$ is a possibility. Let us suppose that $\sum_{i;\beta_i=k} \rho^{\alpha_i} (-1)^{\gamma_i} \neq 0$. Then these exponents α_i are not all congruent to m, nor all congruent to n, modulo p. The complementary sets of α_i congruent to m modulo p and to n modulo p must occur in $\sum_{i;\beta_i=h} \rho^{\alpha_i} (-1)^{\gamma_i}$. Let $0 \leq l < q$ If $A_{k,l}(x) = 0$ then $\sum_{i;\beta_i=l} x^{\alpha_i}$ contains the same exponents α_i as $\sum_{i;\beta_i=k} x^{\alpha_i}$. If $A_{k,l}(x) \neq 0$ then, from the above, $\sum_{i;\beta_i=l} x^{\alpha_i}$ contains the complementary sets of exponents α_i to $\sum_{i;\beta_i=k} x^{\alpha_i}$ and so the same sets as $\sum_{i;\beta_i=h} x^{\alpha_i}$. Now $F_p(x)$ or $F_{p^2}(x)$ divides $\sum_{i=1}^{pq} x^{\alpha_i}$. If $F_p(x) \mid \sum_{i=1}^{pq} x^{\alpha_i}$ then there are the same number of α_i, namely q, congruent to 0, to 1, ..., and to p-1 modulo p. This is impossible since every α_i is congruent to m or to n modulo p and since r = 2, $p \neq 2$. If $F_{p^2}(x) \mid \sum_{i=1}^{pq} x^{\alpha_i}$ then there must be the same number of exponents α_i equal to m, to m+p, ..., to $m+p^2-p$. But certain of these occur with those $\beta_i = l$ such that $A_{k,l}(x) = 0$, while others occur with those $\beta_i = l$ such that $A_{k,l}(x) \neq 0$ and these two numbers cannot be equal, since their sum is q and q is odd as r = 2. Therefore if r = 2, $\sum_{i;\beta_i = t} \rho^{\alpha_i}(-1)^{\gamma_i} = 0$ for $t = 0, 1, \ldots, q-1$ also.

If $A_{k,h}(x) \neq 0$ for some pair k, h, but in every such case m = n, then the coefficients in $A_{k,h}(x)$ of $x^m, x^{m+p}, \ldots, x^{m+p^2-p}$ are equal. These coefficients are of one of the forms $\tau^{t_1}+\tau^{t_2}$, $\tau^{t_1}-\tau^{t_2}$ or $-\tau^{t_1}-\tau^{t_2}$. If $r \neq 2$, then it is easily seen that different types cannot be equal to each other. But neither the first type only nor the last type only can occur, as there are both plus and minus signs in $A_{k,h}(x)$. Therefore only the second type occurs. Now as $A_{h,l}(x) \neq 0$ the coefficients cannot be zero. If $\tau^{t_1}-\tau^{t_2} = \tau^{t_3}-\tau^{t_4}$ with $t_1 \neq t_2$ and $t_3 \neq t_4$ then $\tau^{t_1}+\tau^{t_4}-\tau^{t_2}-\tau^{t_3} = 0$. Therefore $F_r(x) \mid x^{t_1}+x^{t_4}-x^{t_2}-x^{t_3}$. Since $0 \leq t_i < r$ the remaining factor can only be constant and since all the coefficients in $F_r(x)$ are positive it must be zero. Therefore $t_1 = t_3$ and $t_2 = t_4$. It follows that all the powers of τ with a plus sign are equal, and all the powers of τ with a minus sign are equal. But the plus signs occur with $\beta_i = k$. Therefore in $\sum_{i;\beta_i = k} \rho^{\alpha_i}\tau^{\gamma_i}$ the exponents α_i are m, m+p, ..., $m+p^2-p$ and all the exponents γ_i are equal. Therefore $\sum_{i;\beta_i = k} \rho^{\alpha_i}\tau^{\gamma_i} = 0$ and hence $\sum_{i;\beta_i = t} \rho^{\alpha_i}\tau^{\gamma_i} = 0$ for $t = 0, 1, \ldots, q-1$.

If r = 2 then τ = -1 and the coefficients in $A_{k,h}(x)$ must all be +2 or all -2. If all are +2, then $\gamma_i = 0$ when $\beta_i = k$ and $\gamma_i = 1$ when $\beta_i = h$. Since no element occurs twice in A no α_i can occur twice with $\beta_i = k$ and $\gamma_i = 0$. Therefore the numbers α_i occurring with $\beta_i = k$ are m, m+p, ..., m+p^2-p. Similarly, if all the coefficients are -2, the exponents α_i occurring with $\beta_i = k$ are m, m+p, ..., m+p^2-p and all γ_i are equal. Therefore, in each case $\sum_{i;\beta_i = k} \rho^{\alpha_i} \tau^{\gamma_i}$ and so $\sum_{i;\beta_i = t} \rho^{\alpha_i} \tau^{\gamma_i} = 0$ for t = 0, 1, ..., q-1.

Thus, if for some pair k, h, $A_{k,h}(x) \neq 0$, $\sum_{i;\beta_i = t} \rho^{\alpha_i} \tau^{\gamma_i} = 0$ for $t = 0, 1, \dots, q-1$. Therefore $F_{p^2}(x)$ divides $\sum_{i;\beta_i = t} x^{\alpha_i} \tau^{\gamma_i}$ and since there are p terms in the sum it follows that the numbers α_i are m_t, m_t + p, ..., m_t + p^2 - p and that all γ_i in each sum are equal. Hence a^p is a period of A.

There remains the case where $A_{k,h}(x) = 0$ for all pairs k and h. In this case the coefficients of each x^{α_i} in $A_{k,h}(x)$ are zero. Thus for all k, h and t

$$\sum_{i;\, \beta_i = k,\, \alpha_i = t} \tau^{\gamma_i} - \sum_{i;\, \beta_i = h,\, \alpha_i = t} \tau^{\gamma_i} = 0 .$$

From this it follows that $F_r(x)$ divides $\sum_{i;\, \beta_i = k,\, \alpha_i = t} x^{\gamma_i} - \sum_{i;\, \beta_i = h,\, \alpha_i = t} x^{\gamma_i}$. This polynomial is either equal to zero or to $\pm F_r(x)$. For since its degree is less than or equal to r - 1 it must be a constant multiple of $F_r(x)$ and as A contains no element twice there cannot be two or more equal γ_i with $\beta_i = k$ and $\alpha_i = t$ or with $\beta_i = h$ and $\alpha_i = t$. It follows that any given exponent α_i occurs the same number of times with each β_i, or else r times with some

β_i and not at all with others. Each β_i occurs precisely p times and from $F_p(x)$ or $F_{p^2}(x)$ divides $\sum_{i=1}^{pq} x^{\alpha_i}$ there are at most q of any α_i. Since there are q distinct β_i, those α_i occurring with each β_i occur only once with each β_i and from the above occur with the same γ_i. If $F_{p^2}(x)$ divides $\sum_{i=1}^{pq} x^{\alpha_i}$ then there are q exponents α_i such that $0 \leq \alpha_i \leq p-1$, q exponents α_i such that $p \leq \alpha_i \leq 2p-1, \ldots$, and q exponents α_i such that $p^2 - p \leq \alpha_i \leq p^2-1$. If $F_p(x)$ divides $\sum_{i=1}^{pq} x^{\alpha_i}$ there are q exponents α_i congruent to 0, to 1, ..., and to p-1 modulo p. Now from the above any given exponent occurs q times or in multiples of r. Since r does not divide q the second case cannot arise. Hence b is a period of A.

This completes the proof.

THEOREM 3.5 If G is a group of type $\{p, q, r, s\}$, where p, q, r and s are distinct primes, then G is good.

Proof. Let a, b, c and d be generators of G of orders p, q, r and s respectively. Let ρ, σ, τ and ω be primitive roots f unity of orders p, q, r and s respectively.

Let AB = G. The essentially different cases to be considered are those in which A has p elements and pq elements.

The first of these is covered by Theorem 3.2.

Let A have pq elements. Then B has rs elements. Let $A = \sum_{i=1}^{pq} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i}$ and $B = \sum_{i=1}^{rs} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}$. It is assumed that $\alpha_1 = \beta_1 = \gamma_1 = \delta_1 = \lambda_1 = \mu_1 = \nu_1 = \theta_1 = 0$. Then, it can be shown as before in the proof of Theorem 3.4, that the numbers α_i are

$0, 1, \ldots, p-1$, each occurring q times, that the numbers β_i are $0, 1, \ldots, q-1$, each occurring p times, that the numbers ν_i are $0, 1, \ldots, r-1$, each occurring s times and that the numbers θ_i are $0, 1, \ldots, s-1$, each occurring r times.

When a, b, c and d are replaced by roots of unity of suitable orders, in AB = G, products of sums of complex numbers equal to zero are obtained. Use will be made of the fact that one or other of the corresponding sums arising from A and from B is zero in each case. It may be assumed, without loss of generality, that

$$\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} \omega^{\delta_i} = 0.$$

G is shown to be good by consideration of the various combinations of sums of products of two roots of unity, one ρ or σ the other τ or ω, equal to zero.

$$(1) \qquad \sum_{i=1}^{pq} \rho^{\alpha_i} \tau^{\gamma_i} = 0$$

implies that $F_p(x) \mid \sum_{i=1}^{pq} x^{\alpha_i} \tau^{\gamma_i}$ and so that

$$\sum_{i;\alpha_i=0} \tau^{\gamma_i} = \sum_{i;\alpha_i=1} \tau^{\gamma_i} = \ldots = \sum_{i;\alpha_i=p-1} \tau^{\gamma_i}.$$

Since there are q terms in each of these sums, there must be precisely the same powers of τ occurring in each sum. Therefore, if (1) holds, the numbers γ_i consist of q blocks, each block containing p equal elements.

Similarly,

$$(2) \qquad \sum_{i=1}^{pq} \rho^{\alpha_i} \omega^{\delta_i} = 0$$

implies that δ_i consists of q blocks of p equal elements,

$$(3) \qquad \sum_{i=1}^{pq} \sigma^{\beta_i} \tau^{\gamma_i} = 0$$

implies that γ_i consists of p blocks of q equal elements,

(4) $\sum_{i=1}^{pq} \sigma^{\beta_i} \omega^{\delta_i} = 0$

implies that δ_i consists of p blocks of q equal elements,

(5) $\sum_{i=1}^{rs} \rho^{\lambda_i} \tau^{\nu_i} = 0$

implies that λ_i consists of s blocks of r equal elements,

(6) $\sum_{i=1}^{rs} \rho^{\lambda_i} \omega^{\theta_i} = 0$

implies that λ_i consists of r blocks of s equal elements,

(7) $\sum_{i=1}^{rs} \sigma^{\mu_i} \tau^{\nu_i} = 0$

implies that μ_i consists of s blocks of r equal elements, and

(8) $\sum_{i=1}^{rs} \sigma^{\mu_i} \omega^{\theta_i} = 0$

implies that μ_i consists of r blocks of s equal elements.

From AB = G it follows that (1) or (5) is true, (2) or (6) is true, (3) or (7) is true and (4) or (8) is true. The possible combinations of these are now considered.

(i) (1), (2), (3) and (4) true.

(1) and (3) imply that all γ_i are equal. (2) and (4) imply that all δ_i are equal. Since no element can occur twice in A and there are only pq different pairs (α_i, β_i) each of these pairs must be present precisely once. It follows that ab is a period of A.

(ii) (1), (2) and (3) true

(1) and (3) imply that all γ_i are equal and so that $\gamma_i = 0$ for all i. Therefore from $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} \omega^{\delta_i} = 0$ it follows that $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \omega^{\delta_i} = 0$. Therefore $F_q(x)$ divides $\sum_{i=1}^{pq} \rho^{\alpha_i} \omega^{\delta_i} x^{\beta_i}$.

It follows that

$$\sum_{i;\beta_i=0} \rho^{\alpha_i}\omega^{\delta_i} = \sum_{i;\beta_i=1} \rho^{\alpha_i}\omega^{\delta_i} = \ldots = \sum_{i;\beta_i=q-1} \rho^{\alpha_i}\omega^{\delta_i}.$$

But, from (2), $\sum_{i=1}^{pq} \rho^{\alpha_i}\omega^{\delta_i} = 0$. Therefore for each k, k = 0, 1, ..., q-1, $\sum_{i;\beta_i=k} \rho^{\alpha_i}\omega^{\delta_i} = 0$. But β_i takes the value k, p times. Therefore, from $F_p(x) \mid \sum_{i;\beta_i=k} \omega^{\delta_i} x^{\alpha_i}$ it follows that the numbers α_i in each such sum are 0, 1, ..., p-1 and that all δ_i in each sum are equal.

Hence a is a period of A.

(iii) The other cases involving three of the first four relationships being true are similar to (ii).

(iv) (1), (3), (6) and (8) true.

(1) and (3) imply that $\gamma_i = 0$ for all i.

If $\sum_{i=1}^{pq} \rho^{\alpha_i}\tau^{\gamma_i}\omega^{\delta_i} = 0$ then, since $\gamma_i = 0$, $\sum_{i=1}^{pq} \rho^{\alpha_i}\omega^{\delta_i} = 0$ which is (2). (1), (2) and (3) imply that A is periodic, from (ii). Similarly if $\sum_{i=1}^{pq} \sigma^{\beta_i}\tau^{\gamma_i}\omega^{\delta_i} = 0$ then, since $\gamma_i = 0$, $\sum_{i=1}^{pq} \sigma^{\beta_i}\omega^{\delta_i} = 0$, which is (4). (1), (3) and (4) imply that A is periodic, from (iii). Thus it may be assumed that $\sum_{i=1}^{rs} \rho^{\lambda_i}\tau^{\nu_i}\omega^{\theta_i} = 0$ and that $\sum_{i=1}^{rs} \sigma^{\mu_i}\tau^{\nu_i}\omega^{\theta_i} = 0$. It follows from these that

$$\sum_{i;\nu_i=0} \rho^{\lambda_i}\omega^{\theta_i} = \ldots = \sum_{i;\nu_i=r-1} \rho^{\lambda_i}\omega^{\theta_i}$$

and that

$$\sum_{i;\nu_i=0} \sigma^{\mu_i}\omega^{\theta_i} = \ldots = \sum_{i;\nu_i=r-1} \sigma^{\mu_i}\omega^{\theta_i}.$$

It follows from (6) and (8) that $\sum_{i;\nu_i=k} \rho^{\lambda_i}\omega^{\theta_i} = \sum_{i;\nu_i=k} \sigma^{\mu_i}\omega^{\theta_i} = 0$ for k = 0, 1, ..., r-1. But there are s terms in each sum. Therefore, from $F_s(x) \mid \sum_{i;\nu_i=k} \rho^{\lambda_i} x^{\theta_i}$ and $F_s(x) \mid \sum_{i;\nu_i=k} \sigma^{\mu_i} x^{\theta_i}$ it follows that the numbers θ_i occurring in each sum are 0, 1, ..., s-1 and that all λ_i and all μ_i in each sum are equal. Thus d is a period of B.

(v) (2), (4), (5) and (7) true is similar to (iv).

(vi) (5), (6), (7) and (8) true is similar to (i).

(vii) (5), (6) and (7) true.

It may be assumed that (8) is not true and thus that (4) is true. From (5) and (6) it follows that all $\lambda_i = 0$. It follows that if $\sum_{i=1}^{rs} \rho^{\lambda_i} \sigma^{\mu_i} \omega^{\theta_i} = 0$ then $\sum_{i=1}^{rs} \sigma^{\mu_i} \omega^{\theta_i} = 0$, which is (8). Therefore it may be assumed that $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \omega^{\delta_i} = 0$.

If $\sum_{i=1}^{rs} \sigma^{\mu_i} \tau^{\nu_i} \omega^{\theta_i} = 0$ then it follows that

$$\sum_{i;\theta_i=0} \sigma^{\mu_i} \tau^{\nu_i} = \dots = \sum_{i;\theta_i=s-1} \sigma^{\mu_i} \tau^{\nu_i}.$$

From (7) it follows that $\sum_{i;\theta_i=k} \sigma^{\mu_i} \tau^{\nu_i} = 0$, for k = 0, 1, ..., s-1. But there are r terms in each sum. Therefore, from $F_r(x) \mid \sum_{i;\theta_i=k} \sigma^{\mu_i} x^{\nu_i}$, the numbers ν_i in each sum are 0, 1, ..., r-1 and the numbers μ_i in each sum are all equal. Hence c is a period of B.

Therefore it may be assumed that $\sum_{i=1}^{pq} \sigma^{\beta_i} \tau^{\gamma_i} \omega^{\delta_i} = 0$. The following sums derived from A can now be taken to be zero:

$$\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} \omega^{\delta_i}, \sum_{i=1}^{pq} \sigma^{\beta_i} \tau^{\gamma_i} \omega^{\delta_i}, \sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \omega^{\delta_i}, \sum_{i=1}^{pq} \sigma^{\beta_i} \omega^{\delta_i}.$$

From the last two of these it follows, by a now familiar argument, that $\sum_{i;\alpha_i=k} \sigma^{\beta_i} \omega^{\delta_i} = 0$ for k = 0, 1, ..., p-1. There are q terms in each such sum and therefore the numbers β_i are 0, 1, ..., q-1 and the numbers δ_i are all equal in each sum. From the first two sums above it follows, by a similar argument, that $\sum_{i;\alpha_i=k} \sigma^{\beta_i} \tau^{\gamma_i} \omega^{\delta_i} = 0$ for k = 0, 1, ..., q-1. But from the above the numbers β_i in each such sum are 0, 1, ..., q-1 and all the numbers δ_i are equal. It follows that the numbers γ_i in each such sum are also equal. Therefore b is a period of A.

(viii) The other cases with three of (5), (6), (7) and (8) true are similar to (vii).

(ix) (1), (2), (7) and (8) true.

From (7) and (8) it follows that $\mu_i = 0$ for all i. If $\sum_{i=1}^{rs} \rho^{\lambda_i} \sigma^{\mu_i} \tau^{\nu_i} = 0$ or $\sum_{i=1}^{rs} \rho^{\lambda_i} \sigma^{\mu_i} \omega^{\theta_i} = 0$ it follows that (5) or (6) hold true and thus by (viii) that A or B is periodic. Therefore it may be assumed that $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} = 0$ and that $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \omega^{\delta_i} = 0$. It follows from these that

$$\sum_{i;\beta_i=0} \rho^{\alpha_i} \tau^{\gamma_i} = \dots = \sum_{i;\beta_i=q-1} \rho^{\alpha_i} \tau^{\gamma_i} \quad \text{and}$$

$$\sum_{i;\beta_i=0} \rho^{\alpha_i} \omega^{\delta_i} = \dots = \sum_{i;\beta_i=q-1} \rho^{\alpha_i} \omega^{\delta_i} .$$

Therefore, from (1) and (2), $\sum_{i;\beta_i=k} \rho^{\alpha_i} \tau^{\gamma_i} = \sum_{i;\beta_i=k} \rho^{\alpha_i} \omega^{\delta_i} = 0$ for k = 0, 1, .., q-1. Since there are p elements in each sum it follows that the numbers α_i in each sum are 0, 1, ..., p-1 and that all γ_i and all δ_i in each sum are equal. Thus a is a period of A.

(x) (3), (4), (5) and (6) true is similar to (ix).

(xi) (1), (4), (6) and (7) true.

Suppose that $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} = 0$. From this and (1) it follows, by a familiar argument, that $\sum_{i;\beta_i=k} \rho^{\alpha_i} \tau^{\gamma_i} = 0$ for k = 0, 1, ..., q-1. Since there are p terms in each sum it follows that all γ_i in each sum are equal and that the numbers α_i in each sum are 0, 1, ..., p-1. Also from $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} \omega^{\delta_i} = 0$ and $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} = 0$ it follows that $\sum_{i;\delta_i=k} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} = 0$ for k = 0, 1, ..., s-1. By

(4) each δ_i occurs a multiple of q times, say $h_k q$ times for $\delta_i = k$, and that the numbers β_i occurring with it are 0, 1, ..., q-1 each occurring h_k times. Now, if for some k, $h_k = p$, then all δ_i are equal, and so equal to zero, and $\sum_{i=1}^{pq} \rho^{\alpha_i} \omega^{\delta_i} = 0$ which is (2). Then, from (1), (2) and (4), A is periodic by (iii). It may be assumed that $h_k < p$ for each k. From $\sum_{i;\delta_i = k} \rho^{\alpha_i} \sigma^{\beta_i} \tau^{\gamma_i} = 0$ it follows that

$$\sum_{i;\delta_i = k, \beta_i = 0} \rho^{\alpha_i} \tau^{\gamma_i} = \ldots = \sum_{i;\delta_i = k, \beta_i = q-1} \rho^{\alpha_i} \tau^{\gamma_i}.$$

But it is known that in each sum $\beta_i = k$, all γ_i are equal, say to γ'_k. It follows that

$$\tau^{\gamma'_0} \sum_{i;\delta_i = k, \beta_i = 0} \rho^{\alpha_i} = \ldots = \tau^{\gamma'_{q-1}} \sum_{i;\delta_i = k, \beta_i = q-1} \rho^{\alpha_i}.$$

Therefore for each pair l, m with $0 \leq l < q$, $0 \leq m < q$, $F_s(x)$ divides $x^{\gamma'_l} \sum_{i;\delta_i = k, \beta_i = l} \rho^{\alpha_i} - x^{\gamma'_m} \sum_{i;\delta_i = k, \beta_i = m} \rho^{\alpha_i}$. If s ≠ 2, this polynomial is zero. But, since $h_k < p$ and there are h_k terms, $\sum_{i;\delta_i = k, \beta_i = l} \rho^{\alpha_i} \neq 0$. Therefore $\gamma'_l = \gamma'_m$. It follows that all γ'_i and so that all γ_i are equal. If s = 2 and $\gamma'_l \neq \gamma'_m$ then $\sum_{i;\delta_i = k, \beta_i = l} \rho^{\alpha_i} + \sum_{i;\delta_i = k, \beta_i = m} \rho^{\alpha_i} = 0$. But since s = 2, p is odd and so does not divide $2h_k$. Therefore this is impossible and so all γ_i are equal.

Therefore $\sum_{i=1}^{pq} \sigma^{\beta_i} \tau^{\gamma_i} = \sum_{i=1}^{pq} \sigma^{\beta_i} = 0$, which is (3). From (1), (3) and (4) A is periodic by (iii).

Similarly it can be shown that if $\sum_{i=1}^{pq} \rho^{\alpha_i} \sigma^{\beta_i} \omega^{\delta_i} = 0$ then A is periodic. Therefore it may be assumed that $\sum_{i=1}^{rs} \rho^{\lambda_i} \sigma^{\mu_i} \tau^{\nu_i} = 0$ and that $\sum_{i=1}^{rs} \rho^{\lambda_i} \sigma^{\mu_i} \omega^{\delta_i} = 0$. Now from (7) and $\sum_{i=1}^{rs} \rho^{\lambda_i} \sigma^{\mu_i} \tau^{\nu_i} = 0$

it follows that $\sum_{i;\lambda_i=k} \sigma^{\mu_i}\tau^{\nu_i} = 0$ for k = 0, 1, ..., p-1. But from (6) it follows that each λ_i occurs a multiple of s times, say $h_k s$ times for $\lambda_i = k$. If $h_k = r$, for some k, then all λ_i are equal and so (5) is true. (5), (6) and (7) imply A or B periodic by (vii). Thus it may be assumed that $h_k < r$ for all k. For some k, $h_k > 0$. Then from $\sum_{i;\lambda_i=k} \sigma^{\mu_i}\tau^{\nu_i} = 0$ it follows that $F_{qr}(x)$ divides $\sum_{i;\lambda_i=k} x^{\kappa_i}$, where $0 \leq \kappa_i < qr$ and $\kappa_i \equiv \mu_i \pmod{q}$, $\kappa_i \equiv \nu_i \pmod{r}$. Therefore by Theorem 2 of (2, p. 374)

$$\sum_{i;\lambda_i=k} x^{\kappa_i} = \frac{x^{qr}-1}{x^q-1} f_q(x) + \frac{x^{qr}-1}{x^r-1} f_r(x)$$

where $f_q(x)$ and $f_r(x)$ have non-negative integral coefficients. Substituting x = 1 it follows that $h_k s = m_1 q + n_1 r$ where $m_1 = f_r(1) \geq 0$ and $n_1 = f_q(1) \geq 0$. If $m_1 = 0$ then r divides h_k, which is not possible with $0 < h_k < r$. Therefore $m_1 > 0$. Summing over all k it follows that $\sum h_k s = rs = mq + nr$ where $m > 0$. From this it is seen that r divides m and therefore $m \geq r$. But $rs \geq mq$. It follows that q is less than s. Similarly, using $\sum_{i=1}^{rs} \rho^{\lambda_i}\sigma^{\mu_i}\omega^{\theta_i} = 0$ and (6) it can be shown that A or B is periodic or that p < r.

If $\sum_{i=1}^{pq} \rho^{\alpha_i}\tau^{\gamma_i}\omega^{\delta_i} = 0$ then, since $\sum_{i=1}^{pq} \rho^{\alpha_i}\tau^{\gamma_i} = 0$, the same argument can be used again and it is found that A or B is periodic or that r < q. If $\sum_{i=1}^{pq} \sigma^{\beta_i}\tau^{\gamma_i}\omega^{\delta_i} = 0$ then, since $\sum_{i=1}^{pq} \sigma^{\beta_i}\omega^{\delta_i} = 0$, it can be similarly shown that A or B is periodic or that s < p.

But it is not possible that q < s < p < r < q. It follows that $\sum_{i=1}^{pq} \rho^{\alpha_i}\tau^{\gamma_i}\omega^{\delta_i} \neq 0$ or that $\sum_{i=1}^{pq} \sigma^{\beta_i}\tau^{\gamma_i}\omega^{\delta_i} \neq 0$. From the symmetry of this case in p and q it may be assumed, without loss of generality, that $\sum_{i=1}^{rs} \rho^{\lambda_i} \tau^{\nu_i} \omega^{\theta_i} = 0$. From (6) it follows that $\sum_{i;\nu_i=k} \rho^{\lambda_i} \omega^{\theta_i} = 0$ for k = 0, 1, ..., r-1. Since there are s elements in each sum it follows, as before, that all λ_i in each sum are equal, say to λ'_k and that the numbers θ_i in each sum are 0, 1, ..., s-1. But $\sum_{i=1}^{rs} \rho^{\lambda_i} \sigma^{\mu_i} \tau^{\nu_i} = 0$.

Therefore

$$\sum_{i;\nu_i=0} \rho^{\lambda_i} \sigma^{\mu_i} = \dots = \sum_{i;\nu_i=r-1} \rho^{\lambda_i} \sigma^{\mu_i}$$

But, from above, all λ_i in each sum are equal. Hence

$$\rho^{\lambda'_0} \sum_{i;\nu_i=0} \sigma^{\mu_i} = \dots = \rho^{\lambda'_{r-1}} \sum_{i;\nu_i=r-1} \sigma^{\mu_i}.$$

Since there are s terms in each sum and q does not divide s no sum is zero. Therefore, as before, $\lambda'_0 = \lambda'_1 = \dots = \lambda'_{r-1}$. It follows that all λ_i are equal and so that $\sum_{i=1}^{rs} \rho^{\lambda_i} \tau^{\nu_i} = 0$, which is (5). From (5), (6) and (7) A or B is periodic by (vii).

(xii) (2), (3), (5) and (8) true is similar to (xi).

This completes the proof.

It had previously been shown that the groups of type $\{p^\lambda\}$, $\{p^\lambda, q\}$ and $\{p, q, r\}$, where p, q and r are distinct primes, are good.* Each of these results is an immediate consequence of Theorem 3.2.

*- See Hajós (6), Rédei (9) and de Bruijn (2).

CHAPTER IV

Introduction

The following is the list of types of groups which have not yet been shown to be good or bad, as given by de Bruijn in (1, p.259):

$\{2^\lambda, 2\}$ $(\lambda > 1)$; $\{2^\lambda, 2, 2\}$ $(\lambda > 1)$; $\{2^2, 2, 2, 2\}$; $\{2^2, 2^2\}$;
$\{p^\lambda, 2, 2\}$; $\{p, 2^2, 2\}$; $\{p, 2, 2, 2\}$; $\{p^2, 2, 2, 2\}$;
$\{p, 2, 2, 2, 2\}$; $\{p, q, 2, 2\}$; $\{2, 3, 3\}$; $\{p, 3, 3\}$ $(p > 3)$;
$\{3^2, 3\}$:

where p and q are distinct odd primes.

It has been shown in Chapter II that the groups of type $\{p^\lambda, 2, 2\}$ and $\{2^\lambda, 2, 2\}$ are bad whenever $\lambda \geq 4$. It is the purpose of this chapter to show that the remaining groups listed above are good.

Good Non-Cyclic Groups

THEOREM 4.1 The groups of type $\{2, 3, 3\}$ and $\{3^2, 3\}$ are good.

Proof. This follows immediately from Lemma 3.1.

The following lemma, which is similar to Lemma 3.1, is useful in shortening many of the proofs for groups with subgroups of type $\{2, 2\}$.

LEMMA 4.2 If G is a group, AB = G, A has four elements and two of these elements have a common square then A or B is periodic.

Proof. Let the elements of A be (a, b, c, d) with $a^2 = b^2$.

Then

(1) $(a, b, c, d)\ B = G$

Multiplying (1) by a and by b it follows that

(2) $(a^2, ab, ac, ad)\ B = G$,

(3) $(ab, b^2, bc, bd)\ B = G$

Comparing (2) and (3) and using $a^2 = b^2$, it follows that $(ac, ad)\ B = (bc, bd)\ B$. Now if $ac\,B$ and $bc\,B$ have an element in common so also do $a\,B$ and $b\,B$, which contradicts (1). Therefore $ac\,B = bd\,B$ and $ad\,B = bc\,B$. Thus B is periodic or $ac = bd$ and $ad = bc$. In the latter case

$$ab^{-1}A = (a^2b^{-1}, a, ab^{-1}c, ab^{-1}d) = (b^2b^{-1}, a, b^{-1}bd, b^{-1}bc) = (b, a, d, c),$$

and so A is periodic.

This completes the proof.

THEOREM 4.3 If G is a group of type $\{2^2, 2, 2, 2\}$ then G is good.

Proof. Let a be an element of G of order four. Then the square of any element of G is either a^2 or e. Let $AB = G$. It may be assumed that A has two or four elements. If A has two elements then, by Lemma 3.1, A or B is periodic. If A has four elements, then, since there are only two squares in G, two elements of A must have a common square. Therefore, by Lemma 4.2, A or B is periodic.

This completes the proof.

THEOREM 4.4 The group G of type $\{2^2, 2^2\}$ is good.

Proof. Let a and b generate G with $a^4 = b^4 = e$. Let $AB = G$. If A has two elements then, by Lemma 3.1, A or B is periodic. It may be supposed that A and B have each four elements. By Lemma 4.2, if a factorisation exists in which A and B are both non-periodic, then no two elements of A and no two elements of B have a common square. There are only four squares in G, namely e, a^2, b^2 and a^2b^2. It follows that the squares of the elements of A and of B must take these once each. Let

$$A = \sum a^{\alpha_i} b^{\beta_i} \quad \text{and} \quad B = \sum a^{\lambda_i} b^{\mu_i}.$$

Then, from $AB = G$, it follows that

$$(\sum x^{\alpha_i})(\sum x^{\lambda_i}) \equiv 4(1+x+x^2+x^3)(\mathrm{mod}(x^4-1)).$$

Therefore $F_4(x) = (x^2+1)$ divides $\sum x^{\alpha_i}$ or $\sum x^{\lambda_i}$. It may be assumed without loss of generality that $(x^2+1) \mid \sum x^{\alpha_i}$. Then the numbers α_i are 0,0,2,2 or 0,1,2,3. From the form of the squares of A they must be 0,1,2,3. Now if $a^3 = c$ then $c^3 = a$ and if $b^3 = d$ then $d^3 = b$. Thus, by renaming generators if necessary, it may be assumed that A has the form $e, a.(e \text{ or } b^2), a^2b, a^3.(b \text{ or } b^3)$. The four possible cases are considered. Now if g_1 and g_2 are different elements of A then $g_1 g_2^{-1}$ cannot occur in B. Otherwise g_1 occurs twice in AB as $g_1 = (g_1)(e) = (g_2)(g_1 g_2^{-1})$. If A is e, a, a^2b, a^3b then, letting $g_1 = e, g_2 = a^3b$; $g_1 = a^3b, g_2 = e$; $g_1 = a, g_2 = a^2b$; $g_1 = a^2b, g_2 = a$, it follows that B can have no element whose square is a^2b^2;

if A is e, ab^2, a^2b, a^3b then, letting $g_1 = e, g_2 = ab^2$; $g_1 = ab^2, g_2 = e$; $g_1 = a^2b, g_2 = a^3b$; $g_1 = a^3b, g_2 = a^2b$, it follows that B can have no element whose square is a^2: if A is e, a, a^2b, a^3b^3 then, letting $g_1 = e, g_2 = a$; $g_1 = a, g_2 = e$; $g_1 = a^2b, g_2 = a^3b^3$; $g_1 = a^3b^3, g_2 = a^2b$, it follows that B can have no element whose square is a^2: finally if A is e, ab^2, a^2b, a^3b^3 then, letting $g_1 = e, g_2 = a^3b^3$; $g_1 = a^3b^3, g_2 = e$; $g_1 = ab^2, g_2 = a^2b$; $g_1 = a^2b, g_2 = ab^2$, it follows that B can have no element whose square is a^2b^2. Therefore no factorisation exists in which A and B are both non-periodic. It follows that G is good.

THEOREM 4.5 If G is a group of type $\{2^\lambda, 2, 2\}$ and $AB = G$, where A has four elements, then A or B is periodic.

Proof. Let $2^{\lambda-1} = m$. Let a, b and c generate G where $a^{2m} = b^2 = c^2 = e$. Let

$$A = \sum a^{\alpha_i} b^{\beta_i} c^{\gamma_i} = \sum a^{\alpha_i + m\beta_i} (a^m b)^{\beta_i} c^{\gamma_i}$$

$$= \sum a^{\alpha_i + m\gamma_i} b^{\beta_i} (a^m c)^{\gamma_i} = \sum a^{\alpha_i + m\beta_i + m\gamma_i} (a^m b)^{\beta_i} (a^m c)^{\gamma_i} .$$

Let $B = \sum a^{\lambda_i} b^{\mu_i} c^{\nu_i}$. If two elements of common square occur in A then, by Lemma 4.2, A or B is periodic. Therefore it may be assumed that no two exponents α_i are congruent modulo m.

From $AB = G$ it follows that

$$(\sum_{i=1}^{4} x^{\alpha_i})(\sum_{i=1}^{2m} x^{\lambda_i}) \equiv 4(1+x+\cdots+x^{2m-1})(\bmod (x^{2m}-1)).$$

Therefore $F_{2m}(x) = x^m+1$ divides $\sum_{i=1}^{4} x^{\alpha_i}$ or $\sum_{i=1}^{2m} x^{\lambda_i}$. Since the degree of $\sum_{i=1}^{4} x^{\alpha_i}$ is less than $2m$, it follows that if $(x^m+1) \mid \sum_{i=1}^{4} x^{\alpha_i}$ then if x^{n_1} occurs in the polynomial so does x^{n_1+m} . But it has been assumed that this is not so. Thus $x^m + 1$ divides $\sum_{i=1}^{2m} x^{\lambda_i}$. Similarly it can be shown that $x^m + 1$ divides $\sum_{i=1}^{2m} x^{\lambda_i+m\mu_i}$, $\sum_{i=1}^{2m} x^{\lambda_i+m\nu_i}$ and $\sum_{i=1}^{2m} x^{\lambda_i+m\mu_i+m\nu_i}$.

These results are now used to show that a^m is a period of B.

The following notation is used: $(k_1, l_1, m_1) \equiv (k_2, l_2, m_2)$ modulo (2m, 2, 2) is defined to mean $k_1 \equiv k_2 (\bmod 2m)$, $l_1 \equiv l_2 (\bmod 2)$ and $m_1 \equiv m_2 (\bmod 2)$. It is shown that (m, 0, 0) is a period under addition of the three-tuples $(\lambda_i, \mu_i, \nu_i)$ modulo (2m, 2, 2).

Suppose that k occurs in the exponents λ_i . Since no element occurs twice in B, k can occur at most four times. Let k occur four times. Then (k, 0, 0), (k, 0, 1), (k, 1, 0) and (k, 1, 1) must be the corresponding three-tuples. Since $(x^m+1) \mid \sum_{i=1}^{2m} x^{\lambda_i}$ the numbers λ_i have m as a period modulo 2m. Therefore k + m also occurs four times. It follows that the corresponding three-tuples must be (k+m, 0, 0), (k+m, 0, 1), (k+m, 1, 0) and (k+m, 1, 1). (m, 0, 0) is clearly a period of these sets modulo (2m, 2, 2).

Let k occur precisely three times among the exponents λ_i. Let (k, l, n) be the missing three-tuple. As above, since k occurs three times precisely so also does k + m in the numbers λ_i In the numbers $\lambda_i + m\mu_i$, $k+m(l+1)$ occurs twice and k + m l once from $\lambda_i = k$. The only other λ_i giving rise to these two numbers is $k + m$. Therefore from $(k+m, \mu_i, \nu_i)$, $k+m(l+1)$ occurs once and $k + m\ l$ twice, since $\lambda_i + m\mu_i$ has also m as a period modulo $2m$. It follows that l occurs once and $(l+1)$ twice with $k + m$. Similarly, using $\lambda_i + m\nu_i$, it can be shown that n occurs once and $(n+1)$ twice with $k + m$. It is easily seen that $(k+m, l, n+1)$, $(k+m, l+1, n)$ and $(k+m, l+1, n+1)$ must be the three-tuples occurring. Hence $(m, 0, 0)$ is again a period of these sets modulo $(2m, 2, 2)$.

Suppose that only one k occurs among the numbers λ_i. Let the corresponding three-tuple be (k, l, n). Then, as above, precisely one $k + m$ occurs. It is easily verified that $(k+m, l, n)$ is the only three-tuple which satisfies $\lambda_i + m\mu_i$ and $\lambda_i + m\nu_i$ periodic, with period m, modulo $2m$. Hence $(m, 0, 0)$ is again a period of these sets modulo $(2m, 2, 2)$.

There remains the case in which k occurs twice among the numbers λ_i. The corresponding three-tuples may be of the form $(k, l, n), (k, l+1, n)$; $(k, l, n)(k, l, n+1)$ or $(k, l, n), (k, l+1, n+1)$. The first two of these are similar and only the first and the third cases are considered. Let (k, l, n) and $(k, l+1, n)$ occur. Then it is readily verified from λ_i that $k + m$ occurs twice, from $\lambda_i + m\nu_i$ that $(k + m, n)$ occurs twice and from $\lambda_i + m\mu_i$ that $(k+m, l)$ and $(k+m, l+1)$ occur once each. Therefore $(k+m, l, n)$ and $(k+m, l+1, n)$ occur. Hence $(m, 0, 0)$ is a period of these sets modulo $(2m, 2, 2)$. Let (k, l, n) and $(k, l+1, n+1)$ occur. Then it is readily verified as before that $k + m$ occurs twice and that $l, l+1, n, n+1$ occur with it once each. But if $(k+m, l, n+1)$ and $(k+m, l+1, n)$ occur then the numbers $\lambda_i + m\mu_i + m\nu_i$ arising from these four three-tuples are all congruent to $k+m(l+n)$ modulo 2m. But numbers congruent to k (modulo m) only arise from $\lambda_i = k$ and $\lambda_i = k+m$. Thus these sets do not give $\lambda_i + m\mu_i + m\nu_i$ periodic, with period m, modulo 2m. The only other possibility, which must therefore happen, is that the three-tuples are $(k+m, l, n)$ and $(k+m, l+1, n+1)$. These sets have (m, 0, 0) as a period modulo (2m, 2, 2).

Since (m, 0, 0) is a period in all cases, it follows that a^m is a period of B.

THEOREM 4.6 If G is a group of type $\{2^2, 2, 2\}$ or $\{2^3, 2, 2\}$ then G is good.

Proof. Let AB = G. It may be assumed that A has two or four elements. In the first case A or B is periodic by Lemma 3.1. In the second case A or B is periodic by Theorem 4.5.

THEOREM 4.7 If G is a group of type $\{2^\lambda, 2\}$ then G is good.

Proof. Let $2^{\lambda-1} = m$. Let a and b generate G with $a^{2m} = b^2 = e$. Then a and $a^m b$ also generate G. Let AB = G.

Let $A = \sum a^{\alpha_i} b^{\beta_i} = \sum a^{\alpha_i + m\beta_i} (a^m b)^{\beta_i}$ and

$$B = \sum a^{\lambda_i} b^{\mu_i} = \sum a^{\lambda_i + m\mu_i} (a^m b)^{\mu_i}.$$

From AB = G it follows that

$$(\sum x^{\alpha_i})(\sum x^{\lambda_i}) \equiv (\sum x^{\alpha_i + m\beta_i})(\sum x^{\lambda_i + m\mu_i}) \equiv (1 + x + \dots + x^{2m-1}) (\mathrm{mod}\, (x^{2m} - 1)).$$

Therefore $F_{2m}(x) = x^m + 1$ divides $\sum x^{\alpha_i}$ or $\sum x^{\lambda_i}$ and divides $\sum x^{\alpha_i + m\beta_i}$ or $\sum x^{\lambda_i + m\mu_i}$. The two essential cases to consider are that in which $F_{2m}(x)$ divides two polynomials arising from the same factor, say A, and that in which $F_{2m}(x)$ divides one polynomial arising from A and one arising from B.

Let x^m+1 divide $\sum x^{\alpha_i}$ and $\sum x^{\alpha_i+m\beta_i}$. Then the numbers α_i and the numbers $\alpha_i+m\beta_i$ are periodic, with period m, modulo 2m. If k occurs twice among the numbers α_i then so also does k + m and since no element can occur twice in A the corresponding pairs (α_i, β_i) are $(k,0), (k,1), (k+m,0)$ and $(k+m,1)$. Thus (m, 0) is a period of these numbers (α_i, β_i) modulo (2m, 2). If k occurs only once then so also does k + m. If (k, l) occurs then it is easily verified, using $\alpha_i+m\beta_i$, that $(k+m, l)$ must also occur. Thus (m, 0) is again a period of these numbers (α_i, β_i) modulo (2m, 2). It follows that in this case a^m is a period of A.

In the second case, it may be assumed, by renaming generators if necessary, that x^m+1 divides $\sum x^{\alpha_i}$ and $\sum x^{\lambda_i+m\mu_i}$. Then if (k, l) occurs among (α_i, β_i) so must $(k+m, l)$ or $(k+m, l+1)$ and if (k, l) occurs among (λ_i, μ_i) so must $(k, l+1)$ or $(k+m, l)$.

If always whenever (k, l) occurs among (λ_i, μ_i) so also does $(k, l+1)$ then b is a period of B. Let (k, l) and $(k+m, l)$ occur among (λ_i, μ_i). Let (k_1, l_1) be any pair among (α_i, β_i). If (k_1+m, l_1) occurs then $a^{k+k_1}b^{l+l_1}$ arises twice in AB as $(a^{k_1}b^{l_1})(a^{k}b^{l})$ and as $(a^{k_1+m}b^{l_1})(a^{k+m}b^{l})$. But this is not possible. Therefore (k_1+m, l_1+1) occurs among (α_i, β_i) whenever (k_1, l_1) occurs. It follows that a^m b is a period of A.

This completes the proof.

THEOREM 4.8 If G is a group of type $\{p, 2^2, 2\}$, where p is an odd prime, then G is good.

Proof. Let a, b and c be independent generators of G of orders p, 4 and 2 respectively. Let ρ and σ be primitive roots of unity of orders p and 4 respectively. Let $AB = G$. The essentially different cases to be considered are those in which A has two, four or eight elements.

If A has two elements then A or B is periodic by Lemma 3.1.

Let A have four elements. Then B has $2p$ elements. By Lemma 4.2 if two elements of A have a common square, then A or B is periodic. Let $A = \sum_{i=1}^{4} a^{\alpha_i} b^{\beta_i} c^{\gamma_i}$ and $B = \sum_{i=1}^{2p} a^{\lambda_i} b^{\mu_i} c^{\nu_i}$. From $AB = G$ it follows that $(\sum_{i=1}^{4} \rho^{\alpha_i})(\sum_{i=1}^{2p} \rho^{\lambda_i}) = 0$ and therefore since p does not divide 4 that $\sum_{i=1}^{2p} \rho^{\lambda_i} = 0$. Therefore $F_p(x) \mid \sum_{i=1}^{2p} x^{\lambda_i}$ and so the numbers λ_i are $0, 0, 1, 1, \dots, p-1, p-1$. They may be assumed to be in this order. Also

$$(\sum_{i=1}^{4} \rho^{\alpha_i} \sigma^{\beta_i})(\sum_{i=1}^{2p} \rho^{\lambda_i} \sigma^{\mu_i}) = 0$$

If $\sum_{i=1}^{4} \rho^{\alpha_i} \sigma^{\beta_i} = 0$ then $F_4(x)$ divides $\sum_{i=1}^{4} \rho^{\alpha_i} x^{\beta_i}$. It follows that if A contains the element $a^{\alpha} b^{\beta} c^{\gamma}$ then it also contains $a^{\alpha} b^{\beta+2} c^{\gamma'}$. But this is not possible since these two elements have a common square Therefore $\sum_{i=1}^{2p} \rho^{\lambda_i} \sigma^{\mu_i} = 0$ Similarly, it may be assumed that $\sum_{i=1}^{2p} \rho^{\lambda_i} \sigma^{\mu_i + 2\nu_i} = 0$, using a, b and b^2c as generators. It follows that $F_p(x)$ divides $\sum_{i=1}^{2p} x^{\lambda_i} \sigma^{\mu_i}$ and $\sum_{i=1}^{2p} x^{\lambda_i} \sigma^{\mu_i + 2\nu_i}$. Therefore the coefficients of $x^0, x^1, \dots, x^{p-1}$ are all equal in each polynomial. From the first polynomial it follows that

$$\sigma^{\mu_1} + \sigma^{\mu_2} = \sigma^{\mu_3} + \sigma^{\mu_4} = \dots = \sigma^{\mu_{2p-1}} + \sigma^{\mu_{2p}}$$

From $F_4(x)$ divides $x^{\mu_{2k-1}} + x^{\mu_{2k}} - x^{\mu_{2\ell-1}} - x^{\mu_{2\ell}}$ it follows that $\mu_{2k-1} \equiv \mu_{2k} + 2 \pmod 4$ and $\mu_{2\ell-1} \equiv \mu_{2\ell} + 2 \pmod 4$ or that the polynomial is zero. In the first case every coefficient in $\sum_{i=1}^{2p} x^{\lambda_i} \sigma^{\mu_i}$ must be zero and so $\mu_{2k-1} \equiv \mu_{2k} + 2 \pmod 4$ for all k. If this is not so then the second must hold for all k and ℓ and so, by re-ordering pairs if necessary, it follows that $\mu_1 = \mu_3 = \dots = \mu_{2p-1}$ and that $\mu_2 = \mu_4 = \dots = \mu_{2p}$. Similarly results hold for $\mu_i + 2\nu_i$ (mod 4) except that no re-ordering is possible if the μ_i have already been re-ordered. From these two possibilities in each case there are four possibilities to consider.

(i) $\mu_{2k-1} \equiv \mu_{2k} + 2 \pmod 4$; $\mu_{2k-1} + 2\nu_{2k-1} \equiv \mu_{2k} + 2\nu_{2k} + 2 \pmod 4$ for k = 1, 2, ..., p. Then subtracting it follows that $2\nu_{2k-1} \equiv 2\nu_k$ (mod 4) and so that $\nu_{2k-1} \equiv \nu_{2k}$ (mod 2) for k = 1, ..., p. In this case b^2 is a period of B.

(ii) $\mu_{2k-1} \equiv \mu_{2k} + 2 \pmod 4$;

$\mu_1 + 2\nu_1 \equiv \mu_3 + 2\nu_3 \equiv \dots \equiv \mu_{2p-1} + 2\nu_{2p-1} \pmod 4$ and

$\mu_2 + 2\nu_2 \equiv \mu_4 + 2\nu_4 \equiv \dots \equiv \mu_{2p} + 2\nu_{2p} \pmod 4$.

Since e is in B it may be assumed that $\mu_1 = \nu_1 = 0$ and so that $\mu_1 + 2\nu_1 = 0$. If $\mu_2 + 2\nu_2$ is odd then μ_2 is odd which is not consistent with $\mu_1 \equiv \mu_2 + 2 \pmod 4$. Then

$\mu_{2k-1} + 2\nu_{2k-1} - \mu_{2k} - 2\nu_{2k} \equiv 0$ (mod 4) for all k or

$\mu_{2k-1} + 2\nu_{2k-1} - \mu_{2k} - 2\nu_{2k} \equiv 2$ (mod 4) for all k.

Subtracting $\mu_{2k-1} - \mu_{2k} - 2 \equiv 0$ (mod 4) it follows in the first case that $2\nu_{2k-1} - 2\nu_{2k} + 2 \equiv 0$ (mod 4) and so that $\nu_{2k-1} + 1 \equiv \nu_{2k}$ (mod 2) and in the second case that $2\nu_{2k-1} - 2\nu_{2k} \equiv 0$ (mod 4) and so that $\nu_{2k-1} - \nu_{2k} \equiv 0 \ (\mathrm{mod}\ 2)$ for all k. In the first case b^2c is a period of B and in the second case b^2 is a period of B.

(iii) $\mu_1 = \mu_3 = \dots = \mu_{2p-1}; \mu_2 = \mu_4 = \dots = \mu_{2p}; \mu_{2k-1} + 2\nu_{2k-1} \equiv \mu_{2k} + 2\nu_{2k} + 2 \ (\mathrm{mod}\ 4)$ is similar to (ii).

(iv) $\mu_1 = \mu_3 = \dots = \mu_{2p-1}; \mu_2 = \mu_4 = \dots = \mu_{2p};$

$\mu_{2k-1} + 2\nu_{2k-1} \equiv l$ or $m \ (\mathrm{mod}\ 4)$ and $\mu_{2k} + 2\nu_{2k} \equiv m$ or $l \ (\mathrm{mod}\ 4)$ in the sense that if, for some k, one is l then the other is m. If 1 = m, then $\nu_1 = \nu_3 = \dots = \nu_{2p-1}$; $\nu_2 = \nu_4 = \dots = \nu_{2p}$ and a is a period of B. Now if $l \equiv m+2 \ (\mathrm{mod}\ 4)$ then

$$\mu_{2k-1} + 2\nu_{2k-1} - \mu_{2k} - 2\nu_{2k} \equiv 2 \ (\mathrm{mod}\ 4)$$

and so by (iii) B is periodic. Thus it may be assumed that l and m are of different parity. For some k_1, let $\mu_{2k_1} + 2\nu_{2k_1} \equiv l \ (\mathrm{mod}\ 4)$ Then $2\nu_{2k_1} \equiv l - \mu_{2k_1} \equiv l - \mu_2 \ (\mathrm{mod}\ 4)$. If for some k_2 $\mu_{2k_2} + 2\nu_{2k_2} \equiv m \ (\mathrm{mod}\ 4)$ then $2\nu_{2k_2} \equiv m - \mu_2 \ (\mathrm{mod}\ 4)$. It follows that $m - \mu_2$ and $l - \mu_2$ are both even. But this contradicts m and l having different parity. Therefore all $\mu_{2k} + 2\nu_{2k}$ are congruent modulo 4 and so also are all $\mu_{2k-1} + 2\nu_{2k-1}$. But since all μ_{2k-1} are equal and all μ_{2k} are equal it follows that all $2\nu_{2k-1}$ and all $2\nu_{2k}$ are equal mod 4 and so that all ν_{2k-1} and all ν_{2k} are equal mod 2. Therefore a is a period of B.

Let A have eight elements. Then B has p elements. Let $A = \sum_{i=1}^{8} a^{\alpha_i} b^{\beta_i} c^{\gamma_i}$ and $B = \sum_{i=1}^{p} a^{\lambda_i} b^{\mu_i} c^{\nu_i}$. Then, as before, $F_p(x)$ divides $\sum_{i=1}^{p} x^{\lambda_i}$ and the numbers λ_i are 0, 1, ..., p-1. Also, by a similar argument, $\sum_{i=1}^{8} \sigma^{\beta_i} = \sum_{i=1}^{8} \sigma^{\beta_i+2\gamma_i} =$

$$= \sum_{i=1}^{8} (-1)^{\beta_i} = \sum_{i=1}^{8} (-1)^{\beta_i+2\gamma_i} = \sum_{i=1}^{8} (-1)^{\gamma_i} = \sum_{i=1}^{8} (-1)^{\beta_i+\gamma_i} = 0 .$$

Therefore $F_4(x)$ divides $\sum_{i=1}^{8} x^{\beta_i}$ and $\sum_{i=1}^{8} x^{\beta_i+2\gamma_i}$ and $F_2(x)$ divides $\sum_{i=1}^{8} x^{\beta_i}$, $\sum_{i=1}^{8} x^{\beta_i+2\gamma_i}$, $\sum_{i=1}^{8} x^{\gamma_i}$ and $\sum_{i=1}^{8} x^{\beta_i+\gamma_i}$. Therefore $F_4(x) \cdot F_2(x) = (1+x+x^2+x^3)$ divides $\sum_{i=1}^{8} x^{\beta_i}$ and $\sum_{i=1}^{8} x^{\beta_i+2\gamma_i}$ and so the numbers β_i and the numbers $\beta_i+2\gamma_i$ (mod 4) are 0, 0, 1, 1, 2, 2, 3, 3. Also the numbers γ_i and the numbers $\beta_i+\gamma_i$ (mod 2) are 0, 0, 0, 0 1, 1, 1, 1. Let $x_{k,l}$ denote the number of times the pair (k, l) occurs among (β_i, γ_i) Then the results above about β_i and γ_i can be expressed in the following set of equations:

(1) all $\quad x_{0,0} + x_{0,1} + x_{1,0} + x_{1,1} + x_{2,0} + x_{2,1} + x_{3,0} + x_{3,1} = 8$.

(2) $\gamma_i \equiv 0 \pmod 2$ $\quad x_{0,0} + x_{1,0} + x_{2,0} + x_{3,0} = 4$.

(3) $\gamma_i \equiv 1 \pmod 2$ $\quad x_{0,1} + x_{1,1} + x_{2,1} + x_{3,1} = 4$.

(4) $\beta_i+\gamma_i \equiv 0 \pmod 2$ $\quad x_{0,0} + x_{1,1} + x_{2,0} + + x_{3,1} = 4$

(5) $\beta_i+\gamma_i \equiv 1 \pmod 2$ $\quad x_{0,1} + x_{1,0} + x_{2,1} + x_{3,0} = 4$

(6) $\beta_i \equiv 0 \pmod 4$ $\quad x_{0,0} + x_{0,1} = 2$

(7) $\beta_i \equiv 1 \pmod 4$ $\quad x_{1,0} + x_{1,1} = 2$

(8) $\beta_i \equiv 2 \pmod 4$ $\quad x_{2,0} + x_{2,1} = 2$

(9) $\beta_i \equiv 3 \pmod 4$ $\qquad x_{3,0} + x_{3,1} = 2.$

(10) $\beta_i + 2\gamma_i \equiv 0 \pmod 4$ $\qquad x_{0,0} + x_{2,1} = 2.$

(11) $\beta_i + 2\gamma_i \equiv 2 \pmod 4$ $\qquad x_{0,1} + x_{2,0} = 2.$

(12) $\beta_i + 2\gamma_i \equiv 1 \pmod 4$ $\qquad x_{1,0} + x_{3,1} = 2.$

(13) $\beta_i + 2\gamma_i \equiv 3 \pmod 4$ $\qquad x_{1,1} + x_{3,0} = 2.$

(2) + (4) + (6) + (8) - (1) gives (14), $2x_{0,0} + 2x_{2,0} = 4$

(3) + (5) + (6) + (8) - (1) gives (15), $2x_{0,1} + 2x_{2,1} = 4$

(2) + (5) + (7) + (9) - (1) gives (16), $2x_{1,0} + 2x_{3,0} = 4$

(3) + (4) + (7) + (9) - (1) gives (17), $2x_{1,1} + 2x_{3,1} = 4$

(6) and (11) give $x_{0,0} = x_{2,0}$ and from (14) $x_{0,0} = x_{2,0} = 1$

(7) and (12) give $x_{1,1} = x_{3,1}$ and from (17) $x_{1,1} = x_{3,1} = 1$

(8) and (11) give $x_{0,1} = x_{2,1}$ and from (15) $x_{0,1} = x_{2,1} = 1$

(9) and (12) give $x_{1,0} = x_{3,0}$ and from (16) $x_{1,0} = x_{3,0} = 1$

Therefore the pairs (β_i, γ_i) are $(0,0), (0,1), (1,0), (1,1), (2,0), (2,1), (3,0)$ and $(3,1)$. They are assumed to be in this order.

From AB = C it follows that

$$\sum_{i=1}^{8} \rho^{\alpha_i} \sigma^{\beta_i} \sum_{i=1}^{p} \rho^{\lambda_i} \sigma^{\mu_i} = \sum_{i=1}^{8} \rho^{\alpha_i} \sigma^{\beta_i + 2\gamma_i} \sum_{i=1}^{p} \rho^{\lambda_i} \sigma^{\mu_i + 2\nu_i}$$
$$= \sum_{i=1}^{8} \rho^{\alpha_i} (-1)^{\beta_i + \gamma_i} \sum_{i=1}^{p} \rho^{\lambda_i} (-1)^{\mu_i + \nu_i} = \sum_{i=1}^{8} \rho^{\alpha_i} (-1)^{\gamma_i} \sum_{i=1}^{p} \rho^{\lambda_i} (-1)^{\mu_i} = 0.$$

Therefore one term or the other in each product is zero If $\sum_{i=1}^{p} \rho^{\lambda_i} \sigma^{\mu_i} = 0$ then $F_p(x)$ divides $\sum_{i=1}^{p} x^{\lambda_i} \sigma^{\mu_i}$ and so all σ^{μ_i} are equal and thus all μ_i are equal and so equal to zero mod 4. If $\sum_{i=1}^{8} \rho^{\alpha_i} \sigma^{\beta_i} = 0$ then $F_4(x)$ divides $\sum_{i=1}^{8} \rho^{\alpha_i} x^{\beta_i}$ and therefore the coefficients of x^0 and x^2 are equal and the coefficients of x and x^3 are equal, i.e. $\rho^{\alpha_1} + \rho^{\alpha_2} = \rho^{\alpha_5} + \rho^{\alpha_6}$ and $\rho^{\alpha_3} + \rho^{\alpha_4} = \rho^{\alpha_7} + \rho^{\alpha_8}$. Similarly from the other products it follows that all $\mu_i + 2\nu_i \equiv 0$ (mod 4) or that $\rho^{\alpha_1} + \rho^{\alpha_6} = \rho^{\alpha_2} + \rho^{\alpha_5}$ and $\rho^{\alpha_3} + \rho^{\alpha_8} = \rho^{\alpha_4} + \rho^{\alpha_7}$; that all $\mu_i + \nu_i \equiv 0$ (mod 2) or that $\rho^{\alpha_1} + \rho^{\alpha_4} + \rho^{\alpha_5} + \rho^{\alpha_8} = \rho^{\alpha_2} + \rho^{\alpha_3} + \rho^{\alpha_6} + \rho^{\alpha_7}$; and that all $\nu_i \equiv 0$ (mod 2) or that $\rho^{\alpha_1} + \rho^{\alpha_3} + \rho^{\alpha_5} + \rho^{\alpha_7} = \rho^{\alpha_2} + \rho^{\alpha_4} + \rho^{\alpha_6} + \rho^{\alpha_8}$.

Let $\rho^{\alpha_i} = \rho_i$. If $\mu_i \equiv 0$ (mod 4) and $\nu_i \equiv 0$ (mod 2) for all i then a is a period of B.

If $\mu_i \equiv 0$ (mod 4), all i, but not all $\nu_i \equiv 0$ (mod 2) then

(18) $\rho_1 + \rho_6 = \rho_2 + \rho_5$; (19) $\rho_3 + \rho_8 = \rho_4 + \rho_7$;

(20) $\rho_1 + \rho_3 + \rho_5 + \rho_7 = \rho_2 + \rho_4 + \rho_6 + \rho_8$ and

(21) $\rho_1 + \rho_4 + \rho_5 + \rho_8 = \rho_2 + \rho_5 + \rho_6 + \rho_7$.

Then from (20) and (21) each sum of four is equal to $\frac{1}{2}(\sum_{i=1}^{8} \rho_i)$ and therefore the sums in (20) and in (21) are equal. Therefore

(22) $\rho_3 + \rho_7 = \rho_4 + \rho_8$ and (23) $\rho_1 + \rho_5 = \rho_2 + \rho_6$.

From (18) and (23) $\rho_1 = \rho_2$ and $\rho_5 = \rho_6$. From (19) and (22) $\rho_3 = \rho_4$ and $\rho_7 = \rho_8$. It follows that c is a period of A.

If all $\nu_i \equiv 0$ (mod 2) but not all $\mu_i \equiv 0$ (mod 4) then $\rho_1 + \rho_2 = \rho_5 + \rho_6$; $\rho_3 + \rho_4 = \rho_7 + \rho_8$; $\rho_1 + \rho_6 = \rho_2 + \rho_5$; $\rho_3 + \rho_8 = \rho_4 + \rho_7$.

It is easily seen from the first and third of these that $\rho_1 = \rho_5$, $\rho_2 = \rho_6$ and from the second and fourth that $\rho_3 = \rho_7$, $\rho_4 = \rho_8$. It follows that

b^2 is a period of A.

If not all $\mu_i \equiv 0 \pmod 4$ nor all $\nu_i \equiv 0 \pmod 2$ then both $\mu_i + 2\nu_i \equiv 0 \pmod 4$ and $\mu_i + \nu_i \equiv 0 \pmod 2$ do not hold. Therefore $\rho_1 + \rho_2 = \rho_5 + \rho_6$; $\rho_3 + \rho_4 = \rho_7 + \rho_8$; $\rho_1 + \rho_3 + \rho_5 + \rho_7 = \rho_2 + \rho_4 + \rho_6 + \rho_8$ and either $\rho_1 + \rho_6 = \rho_2 + \rho_5$; $\rho_3 + \rho_8 = \rho_4 + \rho_7$ or else $\rho_1 + \rho_4 + \rho_5 + \rho_8 = \rho_2 + \rho_3 + \rho_6 + \rho_7$. In the first case b^2 is a period of A by the preceding result. In the second case again each sum of four elements is $(\frac{1}{2}\sum_{i=1}^{8} \rho_i)$ and therefore $\rho_3 + \rho_7 = \rho_4 + \rho_8$ and $\rho_1 + \rho_5 = \rho_2 + \rho_6$. This leads to $\rho_1 = \rho_6, \rho_2 = \rho_5, \rho_3 = \rho_8, \rho_4 = \rho_7$ and thus b^2c is a period of A.

This completes the proof.

THEOREM 4.9 If G is a group of type $\{p, 3, 3\}$ where p is a prime, then G is good.

Proof. By Lemma 3.1, it may be assumed that p is greater than three. Let AB = G. If A has three elements, then, by Lemma 3.1, A or B is periodic. It may be assumed that A has p elements. Then B has 9 elements. Let a, b and c of orders p, 3 and 3 respectively be independent generators of G. Let ρ and ω be primitive roots of unity of orders p and 3 respectively. Let $A = \sum_{i=1}^{p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i}$ and $B = \sum_{i=1}^{9} a^{\lambda_i} b^{\mu_i} c^{\nu_i}$. Then from AB = G it follows that $(\sum_{i=1}^{p} \rho^{\alpha_i})(\sum_{i=1}^{9} \rho^{\lambda_i}) = 0$ and so that $F_p(x)$ divides $\sum_{i=1}^{p} x^{\alpha_i}$ as it cannot divide $\sum_{i=1}^{9} x^{\lambda_i}$. Therefore the numbers α_i are 0, 1, ..., p-1. Similarly $\sum_{i=1}^{9} \omega^{k\mu_i + l\nu_i} = 0$, $0 \leq k < 3$, $0 \leq l < 3$, $k + l > 0$.

Therefore these numbers $k\mu_i + l\nu_i$ are 0, 0, 0, 1, 1, 1, 2, 2, 2 (mod 3).

Let (m, n) occur $x_{m,n}$ times among the pairs (μ_i, ν_i). Then the following equations are obtained: $\sum x_{m,n} = 3$ where for each pair k and ℓ the summation is taken over those numbers m and n such that $km + ln \equiv t \pmod 3$ for t = 0, 1, 2. There are thus twenty-four equations. Any given coefficient x_{m_1,n_1} occurs 8 times, by choosing k and ℓ and determining t. If x_{m_2,n_2} occurs in the same equation as x_{m_1,n_1}, then $k(m_1-m_2) + \ell(n_1-n_2) \equiv 0 \pmod 3$. If $m_1 \neq m_2$, ℓ may be chosen as 1 or 2, and k solved for. If $n_1 \neq n_2$, k may be chosen as 1 or 2 and ℓ solved for. Thus if (m_1, n_1) is not the same as (m_2, n_2), x_{m_2,n_2} occurs twice in the same equation as x_{m_1,n_1}. Adding all equations involving x_{m_1,n_1} and subtracting $2\sum x_{m,n} = 18$, where the summation is taken over all m and n, it follows that $6x_{m_1,n_1} = 24 - 18 = 6$. Therefore $x_{m,n} = 1$. The pairs (μ_i, ν_i) are (0, 0) (0, 1) (0, 2) (1, 0) (1, 1) (1, 2) (2, 0) (2, 1) (2, 2).

From AB = G it follows also that

$$\sum_{i=1}^{p} \rho^{\alpha_i} \omega^{k\beta_i + \ell\gamma_i} \cdot \sum_{i=1}^{q} \rho^{\lambda_i} \omega^{k\mu_i + \ell\nu_i} = 0.$$

Suppose that the left hand factor is zero for two independent pairs (k_1, ℓ_1), (k_2, ℓ_2) modulo (3,3), i.e. two pairs such that $(n_1 k_1 + n_2 k_2, n_1 \ell_1 + n_2 \ell_2) \equiv (0,0)$ (mod 3,3) implies $(n_1, n_2) \equiv (0,0) \pmod{(3,3)}$. Then it follows that $k_1\beta_i + \ell_1\gamma_i \equiv 0 \pmod 3$ and that $k_2\beta_i + \ell_2\gamma_i \equiv 0$ (mod 3) for i = 0, 1, ..., p-1. Then $(k_2 k_1 - k_1 k_2)\beta_i +$ $(k_2\ell_1 - k_1\ell_2)\gamma_i \equiv 0 \pmod 3$ and $k_1\ell_1 - k_1\ell_2 \not\equiv$ (mod 3). Therefore $\gamma_i \equiv 0 \pmod 3$ for all i and hence $\beta_i \equiv 0 \pmod 3$ for all i. It follows that a is a period of A. By choosing new generators, if necessary, it may therefore be assumed that

$\sum_{i=1}^{9} \rho^{\lambda_i} \omega^{k\mu_i + l\nu_i} = 0$ for all $l \neq 0$. Consider those pairs (k, l) with $l = 1$. Let $\rho_{m,n} = \sum_{i;\mu_i = m, \nu_i = n} \rho^{\lambda_i}$. Then the following equations are obtained : $\sum_{km+n \equiv t \pmod{3}} \rho_{m,n} = \frac{1}{3} \sum_{i=1}^{9} \rho^{\lambda_i} =$ constant, where $0 \leq k < 3, 0 \leq t < 3$. Written out in full these are

$$\rho_{0,0} + \rho_{1,0} + \rho_{2,0} = \rho_{0,1} + \rho_{1,1} + \rho_{2,1} = \rho_{0,2} + \rho_{1,2} + \rho_{2,2}$$

$$= \rho_{0,0} + \rho_{1,2} + \rho_{2,1} = \rho_{0,1} + \rho_{1,0} + \rho_{2,2} = \rho_{0,2} + \rho_{1,1} + \rho_{2,0}$$

$$= \rho_{0,0} + \rho_{1,1} + \rho_{2,2} = \rho_{0,1} + \rho_{1,2} + \rho_{2,0} = \rho_{0,2} + \rho_{1,0} + \rho_{2,1} .$$

Using each column it is seen that

$$\rho_{1,0} + \rho_{2,0} = \rho_{1,2} + \rho_{2,1} = \rho_{1,1} + \rho_{2,2} = \frac{1}{3} \sum_{i;\mu_i \neq 0} \rho^{\lambda_i} .$$

$$\rho_{1,1} + \rho_{2,1} = \rho_{1,0} + \rho_{2,2} = \rho_{1,2} + \rho_{2,0} = \frac{1}{3} \sum_{i;\mu_i \neq 0} \rho^{\lambda_i} .$$

$$\rho_{1,2} + \rho_{2,2} = \rho_{1,1} + \rho_{2,0} = \rho_{1,0} + \rho_{2,1} = \frac{1}{3} \sum_{i;\mu_i \neq 0} \rho^{\lambda_i} .$$

From these it is clear that $\rho_{2,0} = \rho_{2,1} = \rho_{2,2}$ and $\rho_{1,0} = \rho_{1,1} = \rho_{1,2}$ and going back to the first row of equations that $\rho_{0,0} = \rho_{0,1} = \rho_{0,2}$. But it has been shown that the pairs (m,n) occur once each as (μ_i, ν_i). Therefore c is a period of B.

This completes the proof.

THEOREM 4.10 If G is a group of type $\{p, q, 2, 2\}$ where p and q are distinct odd primes, then G is good.

Proof. Let a, b, c and d be independent generators of G of orders p, q, 2 and 2 respectively. Let ρ and σ be primitive roots of unity of orders p and q respectively. Let AB = G.

If B has two elements then, by Lemma 3.1, A or B is periodic.

Let B have four elements. Then A has pq elements. By Lemma 4.2, it may be assumed that no two elements of B have a common square. Let

$$A = \sum_{i=1}^{pq} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} \ : \ B = \sum_{i=1}^{4} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}.$$

Then, from AB = G, it follows that $(\sum_{i=1}^{pq} \rho^{\alpha_i})(\sum_{i=1}^{4} \rho^{\lambda_i}) =$ $= (\sum_{i=1}^{pq} \sigma^{\beta_i})(\sum_{i=1}^{4} \sigma^{\mu_i}) = (\sum_{i=1}^{pq} \rho^{\alpha_i}\sigma^{\beta_i})(\sum_{i=1}^{4} \rho^{\lambda_i}\sigma^{\mu_i}) = 0.$ Since p does not divide four $\sum_{i=1}^{4} \rho^{\lambda_i} = 0$ is impossible and since q does not divide four $\sum_{i=1}^{4} \sigma^{\mu_i} = 0$ is also impossible. Using Theorem 2 of (2, p.374) and substituting x = 1 it is seen that $\sum_{i=1}^{4} \rho^{\lambda_i}\sigma^{\mu_i} = 0$ implies that $4 = mp + nq$, where $m \geq 0$ and $n \geq 0$. But since p and q are odd primes this is not possible. Therefore

$$\sum_{i=1}^{pq} \rho^{\alpha_i} = \sum_{i=1}^{pq} \sigma^{\beta_i} = \sum_{i=1}^{pq} \rho^{\alpha_i}\sigma^{\beta_i} = 0.$$

From $\sum_{i=1}^{pq} \rho^{\alpha_i} = 0$ it follows that the numbers α_i are 0, 1, ..., p-1, each occurring q times. From $\sum_{i=1}^{pq} \rho^{\alpha_i}\sigma^{\beta_i} = 0$ it follows that $\sum_{i;\alpha_i=0} \sigma^{\beta_i} = \sum_{i;\alpha_i=1} \sigma^{\beta_i} = \ldots = \sum_{i;\alpha_i=p-1} \sigma^{\beta_i}.$ But $\sum_{i=1}^{pq} \sigma^{\beta_i} = 0$. Therefore $\sum_{i;\alpha_i=k} \sigma^{\beta_i} = 0$ for k = 0, 1, ..., p-1. From above there are q terms in each sum. It follows that the numbers β_i in each sum are 0, 1, ..., q-1. Therefore the pairs (α_i, β_i) are $(0,0), (0,1), \ldots, (0, q-1), (1,0), \ldots, ((p-1),(q-1))$. They are assumed to be in this order.

Also from AB = G it follows that

$$\Big(\sum_{i=1}^{pq}(-1)^{\gamma_i}\Big)\Big(\sum_{i=1}^{4}(-1)^{\nu_i}\Big) = \Big(\sum_{i=1}^{pq}(-1)^{\delta_i}\Big)\Big(\sum_{i=1}^{4}(-1)^{\theta_i}\Big) = \Big(\sum_{i=1}^{pq}(-1)^{\gamma_i+\delta_i}\Big)\Big(\sum_{i=1}^{4}(-1)^{\nu_i+\theta_i}\Big) = 0.$$

Since two does not divide pq it follows that $\sum_{i=1}^{4}(-1)^{\nu_i} = \sum_{i=1}^{4}(-1)^{\theta_i} = \sum_{i=1}^{4}(-1)^{\nu_i+\theta_i} = 0$. Therefore the numbers ν_i, the numbers θ_i and the numbers $\nu_i+\theta_i$ (mod 2) are 0, 0, 1, 1. Let (k, ℓ) occur $\varkappa_{k,\ell}$ times among the pairs (ν_i, θ_i).

Then the following equations hold.

$$\begin{aligned}
\varkappa_{0,0} + \varkappa_{0,1} + \varkappa_{1,0} + \varkappa_{1,1} &= 4\\
\varkappa_{0,0} + \varkappa_{0,1} \qquad\qquad\qquad &= 2\\
\varkappa_{0,0} \qquad\quad + \varkappa_{1,0} \qquad\quad &= 2\\
\varkappa_{0,0} \qquad\qquad\qquad + \varkappa_{1,1} &= 2.
\end{aligned}$$

Adding the last three of these and subtracting twice the first it follows that $2\varkappa_{0,0} = 2$. Therefore $\varkappa_{0,0} = 1$ and hence $\varkappa_{0,1} = \varkappa_{1,0} = \varkappa_{1,1} = 1$. Therefore the pairs (ν_i, θ_i) are (0,0) (0,1) (1,0) and (1,1). They are assumed to be in this order.

If $\sum_{i=1}^{4} \rho^{\lambda_i}\sigma^{\mu_i}(-1)^{\omega_i} = 0$, where ω_i is ν_i, θ_i or $\nu_i+\theta_i$, then $\sum_{i;\omega_i=0} \rho^{\lambda_i}\sigma^{\mu_i} = \sum_{i;\omega_i=1} \rho^{\lambda_i}\sigma^{\mu_i}$. There are two terms in each sum. It follows that $F_p(x) \mid \sum_{i;\omega_i=0} \sigma^{\mu_i}x^{\lambda_i} - \sum_{i;\omega_i=0} \sigma^{\mu_i}x^{\lambda_i}$. Therefore the coefficients of $x^0, x, \dots, x^{p-1}$ are equal. If not all the exponents arise then each coefficient is zero and so the sums $\sum_{i;\omega_i=0} \rho^{\lambda_i}\sigma^{\mu_i}$ and $\sum_{i;\omega_i=1} \rho^{\lambda_i}\sigma^{\mu_i}$ are identical. This is the case if p > 3. If p = 3 then q > 3 and the argument can be repeated interchanging p and q and ρ and σ. It follows that B has two elements with equal exponents λ_i and μ_i and so common squares.

Therefore it may be assumed that $\sum_{i=1}^{\lambda q} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i} = 0$; $\sum_{i=1}^{\lambda q} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\delta_i} = 0$; $\sum_{i=1}^{\lambda q} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i + \delta_i} = 0$.

Consider the following relationships

(1) $\sum_{i=1}^{4} \rho^{\lambda_i} (-1)^{\nu_i} = 0$; (2) $\sum_{i=1}^{4} \rho^{\lambda_i} (-1)^{\theta_i} = 0$; (3) $\sum_{i=1}^{4} \rho^{\lambda_i} (-1)^{\nu_i + \theta_i} = 0$;

(4) $\sum_{i=1}^{4} \sigma^{\mu_i} (-1)^{\nu_i} = 0$; (5) $\sum_{i=1}^{4} \sigma^{\mu_i} (-1)^{\theta_i} = 0$; (6) $\sum_{i=1}^{4} \sigma^{\mu_i} (-1)^{\nu_i + \theta_i} = 0$.

(1) implies $\rho^{\lambda_1} + \rho^{\lambda_2} = \rho^{\lambda_3} + \rho^{\lambda_4}$; (2) implies $\rho^{\lambda_1} + \rho^{\lambda_3} = \rho^{\lambda_2} + \rho^{\lambda_4}$;

(3) implies $\rho^{\lambda_1} + \rho^{\lambda_4} = \rho^{\lambda_2} + \rho^{\lambda_3}$; (4) implies $\sigma^{\mu_1} + \sigma^{\mu_2} = \sigma^{\mu_3} + \sigma^{\mu_4}$;

(5) implies $\sigma^{\mu_1} + \sigma^{\mu_3} = \sigma^{\mu_2} + \sigma^{\mu_4}$; (6) implies $\sigma^{\mu_1} + \sigma^{\mu_4} = \sigma^{\mu_2} + \sigma^{\mu_3}$.

(1) and (2) imply $\lambda_1 = \lambda_4$ and $\lambda_2 = \lambda_3$; (1) and (3) imply $\lambda_1 = \lambda_3$ and $\lambda_2 = \lambda_4$

(2) and (3) imply $\lambda_1 = \lambda_2$ and $\lambda_3 = \lambda_4$; (4) and (5) imply $\mu_1 = \mu_4$ and $\mu_2 = \mu_3$

(4) and (6) imply $\mu_1 = \mu_3$ and $\mu_2 = \mu_4$; (5) and (6) imply $\mu_1 = \mu_2$ and $\mu_3 = \mu_4$

Since no two elements of B have a common square no two pairs (λ_i, μ_i) are equal. Certainly not all six relationships can hold. Since p and q could be interchanged and any two of c, d and cd form an independent set of generators, it may be assumed, without loss of generality, that (1) does not hold. Furthermore, if (2) and (3) hold true then both (5) and (6) do not hold. It may be assumed that either (2) does not hold or (5) does not hold. Thus there are two cases to consider.

(i) not (1) and not (2).

Since (1) and (2) do not hold it follows that $\sum_{i=1}^{\lambda q} \rho^{\alpha_i} (-1)^{\gamma_i} = \sum_{i=1}^{\lambda q} \rho^{\alpha_i} (-1)^{\delta_i} = 0$. But $\sum_{i=1}^{\lambda q} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i} = \sum_{i=1}^{\lambda q} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\delta_i} = 0$

Therefore, by a familiar argument, $\sum_{i;\beta_i=k} \rho^{\alpha_i}(-1)^{\gamma_i} = \sum_{i;\beta_i=k} \rho^{\alpha_i}(-1)^{\delta_i} = 0,$ for k = 0, 1, ..., q-1. There are p terms in each sum. Therefore the numbers α_i in each sum are 0, 1, ..., p-1 and all the numbers γ_i and all the numbers δ_i in each sum are equal. Therefore a is a period of A.

(ii) not (1) and not (5).

Since (5) does not hold it follows that $\sum_{i=1}^{pq} \sigma^{\beta_i}(-1)^{\delta_i} = 0.$ As above $\sum_{i;\beta_i=k} \rho^{\alpha_i}(-1)^{\gamma_i} = 0$ and from $\sum_{i=1}^{pq} \rho^{\alpha_i}\sigma^{\beta_i}(-1)^{\delta_i} = 0$ it follows that $\sum_{i;\alpha_i=l} \sigma^{\beta_i}(-1)^{\delta_i} = 0$ for k = 0, 1, ..., q-1 and l = 0, 1, ..., p-1. From the assumption about the ordering of the pairs (α_i, β_i) these results may be expressed as

$$\gamma_r = \gamma_{q+r} = \dots = \gamma_{(p-1)q+r} \quad \text{for} \quad r = 1, \dots, q-1, q. \qquad \text{and}$$

$$\delta_{sq+1} = \delta_{sq+2} = \dots = \delta_{(s+1)q} \quad \text{for} \quad s = 0, 1, \dots, p-1.$$

But $\sum_{i=1}^{pq} \rho^{\alpha_i}\sigma^{\beta_i}(-1)^{\gamma_i+\delta_i} = 0$. It follows that

$$\sum_{i=1}^{q} \sigma^{\beta_i}(-1)^{\gamma_i+\delta_i} = \sum_{i=q+1}^{2q} \sigma^{\beta_i}(-1)^{\gamma_i+\delta_i} = \dots = \sum_{i=(p-1)q+1}^{pq} \sigma^{\beta_i}(-1)^{\gamma_i+\delta_i}.$$

Now the numbers β_i in each sum are 0, 1, ..., q-1. Therefore, subtracting any term from the first and using the fact that $F_q(x)$ divides the corresponding polynomial obtained by replacing σ by x, it follows that $(-1)^{\gamma_1+\delta_1} - (-1)^{\gamma_{sq+1}+\delta_{sq+1}} = (-1)^{\gamma_r+\delta_r} - (-1)^{\gamma_{sq+r}+\delta_{sq+r}}$

for r = 2, ..., q, s = 1, ..., p-1. It may be assumed that $\gamma_1 = \delta_1 = 0$. Therefore, from the above $\gamma_{sq+1} = \delta_r = 0$. Thus $1 - (-1)^{\delta_{sq+1}} = (-1)^{\gamma_r} - (-1)^{\gamma_r+\delta_{sq+1}}$. Each side is either zero or 2. If, for some s, each side is non-zero, then $\gamma_r = 0$ for all r. Therefore $\gamma_i = 0$ for all i and a is a period of A. If, for all s, each side is zero then $\delta_{sq+1} = 0$ for all s and therefore $\delta_i = 0$ for all i. In this case b is a period of A.

Let A have p elements then B has 4q elements. Let $A = \sum_{i=1}^{p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i}$ and $B = \sum_{i=1}^{4q} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}$. From AB = G the following relationships hold: $(\sum_{i=1}^{p} \rho^{\alpha_i})(\sum_{i=1}^{4q} \rho^{\lambda_i}) = 0$. As before $\sum_{i=1}^{p} \rho^{\alpha_i} = 0$ and the numbers α_i are 0, 1, ..., p-1. $(\sum_{i=1}^{p} \sigma^{\beta_i})(\sum_{i=1}^{4q} \sigma^{\mu_i}) = 0$. As before $\sum_{i=1}^{4q} \sigma^{\mu_i} = 0$ and the numbers μ_i are 0,0,0,0,1,1,1,1,..., q-1, q-1, q-1, q-1. Also it is seen, since 2 does not divide p, that $\sum_{i=1}^{4q} (-1)^{\nu_i} = \sum_{i=1}^{4q} (-1)^{\theta_i} = \sum_{i=1}^{4q} (-1)^{\nu_i + \theta_i} = 0$. From these it follows, as above, that the pairs (ν_i, θ_i) are (0,0), (0,1), (1,0) and (1,1), each occurring q times.

Consider the following relationships.

(7) $\sum_{i=1}^{p} \rho^{\alpha_i} \sigma^{\beta_i} = 0$;

(7) implies that $F_p(x) \mid \sum_{i=1}^{p} \sigma^{\beta_i} x^{\alpha_i}$ and therefore that all numbers β_i in this sum are equal and so equal to zero.

(8) $\sum_{i=1}^{p} \rho^{\alpha_i} (-1)^{\gamma_i} = 0$;

(8) implies that all γ_i are zero.

(9) $\sum_{i=1}^{p} \rho^{\alpha_i} (-1)^{\delta_i} = 0$;

(9) implies that all δ_i are zero.

(10) $$\sum_{i=1}^{p} \rho^{\alpha_i} (-1)^{\gamma_i + \delta_i} = 0 \ ;$$

(10) implies that all $\gamma_i + \delta_i$ are zero modulo 2.

(11) $$\sum_{i=1}^{p} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i} = 0 \ ;$$

(11) implies that all β_i and all γ_i are zero.

(12) $$\sum_{i=1}^{p} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\delta_i} = 0 \ ;$$

(12) implies that all β_i and all δ_i are zero.

(13) $$\sum_{i=1}^{p} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i + \delta_i} = 0 \ ;$$

(13) implies that all β_i are zero and that all $\gamma_i + \delta_i$ are zero modulo 2.

If $\beta_i = \gamma_i = \delta_i = 0$, for all i, then a is a period of A. If $\beta_i = \gamma_i = 0$ for all i but not all δ_i are zero then (9), (10), (12) and (13) cannot hold. Therefore from AB = G it follows that

$$\sum_{i=1}^{4q} \rho^{\lambda_i} (-1)^{\theta_i} = \sum_{i=1}^{4q} \rho^{\lambda_i} (-1)^{\nu_i + \theta_i} = \sum_{i=1}^{4q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\theta_i} = \sum_{i=1}^{4q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\nu_i + \theta_i} = 0.$$

Hence $\sum_{i;\mu_i = k} \rho^{\lambda_i} (-1)^{\theta_i} = \sum_{i;\mu_i = k} \rho^{\lambda_i} (-1)^{\nu_i + \theta_i} = 0$ for k = 0, 1, ..., q-1. But there are four terms in each of these sums. Since $F_2(x)$ divides $\sum_{i;\mu_i = k} \rho^{\lambda_i} x^{\theta_i}$ and $\sum_{i;\mu_i = k} \rho^{\lambda_j} x^{\nu_i + \theta_i}$ it follows easily that the numbers θ_i in the first sum are 0, 0, 1, 1, with the coefficient of x^0 equal to the coefficient of x and the numbers $\nu_i + \theta_i$ in the second sum are 0, 0, 1, 1 (mod 2), with the corresponding coefficients also equal. Now, since $\beta_i = 0$ it follows that $\sum_{i=1}^{p} \sigma^{\beta_i} (-1)^{\gamma_i} \neq 0$.

Therefore $\sum_{i=1}^{4q} \sigma^{\mu_i}(-1)^{\nu_i} = 0$. But $\sum_{i=1}^{4q} (-1)^{\nu_i} = 0$. It follows that $\sum_{i;\mu_i=k} (-1)^{\nu_i} = 0$ and so, since there are four terms, that the numbers ν_i in this sum are 0, 0, 1, 1. Therefore, in each sum with $\mu_i = k$ the numbers ν_i, θ_i and the numbers $\nu_i + \theta_i$ (mod 2) are 0, 0, 1, 1. As before it follows that the corresponding pairs (ν_i, θ_i) are (0,0) (0,1) (1,0) and (1,1). Let $\rho_{k,m,n} = \sum_{i;(\mu_i,\nu_i,\theta_i)=(k,m,n)} \rho^{\lambda_i}$. Then from the above results it follows that there is only one term in each sum and that, for each k, k = 0, 1, ..., q-1,

$$\rho_{k,0,0} + \rho_{k,1,1} = \rho_{k,0,1} + \rho_{k,1,0} \text{ and } \rho_{k,0,0} + \rho_{k,1,0} = \rho_{k,0,1} + \rho_{k,1,1}.$$

Therefore $\rho_{k,0,0} = \rho_{k,0,1}$ and $\rho_{k,1,0} = \rho_{k,1,1}$. It follows that d is a period of B.

If $\beta_i = \delta_i = 0$ for all i but not all γ_i are zero it can be shown similarly that c is a period of B.

If $\beta_i = 0$ for all i but not all γ_i nor all δ_i are zero then from not (8), not (9), not (11) and not (12) it can be shown by a similar argument to that used above that cd is a period of B.

If not all β_i are zero then (7), (11), (12) and (13) cannot hold. Therefore

$$\sum_{i=1}^{4q} \rho^{\lambda_i} \sigma^{\mu_i} = \sum_{i=1}^{4q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\nu_i} = \sum_{i=1}^{4q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\theta_i} = \sum_{i=1}^{4q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\nu_i+\theta_i} = 0.$$

From the first two of these it follows that

$$\sum_{i;\nu_i=0} \rho^{\lambda_i} \sigma^{\mu_i} = \sum_{i;\nu_i=1} \rho^{\lambda_i} \sigma^{\mu_i} = 0.$$

There are 2q terms in each sum. Therefore, applying Theorem 2 of (2, p.374) and substituting x = 1 it follows that $2q = mp + nq$, where $m \geqslant 0$ and $n \geqslant 0$. Since $p > 2$, it follows that $m = 0$ and $n = 2$. This implies, by Theorem 2 of (2, p.374), as has been previously shown, that b is a period of $\sum_{i;\, \nu_i = k} a^{\lambda_i} b^{\mu_i}$ for $k = 0, 1$. Therefore the numbers μ_i in each sum are 0, 0, 1, 1, ..., q-1, q-1, and the numbers λ_i are λ_1' occurring with μ_i equal to 0, 1, ..., q-1 and λ_2' occurring with μ_i equal to 0, 1, ..., q-1.

Similar results can also be shown for θ_i and for $\nu_i + \theta_i$. Any given number λ_i must occur a multiple of q times. Let it be lq times where $l = 1, 2, 3$ or 4. Let $x_{0,0}$, $x_{0,1}$, $x_{1,0}$ and $x_{1,1}$ be the number of times that the pairs (0,0), (0,1), (1,0) and (1,1) respectively occur with this number λ_i. Then from the above $x_{0,0} + x_{0,1}$ is a multiple of q, $x_{0,0} + x_{1,0}$ is a multiple of q and $x_{0,0} + x_{1,1}$ is a multiple of q. From the equations

$$x_{0,0} + x_{0,1} + x_{1,0} + x_{1,1} = l q \;;\; x_{0,0} + x_{0,1} = l_1 q \;;\; x_{0,0} + x_{1,0} = l_2 q$$

and $x_{0,0} + x_{1,1} = l_3 q$ it follows that $x_{0,0} = \dfrac{l_1 + l_2 + l_3 - l}{2}\, a$ Since $x_{0,0}$ is an integer and q an odd prime, $x_{0,0}$ must be a multiple of q. Therefore $x_{0,1}$, $x_{1,0}$ and $x_{1,1}$ are multiples of q. Since it has been shown that each pair (ν_i, θ_i) occurs q times altogether these multiples must be 0 or 1 and if it is 1 this accounts for all such pairs (ν_i, θ_i). Consider the numbers μ_i occurring with such a set of q elements, in which all λ_i are equal and all pairs (ν_i, θ_i) are equal. Then since B contains no element twice the numbers μ_i must be different and so must be 0, 1, ..., q-1. Therefore b is a period of B.

The case in which A has q elements and B 4p elements is similar.

There remains the case in which A has $2p$ elements and B has $2q$ elements. Let

$$A = \sum_{i=1}^{2p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} \quad \text{and} \quad B = \sum_{i=1}^{2q} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}.$$

Then, as before, it follows from $AB = G$ that the numbers α_i are $0, 0, 1, 1, \ldots, p-1, p-1$ and the numbers μ_i are $0, 0, 1, 1, \ldots, q-1, q-1$. They are assumed to be in these orders.

From $AB = G$ it follows that

$$(14) \qquad \sum_{i=1}^{2p} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i} = 0.$$

$$\text{or} \quad (15) \qquad \sum_{i=1}^{2q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\nu_i} = 0 \;;$$

$$(16) \qquad \sum_{i=1}^{2p} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\delta_i} = 0$$

$$\text{or} \quad (17) \qquad \sum_{i=1}^{2q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\theta_i} = 0 \;;$$

$$(18) \qquad \sum_{i=1}^{2p} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i + \delta_i} = 0$$

$$\text{or} \quad (19) \qquad \sum_{i=1}^{2q} \rho^{\lambda_i} \sigma^{\mu_i} (-1)^{\nu_i + \theta_i} = 0.$$

At least two relationships derived from the same factor must hold. Since p and q may be interchanged and any two of c, d and cd generate the subgroup of type $\{2,2\}$ it may be assumed, without loss of generality, that (14) and (16) hold.

$\sum_{i=1}^{2p} \rho^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i} = 0.$ Therefore $F_p(x)$ divides $\sum_{i=1}^{2p} x^{\alpha_i} \sigma^{\beta_i} (-1)^{\gamma_i}$. It follows that

$$\sum_{i;\,\alpha_i=0} \sigma^{\beta_i} (-1)^{\gamma_i} = \sum_{i;\,\alpha_i=1} \sigma^{\beta_i} (-1)^{\gamma_i} = \ldots = \sum_{i;\,\alpha_i=p-1} \sigma^{\beta_i} (-1)^{\gamma_i}.$$

There are two terms in each sum. $\sum_{i;\alpha_i=k} \sigma^{\beta_i}(-1)^{\gamma_i} - \sum_{i;\alpha_i=l} \sigma^{\beta_i}(-1)^{\gamma_i} = 0,$ for all pairs k and l, $0 \leq k < p$, $0 \leq l < p$. Therefore $F_2(x)$ divides $\sum_{i;\alpha_i=k} \sigma^{\beta_i}x^{\gamma_i} - \sum_{i;\alpha_i=l} \sigma^{\beta_i}x^{\gamma_i}$. Therefore the coefficient of x^0 and x are equal. If one coefficient is missing a sum of two σ's is equal to another such sum and since $q > 2$, as has been previously shown the sums must be identical.

$\sigma^{\beta_1'} + \sigma^{\beta_2'} - \sigma^{\beta_3'} = -\sigma^{\beta_4'}$ is impossible. Therefore x^0 cannot occur three times and x once or vice versa. If x^0 occurs twice and x twice then either $\sigma^{\beta_1'} + \sigma^{\beta_2'} = -\sigma^{\beta_3'} - \sigma^{\beta_4'}$ or $\sigma^{\beta_1'} - \sigma^{\beta_2'} = \sigma^{\beta_3'} - \sigma^{\beta_4'}$. But the first of these is again impossible. In the second case $\beta_1' = \beta_2'$ and $\beta_3' = \beta_4'$ or $\beta_1' = \beta_3'$ and $\beta_2' = \beta_4'$. These results may be summarised as follows. If in one pair $\sum_{i;\alpha_i=k} \sigma^{\beta_i}x^{\gamma_i}$ the numbers γ_i are both equal to 0 (or to 1) then in all pairs they are equal to 0 (or to 1) and the same two numbers β_i occur in each pair. If the numbers γ_i in one pair are 0 and 1 then in all pairs they are 0 and 1 and either all the β_i occurring with $\gamma_i = 0$ are equal and all the β_i occurring with $\gamma_i = 1$ are equal or else the two β_i in each pair are equal.

Similar results follow from $\sum_{i=1}^{2p} \rho^{\alpha_i}\sigma^{\beta_i}(-1)^{\delta_i} = 0$.

If all $\gamma_i = 0$ and all $\delta_i = 0$ then a is clearly a period of A. If all $\gamma_i = 0$ and the numbers δ_i occur in pairs 0, 1 then, if the numbers β_i occurring with $\delta_i = 0$ are all equal and the numbers β_i occurring with $\delta_i = 1$ are all equal a is a period of A, and if the two β_i in each pair are equal then d is a period of A. The case in which all $\delta_i = 0$ and the γ_i occur in pairs 0 and 1 is similar. Let the numbers γ_i and the numbers δ_i occur in pairs 0 and 1. Then if the two β_i in each pair are equal cd is a period of A. If all β_i with $\gamma_i = 0$ are equal, all β_i with $\gamma_i = 1$ are equal, all β_i with $\delta_i = 0$ are equal and all β_i with $\delta_i = 1$ are equal, then either all β_i are equal and cd is a period or else $\gamma_i = 0$ occurs with the same δ_i and $\gamma_i = 1$ occurs with the other δ_i in every pair so that a is a period of A.

This completes the proof.

THEOREM 4.11 If G is a group of type $\{p, 2, 2, 2, 2\}$, where p is an odd prime, then G is good.

Proof. Let a, b, c, d and f be independent generators of G of orders p, 2, 2, 2 and 2 respectively. Let ρ be a primitive root of unity of order p. Let AB = G.

The cases to be considered are those in which A has p, 2p, 4p and 8p elements.

If A has 8p elements then B has two elements. By Lemma 3.1, A or B is periodic.

If A has 4p elements then B has four elements. By Lemma 4.2 it may be assumed that no two elements of B have a common square. Let

$$A = \sum_{i=1}^{4p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} f^{\epsilon_i} \text{ and } B = \sum_{i=1}^{4} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i} f^{\phi_i}.$$

$0 \leq m < 2$, $0 \leq n < 2$ and $k + l + m + n > 0$, then $F_2(x)$ divides 2,

$\sum^{4} \rho^{\lambda_i} x^{k\mu_i + l\nu_i + m\theta_i + n\phi_i}$ and it follows that the numbers

$0 \leq m < 2$, $0 \leq n < 2$ and $k + l + m + n > 0$, then $F_2(x)$ divides

$\sum_{i=1}^{4} \rho^{\lambda_i} x^{k\mu_i + l\nu_i + m\theta_i + n\phi_i}$ and it follows that the numbers

$k\mu_i + l\nu_i + m\theta_i + n\phi_i$ are 0, 0. 1 and 1 modulo 2 and that the coefficients of x^0 and x are equal. Therefore the powers of ρ in each coefficient are identical. It follows that B has two elements with a common square. Therefore $\sum_{i=1}^{4p} \rho^{\alpha_i}(-1)^{k\beta_i + l\gamma_i + m\delta_i + n\epsilon_i} = 0$ for all such sets k, l, m, and n.

$\sum_{i=1}^{4} \rho^{\lambda_i} = 0$ is not possible since p does not divide four. Therefore $\sum_{i=1}^{4p} \rho^{\alpha_i} = 0$ and it follows that the numbers α_i are 0, 1, ..., p-1 each occurring four times. The coefficients of $\rho^0, \rho, \ldots, \rho^{p-1}$ in $\sum_{i=1}^{4p} \rho^{\alpha_i}(-1)^{k\beta_i + l\gamma_i + m\delta_i + n\epsilon_i}$ are equal, and hence equal to -4, -2, 0, 2 or 4 for each set k, l, m and n. Therefore, for fixed k, l, m and n, in each set of four in a coefficient of ρ^{α_i} there are always the same number of exponents congruent to 0 and congruent to 1 modulo 2. Let the number congruent to 0 be $t_{k,l,m,n}$. For any fixed α_i, say $\alpha_i = \alpha$, let the number of four-tuples occurring among the coefficients $(\beta_i, \gamma_i, \delta_i, \epsilon_i)$, $\alpha_i = \alpha$, equal to (0,0,0,0), (0,0,0,1), (0,0,1,0), (0,0,1,1), (0,1,0,0), (0,1,0,1), (0,1,1,0), (0,1.1,1), (1,0,0,0), (1,0,0,1), (1,0.1,0), (1,0,1,1), (1,1,0,0), (1, 1,0,1) and (1,1,1,1) be $x_{0,0,0,0}$, $x_{0,0,0,1}, \ldots, x_{1,1,1,1}$ respectively. Then the following equations hold.

$$\sum_{(s_1,s_2,s_3,s_4)\,;\, ks_1 + ls_2 + ms_3 + ns_4 \equiv 0 \pmod 2} x_{s_1,s_2,s_3,s_4} = t_{k,l,m,n},$$

$$\sum_{(s_1,s_2,s_3,s_4)\,;\, ks_1 + ls_2 + ms_3 + ns_4 \equiv 1 \pmod 2} x_{s_1,s_2,s_3,s_4} = 4 - t_{k,l,m,n}.$$

These equations are shown to have a unique solution. Any particular unknown $x_{s_{1,1}, s_{2,1}, s_{3,1}, s_{4,1}}$ occurs 15 times by choosing k, l , m and n with $k + l + m + n > 0$. If $x_{s_{1,2}, s_{2,2}, s_{3,2}, s_{4,2}}$ is any other unknown then it occurs in the same equation as $x_{s_{1,1}, s_{2,1}, s_{3,1}, s_{4,1}}$ if and only if

$$k(s_{1,1} - s_{1,2}) + l(s_{2,1} - s_{2,2}) + m(s_{3,1} - s_{3,2}) + n(s_{4,1} - s_{4,2}) \equiv 0 \pmod 2.$$

At least one of the numbers $s_{j,1} - s_{j,2}$, $1 \leq j \leq 4$, is non-zero. The other three coefficients from k, l , m and n may be chosen, with non-zero sum, in seven ways and this coefficient solved for uniquely. Therefore $x_{s_{1,1}, s_{2,1}, s_{3,1}, s_{4,1}}$ and $x_{s_{1,2}, s_{2,2}, s_{3,2}, s_{4,2}}$ both occur in seven equations. Adding all equations involving $x_{s_{1,1}, s_{2,1}, s_{3,1}, s_{4,1}}$ and subtracting seven times $\sum x_{s_1, s_2, s_3, s_4} = 4$ from this, a definite value is obtained for $8x_{s_{1,1}, s_{2,1}, s_{3,1}, s_{4,1}}$ and so for $x_{s_{1,1}, s_{2,1}, s_{3,1}, s_{4,1}}$. Therefore the equations have a unique solution. Therefore for each α, $0 \leq \alpha < p$, the same four 4-tuples ($\beta_i, \gamma_i, \delta_i, \epsilon_i$) occur with $\alpha_i = \alpha$. It follows that a is a period of A.

Let A have 2p elements. Then B has 8 elements. Let

$$A = \sum_{i=1}^{2p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} f^{\epsilon_i} \text{ and } B = \sum_{i=1}^{8} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i} f^{\phi_i}.$$

Then $\sum_{i=1}^{2p} \rho^{\alpha_i} = 0$ and so the numbers α_i are 0,0,1,1, ..., p-1, p-1.

If $\sum_{i=1}^{2p} \rho^{\alpha_i} (-1)^{k\beta_i + l\gamma_i + m\delta_i + n\epsilon_i} = 0$, where $0 \leq k < 2$, $0 \leq l < 2$, $0 \leq m < 2$, $0 \leq n < 2$ and $k + l + m + n > 0$ then the coefficients of $\rho^0, \rho, \cdots, \rho^{p-1}$ are all equal. Therefore each coefficient is -2, 0, or 2 and so the pair of numbers $k\beta_i + l\gamma_i + m\delta_i + n\epsilon_i$ for $\alpha_i = \alpha$ are both 0, both 1, or 0 and 1 for all α . If this happens for four sets (k_1, l_1, m_1, n_1), ... (k_4, l_4, m_4, n_4) independent modulo (2,2,2,2) then it is easily verified that the pairs β_i , the pairs γ_i , the pairs δ_i and the pairs ϵ_i are the same pair for all α in each case. If all these are 0, 0 or all are 1, 1 then A contains the same element twice, which is impossible. Let $g_1, \ldots, g_r$, $1 \leq r \leq 4$, be the generators corresponding to the pairs which are 0, 1. Then $g_1 . g_2 \ldots g_r$ is a period of A.

Therefore it may be assumed that the above result does not hold for four independent sets (k, ℓ, m, n). If (k_i, ℓ_i, m_i, n_i) $i = 1, 2, 3, 4$ are an independent set modulo (2,2,2,2) then the four elements $b^{k_i} c^{\ell_i} d^{m_i} f^{n_i}$ generate the subgroup of type $\{2,2,2,2\}$. By renaming generators if necessary, it may be assumed that for all $k = 1$, $\sum_{i=1}^{2p} \rho^{\alpha_i} (-1)^{k\beta_i + \ell\gamma_i + m\delta_i + n\epsilon_i} \neq 0$. For if this is true for $k_1 = 1$ then the corresponding generator $b^{k_1} c^{\ell_1} d^{m_1} f^{n_1}$ may be renamed b_1 and b_1, c, d, f is a set of generators. If, with this new set of generators, $\sum_{i=1}^{2p} \rho^{\alpha_i} (-1)^{k_2\beta_i + \ell_2\gamma_i + m_2\delta_i + n_2\epsilon_i} = 0$ for some $\ell_2 = 1$ then setting $c_1 = b_1^{k_2} c^{\ell_2} d^{m_2} f^{n_2}$, b_1, c_1, d, f is a new set of generators. If necessary d_1 and f_1 are constructed in the same way. But by the above assumption

$\sum_{i=1}^{2p} \rho^{\alpha_i} (-1)^{k\beta_i + \ell\gamma_i + m\delta_i + n\epsilon_i}$ cannot be zero for the four sets

corresponding to b_1 , c_1 , d_1 and f_1 as these are independent. Thus, by renaming generators, if necessary, it may be assumed that

$\sum_{i=1}^{8} \rho^{\lambda_i} (-1)^{\mu_i + \ell\nu_i + m\theta_i + n\phi_i} = 0$ for all ℓ, m and n, $0 \leq \ell < 2$, $0 \leq m < 2$, $0 \leq n < 2$.

Then $F_{2p}(x)$ divides $\sum_{i=1}^{8} \Sigma^{\sigma_i}$, where $0 \leq \sigma_i < 2p$ and $\sigma_i \equiv \lambda_i \pmod{p}$ and $\sigma_i \equiv \mu_i + \ell\nu_i + m\theta_i + n\phi_i \pmod{2}$. Therefore by Theorem 2 of (2, p 374)

$$\sum_{i=1}^{8} x^{\sigma_i} = \frac{x^{2p}-1}{x^{p}-1} f_p(x) + \frac{x^{2p}-1}{x^{2}-1} f_2(x),$$

where $f_p(x)$ and $f_2(x)$ have non-negative integral coefficients. Substituting $x = 1$ it follows that $8 = 2 f_p(1) + p f_2(1)$. If $p > 3$ then it follows that $f_p(1) = 4$ and $f_2(1) = 0$. If $p = 3$ then $f_p(1) = 4$ and $f_2(1) = 0$ or $f_p(1) = 1$ and $f_2(1) = 2$.

Let p be greater than three. Then $f_2(x) = 0$ and $\frac{x^{2p}-1}{x^{p}-1} = x^{p}+1$ is a factor of $\sum_{i=1}^{8} x^{\sigma_i}$. Since p is odd it follows that half the numbers σ_i are odd and half are even. Therefore the numbers $\mu_i + \ell\nu_i + m\theta_i + n\phi_i$ are 0,0,0,0,1,1,1,1 (modulo 2). Furthermore these split into pairs 0 and 1 such that the two corresponding σ_i are equal modulo p, i.e. such that the two corresponding λ_i are equal. Thus λ_i occur in sets of two equal elements, say $2t_\lambda$ for $\lambda_i = \lambda$ and the corresponding $\mu_i + \ell r_i + m\theta_i + n\phi_i \pmod 2$ are 0 and 1 each occurring t_λ times. Let the number of sets $(\mu_i, \nu_i, \theta_i, \phi_i)$ such that $\mu_i = \mu,\ \nu_i = \nu,\ \theta_i = \theta,\ \phi_i = \phi$ occurring with $\lambda_i = \lambda$ be $x_{\mu,\nu,\theta,\phi}$. Then from the different values of ℓ , m and n the following equations are obtained:- $\sum x_{\mu,\nu,\theta,\phi} = t_\lambda$, where for each ℓ , m, n and t the summation is taken over those μ, ν, θ and ϕ such that $\mu + \ell\nu + m\theta + n\phi \equiv t \pmod 2$ where t = 0 or 1. Let $x_{\mu,\nu,\theta,\phi}$ be any of the unknowns. Then it occurs in eight equations obtained by choosing ℓ , m and n arbitrarily.

$x_{\mu+1,\nu,\theta,\phi}$ can clearly never occur in the same equation as $x_{\mu,\nu,\theta,\phi}$ If $x_{\mu',\nu',\theta',\phi'}$ is any other unknown then it occurs in the same equation if and only if $(\mu-\mu') + \ell(\nu-\nu') + m(\theta-\theta') + n(\phi-\phi') \equiv 0$ (mod 2). Some number from $\nu-\nu'$, $\theta-\theta'$, $\phi-\phi'$ is not congruent to 0 (mod 2). Therefore the other two numbers from ℓ, m and n may be picked arbitrarily and the remaining number found uniquely from the equation. Thus this unknown occurs in the same equation as $x_{\mu,\nu,\theta,\phi}$ four times. Adding all equations involving $x_{\mu,\nu,\theta,\phi}$ and subtracting four times $\sum x_{\mu,\nu,\theta,\phi} = 2t_\lambda$ it follows that

$$4x_{\mu,\nu,\theta,\phi} - 4x_{\mu+1,\nu,\theta,\phi} = 8t_\lambda - 4(2t_\lambda) = 0$$

Therefore $x_{\mu,\nu,\theta,\phi} = x_{\mu+1,\nu,\theta,\phi}$. It follows that b is a period of B.

If p is equal to three but the numbers $\mu_i + \ell\nu_i + m\theta_i + n\phi_i$ are 0,0,0,0,1 1,1,1,1 (modulo 2) for all ℓ, m and n then the proof goes through as above. If for some ℓ m and n $f_\lambda(1) = 1$ and $f_2(1) = 2$ then

$$\sum_{i=1}^{8} x^{\sigma_i} = (x^3+1)x^{T_1} + (1+x^2+x^4)(x^{T_2}+x^{T_3})$$

where $0 \leq T_1 < 3$ and $0 \leq T_2 < 2$, $0 \leq T_3 < 2$. Furthermore if $T_2 \neq T_3$ then $x^{T_2}+x^{T_3} = 1+x$ and $(1+x^2+x^4)(x^{T_2}+x^{T_3}) = (x^3+1)(1+x+x^2)$

Thus $\displaystyle\sum_{i=1}^{8} x^{\sigma_i} = (x^3+1)(1+x+x^2+x^{T_1})$

The result then follows as before. It may therefore be assumed that $T_2 = T_3$. Then from $(x^3+1)x^{T_1}$ there is one odd and one even exponent and from $(1+x^2+x^4)(x^{T_2}+x^{T_3})$ there are six odd or six even exponents. The numbers $\mu_i + \ell\nu_i + m\theta_i + n\phi_i \pmod 2$ in this case are 0,0,0,0,0,0,0,1 or 0,1,1,1,1,1,1,1. Consider such sets, arranged in some order, possibly different from that shown, and added to them in pairs, modulo 2, another set from these or from 0,0,0,0,1,1,1,1 arranged in any order. It is easily verified that four 0's and four 1's cannot arise in the sum. 7 0's and a 1 plus 7 0's and a 1 gives 6 0's and 2 1's or 8 0's; 7 0's and a 1 plus 4 0's and 4 1's gives 3 0's and 5 1's or 5 0's and 3 1's; etc. Therefore if $\mu_i + l_1\nu_i + m_1\theta_i + n_1\phi_i$ are 7 0's and a 1 or 7 1's and a 0 it follows that $\sum_{i=1}^{8}(-1)^{\mu_i + l_1\nu_i + m_1\theta_i + n_1\phi_i + \mu_i + l_2\nu_i + m_2\theta_i + n_2\phi_i} \neq 0$. Therefore for all $(l_2, m_2, n_2) \neq (l_1, m_1, n_1)$, $\sum_{i=1}^{6}(-1)^{\rho_i + \beta_i + (l_1+l_2)\gamma_i + (m_1+m_2)\delta_i + (n_1+n_2)\epsilon_i} = 0$. $\beta_i + \beta_i \equiv 0$ (mod 2). Therefore $\sum_{i=1}^{6}(-1)^{l\gamma_i + m\delta_i + n\epsilon_i} = 0$ for all l, m and n, $0 \leq l < 2$, $0 \leq m < 2$, $0 \leq n < 2$ and l + m + n > 0. It follows that each set of numbers $l\gamma_i + m\delta_i + n\epsilon_i$ is three 0's and three 1's. But if γ_i is three 0's and three 1's and δ_i is three 0's and three 1's then $\gamma_i + \delta_i$ clearly cannot be three 0's and three 1's modulo 2. Thus the case p = 3 is also covered.

There remains the case in which A has p elements and B has sixteen elements. Let

$$A = \sum_{i=1}^{p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} f^{\epsilon_i} \text{ and } B = \sum_{i=1}^{16} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i} f^{\phi_i}.$$

Then, from AB = G, it follows that $\sum_{i=1}^{p} \rho^{\alpha_i} = 0$ and so that the numbers α_i are 0, 1, ..., p-1. Similarly $\sum_{i=1}^{16}(-1)^{k\mu_i + l\nu_i + m\theta_i + n\phi_i} = 0$ for all k, l, m and n such that $0 \leq k < 2$, $0 \leq l < 2$, $0 \leq m < 2$, $0 \leq n < 2$ and $k + l + m + n > 0$. It follows that the corresponding numbers

$k\mu_i+\ell\nu_i+m\theta_i+n\phi_i$ are eight 0's and eight 1's (modulo 2). Let the four-tuple (μ,ν,θ,ϕ) occur $x_{\mu,\nu,\theta,\phi}$ times among $(\mu_i,\nu_i,\theta_i,\phi_i)$. Then the equations $\sum x_{\mu,\nu,\theta,\phi}=8$, where for each k, ℓ, m, n and t the summation is taken over those (μ,ν,θ,ϕ) such that $k\mu+\ell\nu+m\theta+n\phi\equiv t \,(\mathrm{mod}\,2), 0\leq t<2$, follow from above. Any fixed unknown $x_{\mu',\nu',\theta',\phi'}$ occurs fifteen times, choosing k, ℓ, m and n arbitrarily with k + ℓ + m + n > 0. Any different unknown $x_{\mu'',\nu'',\theta'',\phi''}$ occurs in the same equation as $x_{\mu',\nu',\theta',\phi'}$, if and only if $k(\mu'-\mu'')+\ell(\nu'-\nu'')+m(\theta'-\theta'')+n(\phi'-\phi'')\equiv 0$ (mod 2). As before this can happen in seven ways with k + ℓ + m + n > 0. Adding all the equations involving $x_{\mu',\nu',\theta',\phi'}$ and subtracting seven times $\sum x_{\mu,\nu,\theta,\phi}=16$ it follows that $8x_{\mu',\nu',\theta',\phi'}=15.8-7.16=8$ Therefore $x_{\mu',\nu',\theta',\phi'}=1$. Thus the four-tuples $(\mu_i,\nu_i,\theta_i,\phi_i)$ are (0,0,0,0), (0,0,0,1), (0,0,1,0), ..., (1,1,1,1). They are assumed to be in this order.

If $\sum_{i=1}^{p}\rho^{\alpha_i}(-1)^{k\beta_i+\ell\gamma_i+m\delta_i+n\epsilon_i}=0$ then from $F_p(x)$ divides $\sum_{i=1}^{p}x^{\alpha_i}(-1)^{k\beta_i+\ell\gamma_i+m\delta_i+n\epsilon_i}$ it follows that all the numbers $k\beta_i+\ell\gamma_i+m\delta_i+n\epsilon_i$ are equal, and so equal to zero, modulo 2. If this happens for four independent sets $(k_1,\ell_1,m_1,n_1),\ldots,(k_4,\ell_4,m_4,n_4)$ modulo (2,2,2,2) then it follows, as before, that $\beta_i=\gamma_i=\delta_i=\epsilon_i=0$. In this case a is a period of A.

As in the previous section, by renaming generators if necessary, it may be assumed that $\sum_{i=1}^{16}\rho^{\lambda_i}(-1)^{\mu_i+\ell\nu_i+m\theta_i+n\phi_i}=0$ for all ℓ, m and n, $0\leq\ell<2, 0\leq m<2, 0\leq n<2$. But it is known that the numbers $\mu_i+\ell\nu_i+m\theta_i+n\phi_i$ are eight 0's and eight 1's. Therefore in each case one sum of eight powers of ρ is equal to another sum of eight powers of ρ. It is easily seen that this can only be the case if the sums are identical. Writing $\rho^{\lambda_i} = \rho_i$ the following equations hold :-

$(\ell, m, n) = (0,0,0)$; $\rho_1+\rho_2+\rho_3+\rho_4+\rho_5+\rho_6+\rho_7+\rho_8 = \rho_9+\rho_{10}+\rho_{11}+\rho_{12}+\rho_{13}+\rho_{14}+\rho_{15}+\rho_{16} = \frac{1}{2}\sum \rho_i$.

$(\ell, m, n) = (0,0,1)$; $\rho_1+\rho_3+\rho_5+\rho_7+\rho_{10}+\rho_{12}+\rho_{14}+\rho_{16} = \rho_2+\rho_4+\rho_6+\rho_8+\rho_9+\rho_{11}+\rho_{13}+\rho_{15} = \frac{1}{2}\sum \rho_i$.

$(\ell, m, n) = (0,1,0)$: $\rho_1+\rho_2+\rho_5+\rho_6+\rho_{11}+\rho_{12}+\rho_{15}+\rho_{16} = \rho_3+\rho_4+\rho_7+\rho_8+\rho_9+\rho_{10}+\rho_{13}+\rho_{14} = \frac{1}{2}\sum \rho_i$.

$(\ell, m, n) = (0,1,1)$: $\rho_1+\rho_4+\rho_5+\rho_8+\rho_{10}+\rho_{11}+\rho_{14}+\rho_{15} = \rho_2+\rho_3+\rho_6+\rho_7+\rho_9+\rho_{12}+\rho_{13}+\rho_{16} = \frac{1}{2}\sum \rho_i$.

$(\ell, m, n) = (1,0,0)$; $\rho_1+\rho_2+\rho_3+\rho_4+\rho_{13}+\rho_{14}+\rho_{15}+\rho_{16} = \rho_5+\rho_6+\rho_7+\rho_8+\rho_9+\rho_{10}+\rho_{11}+\rho_{12} = \frac{1}{2}\sum \rho_i$.

$(\ell, m, n) = (1,0,1)$; $\rho_1+\rho_3+\rho_6+\rho_8+\rho_{10}+\rho_{12}+\rho_{13}+\rho_{15} = \rho_2+\rho_4+\rho_5+\rho_7+\rho_9+\rho_{11}+\rho_{14}+\rho_{16} = \frac{1}{2}\sum \rho_i$.

$(\ell, m, n) = (1,1,0)$; $\rho_1+\rho_2+\rho_7+\rho_8+\rho_{11}+\rho_{12}+\rho_{13}+\rho_{14} = \rho_3+\rho_4+\rho_5+\rho_6+\rho_9+\rho_{10}+\rho_{15}+\rho_{16} = \frac{1}{2}\sum \rho_i$.

$(\ell, m, n) = (1,1,1)$; $\rho_1+\rho_4+\rho_6+\rho_7+\rho_{10}+\rho_{11}+\rho_{13}+\rho_{16} = \rho_2+\rho_3+\rho_5+\rho_8+\rho_9+\rho_{12}+\rho_{14}+\rho_{15} = \frac{1}{2}\sum \rho_i$.

Clearly ρ_s and ρ_{s+8} cannot occur in the same sum as the corresponding four-tuples have the same (ν, θ, ϕ) but different μ. If ρ_t is any other unknown then ρ_s and ρ_t occur in the same sum if and only if the corresponding four-tuples $(\mu_1,\nu_1,\theta_1,\phi_1)$, $(\mu_2,\nu_2,\theta_2,\phi_2)$ are such that $\mu_1+\ell\nu_1+m\theta_1+n\phi_1 \equiv \mu_2+\ell\nu_2+m\theta_2+n\phi_2 \pmod 2$. This happens for four choices of ℓ, m and n. Thus adding all sums involving ρ_s,

$8\rho_s + 4\sum\limits_{t \not\equiv s \pmod 8} \rho_t = 4\sum \rho_i$ and adding all sums involving ρ_{s+8},

$8\rho_{s+8} + 4\sum\limits_{t \not\equiv s+8 \pmod 8} \rho_t = 4\sum \rho_i$;it follows that $8\rho_s = 8\rho_{s+8}$.

and so that $\rho_s = \rho_{s+\gamma}$. Therefore b is a period of B.

This completes the proof.

COROLLARY If G is a group of type $\{p, 2, 2, 2\}$ or $\{p. 2, 2\}$ where p is an odd prime, then G is good.

THEOREM 4.12 If G is a group of type $\{p^2, 2, 2, 2\}$, where p is an odd prime, then G is good.

Proof. Let a, b, c and d be independent generators of G of orders p^2, 2, 2 and 2 respectively. Let ρ be a $p^2 th$ primitive root of unity. Let AB = G. The essentially different cases which have to be considered are those in which A has 4 p^2 elements, 2 p^2 elements, p^2 elements, 8p elements and 4p elements.

Let A have 4 p^2 elements. Then B has two elements. Therefore, by Lemma 3.1, A or B is periodic.

Let A have 2 p^2 elements. Then B has four elements. By Lemma 4.2, it may be assumed that no two elements of B have a common square. Let:

$$A = \sum_{i=1}^{2p^2} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} \quad \text{and} \quad B = \sum_{i=1}^{4} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}.$$

Then, from AB = G, it follows that $\left(\sum_{i=1}^{2p^2} (\rho^p)^{\alpha_i}\right)\left(\sum_{i=1}^{4} (\rho^p)^{\lambda_i}\right) = 0$ and $\left(\sum_{i=1}^{2p^2} \rho^{\alpha_i}\right)\left(\sum_{i=1}^{4} \rho^{\lambda_i}\right) = 0$. Since p does not divide 4 it follows that $\sum_{i=1}^{2p^2} (\rho^p)^{\alpha_i} = \sum_{i=1}^{2p^2} \rho^{\alpha_i} = 0$. Therefore $F_p(x) \cdot F_{p^2}(x) =$ $= (1 + x + \dots + x^{p^2-1})$ divides $\sum_{i=1}^{2p^2} x^{\alpha_i}$. Hence the numbers α_i are 0, 0, 1, 1, ..., p^2-1, p^2-1. They are assumed to be in this order.

If $\sum_{i=1}^{4} \rho^{\lambda_i} (-1)^{k\mu_i + l\nu_i + m\theta_i} = 0$, where $k + l + m > 0$, then it is easily seen that the numbers $k\mu_i + l\nu_i + m\theta_i$ are 0, 0, 1, 1, (modulo 2) and that the corresponding numbers λ_i are equal in pairs. But if two λ_i in $\sum_{i=1}^{4} a^{\lambda_i}$ are equal then B has two elements with a common square. Therefore it may be assumed that $\sum_{i=1}^{2p^2} \rho^{\alpha_i} (-1)^{k\beta_i + l\gamma_i + m\delta_i} = 0$ for all k, l, m, $0 \leq k < 2$, $0 \leq l < 2$, $0 \leq m < 2$ and $k + l + m > 0$. From this it follows that $F_{p^2}(x)$ divides $\sum_{i=1}^{2p^2} x^{\alpha_i} (-1)^{k\beta_i + l\gamma_i + m\delta_i}$. Hence the coefficients of $x^r, x^{r+p}, \ldots, x^{r+p^2-p}$ are equal for $r = 0, 1, \ldots, p-1$. Therefore

$$\sum_{i=2r-1}^{2r} (-1)^{k\beta_i + l\gamma_i + m\delta_i} = \sum_{i=2r-1+2p}^{2r+2p} (-1)^{k\beta_i + l\gamma_i + m\delta_i} = \ldots = \sum_{i=2r-1+2p^2-2p}^{2r+2p^2-2p} (-1)^{k\rho_i + l\gamma_i + m\delta_i},$$

for $r = 1, 2, \ldots, p$. Each of these is either -2, 0 or 2 and thus the numbers $k\beta_i + l\gamma_i + m\delta_i$ in each sum, for fixed r, are either two 0's, two 1's or 0 and 1. It is now shown that the pairs $(\beta_i, \gamma_i, \delta_i)$ in each sum are the same. For fixed r and s let $x_{\beta,\gamma,\delta}$ denote the number of $(\beta_i, \gamma_i, \delta_i)$ occurring with $\lambda_i = r + ps$. Then the equations $\sum_{k\beta + l\gamma + m\delta \equiv t \pmod 2} x_{\beta,\gamma,\delta} = K_{k,l,m,t,r}$ arise and the constant K does not depend on s. Any fixed unknown occurs seven times with $k + l + m > 0$ and any other unknown occurs in the same equation with it three times. Thus adding all equations involving one unknown and subtracting three times $\sum x_{\beta,\gamma,\delta} = 2$ from it a solution, which must be the only solution to the equations is obtained. It follows that a^p is a period of A.

Let A have p^2 elements. Then B has eight elements. Let $A = \sum_{i=1}^{p^2} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i}$ and $B = \sum_{i=1}^{8} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}$. Then, from AB = G, it follows, as before, that $\sum_{i=1}^{p^2} (\rho^k)^{\alpha_i} = \sum_{i=1}^{p^2} \rho^{\alpha_i} = 0$. Therefore $F_p(x) . F_{p^2}(x)$ divides $\sum_{i=1}^{p^2} x^{\alpha_i}$ and so the numbers α_i are 0, 1, ..., p^2-1. Also from AB = G it follows that $\sum_{i=1}^{8} (-1)^{k\mu_i + l\nu_i + m\theta_i} = 0$ for $0 \leq k < 2$, $0 \leq l < 2$, $0 \leq m < 2$ and $k + l + m > 0$. As in the previous theorem it can be shown that the three-tuples (μ_i, ν_i, θ_i) are (0,0,0), (0,0,1), (0,1,0), ..., (1,1,1). They are assumed to be in this order.

If $\sum_{i=1}^{p^2} \rho^{\alpha_i} (-1)^{k\beta_i + l\gamma_i + m\delta_i} = 0$ then $F_{p^2}(x)$ divides $\sum_{i=1}^{p^2} x^{\alpha_i} (-1)^{k\beta_i + l\gamma_i + m\delta_i}$. Therefore the coefficients of $x^r, x^{r+p}, \ldots, x^{r+p^2-p}$ are equal for r = 0, 1, ..., p-1. Each term arises once only. Therefore the corresponding numbers $k\beta_i + l\gamma_i + m\delta_i$ are congruent to one another modulo 2. If this happens for three linearly independent sets $(k_1, l_1, m_1), (k_2, l_2, m_2), (k_3, l_3, m_3)$ modulo (2,2,2) then the corresponding three-tuples $(\beta_i, \gamma_i, \delta_i)$ are equal. In this case a^p is a period of A.

Therefore it may be assumed that for no set of three independent three-tuples is $\sum_{i=1}^{p^2} \rho^{\alpha_i} (-1)^{k\beta_i + l\gamma_i + m\delta_i} = 0$. As before, by renaming generators if necessary, it may be assumed that $\sum_{i=1}^{8} \rho^{\lambda_i} (-1)^{\mu_i + l\nu_i + m\theta_i} = 0$ for all l and m, $0 \leq l < 2, 0 \leq m < 2$. Therefore the coefficients of $(-1)^{\mu_i + l\nu_i + m\theta_i}$ such that

$\mu_i + l\nu_i + m\theta_i \equiv 0$ (mod 2) and such that $\mu_i + l\nu_i + m\theta_i \equiv 1$ (mod 2) are equal. Letting $\rho^{\lambda_i} = \rho_i$ the following set of equations is obtained.

$$(l,m) = (0,0)\ ;\quad \rho_1 + \rho_2 + \rho_3 + \rho_4 = \rho_5 + \rho_6 + \rho_7 + \rho_8 = \tfrac{1}{2}\sum \rho_i .$$

$$(l,m) = (0,1)\ ;\quad \rho_1 + \rho_3 + \rho_6 + \rho_8 = \rho_2 + \rho_4 + \rho_5 + \rho_7 = \tfrac{1}{2}\sum \rho_i .$$

$$(l,m) = (1,0)\ ;\quad \rho_1 + \rho_2 + \rho_7 + \rho_8 = \rho_3 + \rho_4 + \rho_5 + \rho_6 = \tfrac{1}{2}\sum \rho_i .$$

$$(l,m) = (1,1)\ ;\quad \rho_1 + \rho_4 + \rho_6 + \rho_7 = \rho_2 + \rho_3 + \rho_5 + \rho_8 = \tfrac{1}{2}\sum \rho_i .$$

By inspection it is seen that each ρ_i occurs four times, that $\rho_{i'}$, where $i' \neq i$, $i' \equiv i$ (mod 4), never occurs in the same sum as ρ_i and that ρ_j, where $j \not\equiv i$ (mod 4) occurs twice in the same equation as ρ_i. Thus adding all the sums with ρ_i and subtracting twice $\sum_{j=1}^{8} \rho_j$, it follows that $2\rho_i - 2\rho_{i'} = (4\cdot\frac{1}{2} - 2)\sum \rho_i = 0$. Therefore $\rho_i = \rho_{i'}$, where $i \equiv i'$ (mod 4). It follows that b is a period of B.

Let A have 8p elements. Then B has p elements. Let

$$A = \sum_{i=1}^{8p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} \quad \text{and} \quad B = \sum_{i=1}^{p} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}$$

Then $\left(\sum_{i=1}^{8p} (\rho^p)^{\alpha_i}\right)\left(\sum_{i=1}^{p} (\rho^p)^{\lambda_i}\right) = 0$ and $\left(\sum_{i=1}^{8p} \rho^{\alpha_i}\right)\left(\sum_{i=1}^{p} \rho^{\lambda_i}\right) = 0$. Therefore $F_p(x)$ divides $\sum_{i=1}^{8p} x^{\alpha_i}$ or $\sum_{i=1}^{p} x^{\lambda_i}$ and $F_{p^2}(x)$ divides $\sum_{i=1}^{8p} x^{\alpha_i}$ or $\sum_{i=1}^{p} x^{\lambda_i}$. Since $F_{p^2}(1) = F_p(1) = p$ it follows that $F_p(x)$ and $F_{p^2}(x)$ do not both divide the same polynomial.

Also $\left(\sum_{i=1}^{8p} (-1)^{k\beta_i + \ell\gamma_i + m\delta_i}\right)\left(\sum_{i=1}^{p} (-1)^{k\mu_i + \ell\nu_i + m\theta_i}\right) = 0$ for all k, ℓ, m where $0 \leqslant k < 2$, $0 \leqslant \ell < 2$, $0 \leqslant m < 2$ and $k + \ell + m > 0$. Since 2 does not divide p it follows that $\sum_{i=1}^{8p} (-1)^{k\beta_i + \ell\gamma_i + m\delta_i} = 0$. Therefore the numbers $k\beta_i + \ell\gamma_i + m\delta_i$, modulo 2, are 0 and 1, each occurring 4p times. Letting $x_{\beta,\gamma,\delta}$ be the number of times (β,γ,δ) occurs among the three-tuples $(\beta_i,\gamma_i,\delta_i)$, then equations are obtained, similar to sets previously obtained, and by the same methods it can be shown that $x_{\beta,\gamma,\delta} = p$ for all (β,γ,δ). Thus the three-tuples $(\beta_i,\gamma_i,\delta_i)$ are (0,0,0,), (0,0,1), ..., (1,1,1) each occurring p times. It is assumed that the first p are (0,0,0) the second p are (0,0,1), ..., and that the eighth p are (1,1,1).

Suppose that $F_{p^2}(x)$ does not divide $\sum_{i=1}^{p} x^{\lambda_i}$. If $\sum_{i=1}^{p} \rho^{\lambda_i}(-1)^{k\mu_i + \ell\nu_i + m\theta_i} = 0$ then $F_{p^2}(x)$ divides $\sum_{i=1}^{p} x^{\lambda_i}(-1)^{k\mu_i + \ell\nu_i + m\theta_i}$. It follows that the numbers λ_i are s, s+p, ..., s+p^2-p, with all $k\mu_i + \ell\nu_i + m\theta_i \equiv 0$ (mod 2), and thus that $F_{p^2}(x)$ divides $\sum_{i=1}^{p} x^{\lambda_i}$. It follows that, in this case, $\sum_{i=1}^{8p} \rho^{\alpha_i}(-1)^{k\beta_i + \ell\gamma_i + m\delta_i} = 0$ for all k, ℓ and m. Let $\rho_j = \sum_{i=(j-1)p+1}^{jp} \rho^{\alpha_i}$. Then, from the information about the exponents $k\beta_i + \ell\gamma_i + m\delta_i$, the following equations hold:-

$(k, \ell, m) = (0,0,1)$; $\rho_1 + \rho_3 + \rho_5 + \rho_7 = \rho_2 + \rho_4 + \rho_6 + \rho_8 = \frac{1}{2}\sum \rho_j$.

$(k, \ell, m) = (0,1,0)$; $\rho_1 + \rho_2 + \rho_5 + \rho_6 = \rho_3 + \rho_4 + \rho_7 + \rho_8 = \frac{1}{2}\sum \rho_j$

. . . .

$(k, \ell, m) = (1,1,1)$; $\rho_1 + \rho_4 + \rho_6 + \rho_7 = \rho_2 + \rho_3 + \rho_5 + \rho_8 = \frac{1}{2}\sum \rho_j$.

Using the four equations in which $k = 1$ it can be shown, as before, that $\rho_1 = \rho_5$, $\rho_2 = \rho_6$, $\rho_3 = \rho_7$, $\rho_4 = \rho_8$. Similarly using the equation in which $\ell = 1$ it follows that $\rho_1 = \rho_3$, $\rho_2 = \rho_4$, $\rho_5 = \rho_7$, $\rho_6 = \rho_8$ and using the equations in which $m = 1$ it follows that $\rho_1 = \rho_2$, $\rho_3 = \rho_4$, $\rho_5 = \rho_6$, $\rho_7 = \rho_8$. From these it follows that $\rho_1 = \rho_2 = \rho_4 = \rho_8 = \rho_6 = \rho_5 = \rho_7 = \rho_3$. Now each ρ_j is a sum of p powers of a primitive root of unity of order p^2. It is easily shown, by familiar methods, that two such sums can be equal only if they are each zero or else if they consist of identical powers. If all ρ_j are zero then $F_{p^2}(x)$ divides each corresponding polynomial and a^p is a period of A. If some ρ_j is not zero then all sets ρ_j are identical and all the elements of order two are periods of A.

If $F_{p^2}(x) \mid \sum_{i=1}^{p} x^{\lambda_i}$ then $F_p(x) \mid \sum_{i=1}^{8p} x^{\alpha_i}$. Suppose that $\sum_{i=1}^{p} \rho^{\lambda_i} (-1)^{k\mu_i + \ell\nu_i + m\theta_i} = 0$. Then, as previously stated, the numbers λ_i are $s, s+p, \ldots, s+p^2-p$ and the numbers $k\mu_i + \ell\nu_i + m\theta_i$ are all congruent to 0 modulo 2. If this occurs for three independent sets (k_1, ℓ_1, m_1), (k_2, ℓ_2, m_2) and (k_3, ℓ_3, m_3) modulo $(2,2,2)$ then all the numbers μ_i, all the numbers ν_i and all the numbers θ_i are congruent to 0 modulo 2. In this case a^p is a period of B. It may be assumed that this does not occur for three independent sets (k, ℓ, m) and therefore, by renaming generators, if necessary, that it does not occur for $k = 1$. Thus

$\sum_{i=1}^{8p} \rho^{\alpha_i}(-1)^{\beta_i + l\gamma_i + m\delta_i} = 0$ for all l and m, $0 \leqslant l < 2$ and $0 \leqslant m < 2$. Letting $\rho_j = \sum_{i=(j-1)p+1}^{jp} \rho^{\alpha_i}$ it can again be shown that $\rho_1 = \rho_5, \rho_2 = \rho_6, \rho_3 = \rho_7, \rho_4 = \rho_8$. Either ρ_t and ρ_{t+4} are identical sums or else are zero for t = 1, 2, 3, 4. If all pairs are zero then $F_{p^2}(x) \mid \sum_{i=(j-1)p+1}^{jp} x^{\alpha_i}$ and a^p is a period of A. If ρ_t and ρ_{t+4} are identical for t = 1, 2, 3 and 4 then b is a period of A. Suppose, if possible that some ρ_j are zero and some are non-zero. Since $F_p(x) \mid \sum_{i=1}^{8p} x^{\alpha_i}$ it follows that there are eight α_i congruent to 0, to 1, ..., and to p-1 modulo p. If $\sum_{i=(j-1)p+1}^{jp} \rho^{\alpha_i} = 0$ then all these α_i are congruent modulo p. If $\rho_t = \rho_{t+4}$ then the α_i in each sum are identical and so occur in pairs. It follows, if both cases arise, that 8 = Mp + N2 where $M \geqslant 0$ and $N \geqslant 0$ and in some cases $M > 0$. But this cannot happen if $p > 3$. If p = 3, then B has three elements and by Lemma 3 1, A or B is periodic.

Let A have 4p elements. Then B has 2p elements. Let

$$A = \sum_{i=1}^{4p} a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i} \quad \text{and} \quad B = \sum_{i=1}^{2p} a^{\lambda_i} b^{\mu_i} c^{\nu_i} d^{\theta_i}$$

Then, from AB = G, it follows that

$$\Big(\sum_{i=1}^{4p} x^{\alpha_i}\Big)\Big(\sum_{i=1}^{2p} x^{\lambda_i}\Big) \equiv 8(1 + x + \cdots + x^{p^2-1})(\bmod (x^{p^2}-1)).$$

Therefore $F_p(x)$ divides $\sum_{i=1}^{4p} x^{\alpha_i}$ or $\sum_{i=1}^{2p} x^{\lambda_i}$ and $F_{p^2}(x)$ divides $\sum_{i=1}^{4p} x^{\alpha_i}$ or $\sum_{i=1}^{2p} x^{\lambda_i}$. Since $F_{p^2}(1) = F_p(1) = p$ they cannot both divide the same polynomial.

Let $F_{p^2}(x) \,\Big|\, \sum_{i=1}^{2p} x^{\lambda_i}$ and $F_p(x) \,\Big|\, \sum_{i=1}^{4p} x^{\alpha_i}$. Then the numbers λ_i are $s_1, s_2, s_1+p, s_2+p, \ldots, s_1+p^2-p, s_2+p^2-p$ where $0 \leqslant s_1 < p$, $0 \leqslant s_2 < p$ and $s_1 = s_2$ is possible. The numbers α_i are congruent modulo p to 0, 1, ..., p-1, each number occurring four times. If $\sum_{i=1}^{2p} p^{\lambda_i} (-1)^{k\mu_i + l\nu_i + m\theta_i} = 0$ then $F_{p^2}(x)$ divides $\sum_{i=1}^{2p} x^{\lambda_i} (-1)^{k\mu_i + l\nu_i + m\theta_i}$ and the coefficients of $x^{s_1}, x^{s_1+p}, \ldots, x^{s_1+p^2-p}$ and of $x^{s_2}, x^{s_2+p}, \ldots, x^{s_2+p^2-p}$ are equal. If $s_1 = s_2$ the coefficients are sums of two powers of -1, and the corresponding exponents must be both zero always, both 1 always or 0 and 1 always. If this occurs for three independent sets $(k_1, l_1, m_1), (k_2, l_2, m_2), (k_3, l_3, m_3)$ modulo (2,2,2) then, if $s_1 \neq s_2$ the three-tuples (μ_i, ν_i, θ_i) corresponding to $\lambda_i = s_1$, $\lambda_i = s_1 + p, \ldots, \lambda_i = s_1 + p^2 - p$ and corresponding to $\lambda_i = s_2$, $\lambda_i = s_2 + p, \ldots,$ $\lambda_i = s_2 + p^2 - p$ are equal. Thus a^p is a period of B. If $s_1 = s_2$ and the pairs are always both 0 or both 1 then the pairs corresponding to $\lambda_i = s_1$ are the same and B has two elements the same, which is not possible. If $s_1 = s_1$ and the pairs corresponding to generators $g_1, \ldots, g_n$, where n = 1, 2 or 3 are 0, 1 then $g_1 \ldots g_n$ is a period of B. Thus if for three independent sets (k, l, m) the corresponding sum is zero, B is periodic.

As before, by renaming generators, if necessary, it may be assumed that $\sum_{i=1}^{4p} p^{\alpha_i} (-1)^{\beta_i + l\gamma_i + m\delta_i} = 0$ for all l and m, $0 \leqslant l < 2$, $0 \leqslant m < 2$. Then $F_{2p^2}(x)$ divides $\sum_{i=1}^{4p} x^{\sigma_i}$ where $0 \leqslant \sigma_i < 2p^2$, $\sigma_i \equiv \alpha_i \pmod{p^2}$, $\sigma_i \equiv \beta_i + l\gamma_i + m\delta_i \pmod{2}$.

Therefore by Theorem 2 of (2, p.374) it follows that

$$\sum_{i=1}^{4p} x^{\sigma_i} = \frac{x^{2p^2}-1}{x^{p^2}-1} f_p(x) + \frac{x^{2p^2}-1}{x^{2p}-1} f_2(x)$$

where $f_p(x)$ and $f_2(x)$ have non-negative integral coefficients. Now the numbers α_i (mod p) and therefore the numbers σ_i (mod p) are congruent to 0, 1, ..., p-1, each number occurring four times, i.e. precisely four numbers σ_i are equal modulo p. Now any term in $f_p(x)$ provides two exponents occurring in the product $\frac{x^{2p^2}-1}{x^{p^2}-1} f_p(x)$ congruent modulo p^2 and so congruent modulo p. Any term in $f_2(x)$ provides p exponents in the product $\frac{x^{2p^2}-1}{x^{2p}-1} f_2(x)$ congruent modulo p. It follows that $f_2(x) = 0$, since $4 = 2M + pN$ with $M \geqslant 0$ and $N > 0$ is not possible. Therefore $\sum_{i=1}^{4p} x^{\sigma_i} = (x^{p^2}+1) f_p(x)$. The degree of $f_p(x)$ is clearly less than p^2. It follows that the numbers σ_i occur in pairs s and $s+p^2$. The corresponding numbers α_i are equal and the corresponding numbers $\beta_i + l\gamma_i + m\delta_i$ are 0 and 1. Let any given number $\alpha_i = \alpha$ occur $2t_\alpha$ times. Then the numbers $\beta_i + l\gamma_i + m\delta_i$ occurring with it are 0 and 1 each occurring t_α times.

If $x_{\beta,\gamma,\delta}$ indicates the number of times the three-tuple (β,γ,δ) occurs with $\alpha_i = \alpha$, a set of equations is derived, as before, which show that $x_{\beta,\gamma,\delta} = x_{\beta+b,\gamma,\delta}$. Therefore b is a period of A.

Let $F_{p^2}(x) \mid \sum_{i=1}^{4p} x^{\alpha_i}$ and $F_p(x) \mid \sum_{i=1}^{2p} x^{\lambda_i}$. Then the numbers α_i are s_1, s_2, s_3, s_4, $s_1 + p$, $s_2 + p$, ..., $s_3 + p^2 - p$,

$s_4 + p^2 - p$ where $0 \leq s_i < p$ and the numbers λ_i are congruent modulo p to 0, 0, 1, 1, ..., p-1, p-1. If $\sum_{i=1}^{2p} \rho^{\lambda_i}(-1)^{k\mu_i + \ell\nu_i + m\theta_i} = 0$ where $0 \leq k < 2$, $0 \leq \ell < 2$, $0 \leq m < 2$ and $k + \ell + m > 0$ then, since p numbers λ_i cannot be congruent modulo p, it follows that the numbers λ_i are actually equal in pairs and that the exponents $k\mu_i + \ell\nu_i + m\theta_i$ corresponding to any $\lambda_i = \lambda$ are 0 and 1. If this occurs for three independent three-tuples (k_1, ℓ_1, m_1) (k_2, ℓ_2, m_2) and (k_3, ℓ_3, m_3) modulo (2,2,2) then if the corresponding generators are g_1, g_2 and g_3 it can easily be shown, as before, that $g_1 g_2 g_3$ is a period of B.

If for no three-tuple (k, ℓ, m), $\sum_{i=1}^{2p} \rho^{\lambda_i}(-1)^{k\mu_i + \ell\nu_i + m\theta_i} = 0$ then for every three-tuple (k, ℓ, m), $\sum_{i=1}^{4p} \rho^{\alpha_i}(-1)^{k\beta_i + \ell\gamma_i + m\delta_i} = 0.$ Therefore $F_{p^2}(x)$ divides $\sum_{i=1}^{4p} x^{\alpha_i}(-1)^{k\beta_i + \ell\gamma_i + m\delta_i}$. It follows that the coefficients of $x^s, x^{s+p}, \ldots, x^{s+p^2-p}$ in this polynomial are equal. There may be sums of one, two, three or four powers of (-1) in each coefficient. But for given s there will be the same number for s, for s+p, ..., and for $s+p^2-p$. Thus in each coefficient there must be the same number of exponents congruent to 0 modulo 2 and the same number of exponents congruent to 1, modulo 2. Let $x_{\beta,\gamma,\delta}$ be the number of three-tuples (β, γ, δ) occurring in the three-tuples $(\beta_i, \gamma_i, \delta_i)$ which correspond to $\alpha_i = s + rp$. Then the equations $\sum x_{\beta,\gamma,\delta} = \kappa_{k,\ell,m,t,s}$, where the summation is taken over those numbers $x_{\beta,\gamma,\delta}$ such that $k\beta + \ell\gamma + m\delta \equiv t$ (mod 2), and the constant is independent of r, follow from the above result. By showing that any $x_{\beta',\gamma',\delta'}$ occurs seven times with $k+l+m>0$ and that any other unknown $x_{\beta'',\gamma'',\delta''}$ occurs in the same equation with it three times, it follows, as before, that the solution of these equations is unique. Thus there is the same solution for every r and so a^{p} is a period of A.

Let $\sum_{i=1}^{2p} \rho^{\lambda_i}(-1)^{k'\mu_i+l'\nu_i+m'\theta_i}=0$ for some three-tuple (k',l',m'). Then the numbers λ_i have been shown to be equal in pairs. If $\sum_{i=1}^{2p} (\rho^{p})^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}=0$ then $F_p(x)$ divides $\sum_{i=1}^{2p} x^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}$ and so the coefficients of $x^{r_0}, x^{r_1}, \dots, x^{r_{p-1}}$, where $r_j \equiv j \pmod{p}$, are equal. Thus the corresponding exponents $k\mu_i+l\nu_i+m\theta_i$ must be both 0, or both 1, or 0 and 1 (modulo 2) for every j. If $\sum_{i=1}^{2p} (\rho^{p})^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}=0$ for three independent three-tuples modulo (2,2,2) then, since λ_i are actually equal in pairs, some pairs $k\mu_i+l\nu_i+m\theta_i$ corresponding to $\lambda_i = r_j$ must be 0 and 1. Then if the corresponding generators are $g_1, \dots, g_n$ where $1 \leq n \leq 3$, $g_1 \dots g_n$ is a period of B.

If $\sum_{i=1}^{2p} \rho^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}=0$ then $\sum_{i=1}^{2p} (\rho^{p})^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}=0$ also, since the numbers λ_i are equal in pairs and the corresponding numbers $k\mu_i+l\nu_i+m\theta_i$ are 0 and 1 modulo 2. Therefore if $\sum_{i=1}^{2p} (\rho^{p})^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}\neq 0$ then $\sum_{i=1}^{2p} \rho^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}\neq 0$ and so $\sum_{i=1}^{4p} (\rho^{p})^{\alpha_i}(-1)^{k\beta_i+l\gamma_i+m\delta_i}=0$ and $\sum_{i=1}^{4p} \rho^{\alpha_i}(-1)^{k\beta_i+l\gamma_i+m\delta_i}=0$.

Now it may be assumed that $\sum_{i=1}^{2p} (\rho^{p})^{\lambda_i}(-1)^{k\mu_i+l\nu_i+m\theta_i}=0$

for not more than two independent three-tuples (k_1, ℓ_1, m_1), (k_2, ℓ_2, m_2). By renaming generators, if necessary, it may be assumed that $\sum_{i=1}^{4p} (\rho^{k})^{\alpha_i} (-1)^{\beta_i + \ell\gamma_i + m\delta_i} = 0$ and $\sum_{i=1}^{4p} \rho^{\alpha_i} (-1)^{\beta_i + \ell\gamma_i + m\delta_i} = 0$ for all ℓ and m where $0 \leq \ell \leq 2$, $0 \leq m \leq 2$. It follows that $F_{p^2}(x)$ and $F_p(x)$ divide $\sum_{i=1}^{4p} x^{\alpha_i} (-1)^{\beta_i + \ell\gamma_i + m\delta_i}$. Therefore $\sum_{i=1}^{4p} x^{\alpha_i} (-1)^{\beta_i + \ell\gamma_i + m\delta_i} =$

$F_{p^2}(x) . F_p(x) . C(x)$. But $F_{p^2}(x) . F_p(x) = 1 + x + \cdots + x^{p^2-1}$ and the degree of $\sum_{i=1}^{4p} x^{\alpha_i} (-1)^{\beta_i + \ell\gamma_i + m\delta_i}$ is less than p^2.

Therefore C(x) is just a constant C. Substituting $x = 1$ it follows that $\sum_{i=1}^{4p} (-1)^{\beta_i + \ell\gamma_i + m\delta_i} = p^2 C$. But

$-4p \leq \sum_{i=1}^{4p} (-1)^{\beta_i + \ell\gamma_i + m\delta_i} \leq 4p$ and $\sum_{i=1}^{4p} (-1)^{\beta_i + \ell\gamma_i + m\delta_i}$ is even. Therefore $-4 \leq pC \leq 4$ and C is even. Since p is an odd prime it follows that $C = 0$. Therefore $\sum_{i=1}^{4p} x^{\alpha_i} (-1)^{\beta_i + \ell\gamma_i + m\delta_i} = 0$. Thus any given number $\alpha_i = \alpha$ occurs an even number of times. Let $\alpha_i = \alpha$ occur $2t_\alpha$ times. Then the corresponding numbers $\beta_i + \ell\gamma_i + m\delta_i$ are 0 and 1 modulo 2, each occurring t_α times. Let $x_{\beta,\gamma,\delta}$ be the number of times (β, γ, δ) occurs among the three-tuples $(\beta_i, \gamma_i, \delta_i)$ corresponding to $\alpha_i = \alpha$. Then the following equations arise:

$$(\ell, m) = (0,0) ; \quad x_{0,0,0} + x_{0,0,1} + x_{0,1,0} + x_{0,1,1} \qquad = t_\alpha$$

$$x_{1,0,0} + x_{1,0,1} + x_{1,1,0} + x_{1,1,1} = t_\alpha .$$

$$(l,m) = (0,1) ;\ x_{0,0,0} + x_{0,1,0} + x_{1,0,1} + x_{1,1,1} = t_\alpha ,$$

$$x_{0,0,1} + x_{0,1,1} + x_{1,0,0} + x_{1,1,0} = t_\alpha .$$

$$(l,m) = (1,0) ;\ x_{0,0,0} + x_{0,0,1} + x_{1,1,0} + x_{1,1,1} = t_\alpha ,$$

$$x_{0,1,0} + x_{0,1,1} + x_{1,0,0} + x_{1,0,1} = t_\alpha .$$

$$(l,m) = (1,1) ;\ x_{0,0,0} + x_{0,1,1} + x_{1,0,1} + x_{1,1,0} = t_\alpha ,$$

$$x_{0,0,1} + x_{0,1,0} + x_{1,0,0} + x_{1,1,1} = t_\alpha .$$

$x_{0,\gamma,\delta}$ and $x_{1,\gamma,\delta}$ do not occur in the same equation. $x_{\beta,\gamma,\delta}$ occurs four times in all. $x_{\beta',\gamma',\delta'}$, where (γ',δ') is not identical with (γ,δ) occurs twice in the same equation as $x_{\beta,\gamma,\delta}$ Adding all equations involving $x_{\beta,\gamma,\delta}$ and then subtracting twice $\sum x_{\beta,\gamma,\delta} = 2t_\alpha$ it follows that $2x_{0,\gamma,\delta} - 2x_{1,\gamma,\delta} = 4t_\alpha - 2.2t_\alpha = 0$ Therefore $x_{0,\gamma,\delta} = x_{1,\gamma,\delta}$. It follows that b is a period of A.

This completes the proof.

THEOREM 4.13 If G is a group of type $\{p^3, 2, 2\}$, where p is an odd prime, then G is good.

Proof. Let AB = G. Let a, b and c of orders p^3, 2 and 2 respectively generate G. Let ρ be a primitive root of unity of order p^3. Let

$$A = \sum a^{\alpha_i} b^{\beta_i} c^{\gamma_i} \ ; \ B = \sum a^{\lambda_i} b^{\mu_i} c^{\nu_i}.$$

It is not yet necessary to specify the number of elements in A or B. From AB = G it follows that

$$(\sum \rho^{\alpha_i})(\sum \rho^{\lambda_i}) = (\sum \rho^{\alpha_i}(-1)^{\beta_i})(\sum \rho^{\lambda_i}(-1)^{\mu_i}) =$$

$$= (\sum \rho^{\alpha_i}(-1)^{\gamma_i})(\sum \rho^{\lambda_i}(-1)^{\nu_i}) = (\sum \rho^{\alpha_i}(-1)^{\beta_i+\gamma_i})(\sum \rho^{\lambda_i}(-1)^{\mu_i+\nu_i}) = 0.$$

It may be assumed that $\sum \rho^{\alpha_i} = 0$.

Suppose that two of the other sums of complex numbers arising from B are zero. Since any two of b, c and bc generate the subgroup of type $\{2, 2\}$, it may be assumed, without loss of generality, that $\sum \rho^{\lambda_i}(-1)^{\mu_i} = \sum \rho^{\lambda_i}(-1)^{\nu_i} = 0$. Therefore $F_{p^3}(x)$ divides $\sum x^{\lambda_i}(-1)^{\mu_i}$ and $\sum x^{\lambda_i}(-1)^{\nu_i}$. Then if $0 \leq \alpha < p^2$ the coefficients of $x^{\alpha}, x^{\alpha+p^2}, \ldots, x^{\alpha+(p-1)p^2}$ are equal in each polynomial. If any coefficient is non-zero then each exponent $\alpha, \alpha+p^2, \ldots, \alpha+(p-1)p^2$ must occur at least once. Then since $\sum \rho^{\alpha_i} = 0$ it follows that $F_{p^3}(x) \mid \sum x^{\alpha_i}$ and therefore that if β occurs among the exponents α_i so also does $\beta+p^2, \beta+2p^2, \ldots, \beta+(p-1)p^2$ where $0 \leq \beta < p^2$. It follows that $\alpha+\beta+(p-1)p^2$ occurs among the exponents in $(\sum x^{\alpha_i})(\sum x^{\lambda_i})$ as $(\alpha+(p-1)p^2)+\beta, (\alpha+(p-2)p^2)+(\beta+p^2), \ldots, \alpha+(\beta+(p-1)p^2)$ that is p times. If there are any extra terms with $\lambda_i = \alpha + l p^2$ or any terms for which the coefficient is zero then these exponents must occur an even number of times. Thus any exponent in $(\sum x^{\alpha_i})(\sum x^{\lambda_i})$ occurs $m_1 p + m_2 2$ times. But it occurs four times. Therefore $m_1 = 0$ and every coefficient in $\sum x^{\lambda_i}(-1)^{\mu_i}$ and in $\sum x^{\alpha_i}(-1)^{\nu_i}$ is zero. If an exponent $\lambda_i = \alpha$ occurs four times then the corresponding pairs (μ_i, ν_i) must be all different and so must be (0, 0), (0, 1), (1, 0) and (1, 1). If an exponent $\lambda_i = \alpha$ occurs twice then the corresponding numbers μ_i are 0 and 1 and the corresponding numbers ν_i are 0 and 1. It follows that bc is a period of B.

The other cases to be considered are those in which all the polynomials derived from A are divisible by $F_{p^3}(x)$ and in which precisely one polynomial derived from B is divisible by $F_{p^3}(x)$.

Let $F_{p^3}(x)$ divide $\sum x^{\alpha_i}, \sum x^{\alpha_i}(-1)^{\beta_i}, \sum x^{\alpha_i}(-1)^{\gamma_i}$ and $\sum x^{\alpha_i}(-1)^{\beta_i+\gamma_i}$. Suppose that the exponent α occurs k times among the exponents α_i. Then so also does the exponent $\alpha + l p^2$ The coefficients of $x^{\alpha}, x^{\alpha+p^2}, \ldots, x^{\alpha+(p-1)p^2}$ are equal in each polynomial. Therefore there are k_1 exponents $\beta_i = 0$, k_2 exponents $\gamma_i = 0$ and k_3 exponents $\beta_i + \gamma_i$ congruent to 0 modulo 2, corresponding to $\alpha_i = \alpha + l p^2$, for each l. Let the pair (β, γ) occur $x_{\beta,\gamma}$ times among the pairs (β_i, γ_i) occurring with $\alpha_i = \alpha + l p^2$. Then the following equations arise:

$$x_{0,0} + x_{0,1} = k_1 \; ; \quad x_{1,0} + x_{1,1} = k - k_1 \; ;$$

$$x_{0,0} + x_{1,0} = k_2 \; ; \quad x_{0,1} + x_{1,1} = k - k_2 \; ;$$

$$x_{0,0} + x_{1,1} = k_3 \; ; \quad x_{0,1} + x_{1,0} = k - k_3 \, .$$

Adding the equations involving $x_{\beta,\gamma}$ and subtracting $x_{0,0} + x_{0,1} + x_{1,0} + x_{1,1} = k$ it is seen that there is a unique solution. Therefore the same pairs (β_i, γ_i) arise with $\alpha_i = \alpha + \ell p^2$ for all ℓ. It follows that a^{p^2} is a period of A.

In the remaining case it may be assumed that $F_{p^3}(x)$ divides $\sum x^{\alpha_i}, \sum x^{\alpha_i}(-1)^{\beta_i}, \sum x^{\alpha_i}(-1)^{\gamma_i}$ and $\sum x^{\lambda_i}(-1)^{\mu_i+\nu_i}$. As in the first case it can be shown that every coefficient in $\sum x^{\lambda_i}(-1)^{\mu_i+\nu_i}$ is zero. It follows that each $\lambda_i = \lambda$ occurs an even number of times and so that the number of elements in B is even. If B has two elements then, by Lemma 3.1, A or B is periodic. If B has four elements then, by the above information about the exponents λ_i, B has two elements with a common square and so A or B is periodic. Using the first three polynomials above and the notation of the previous paragraph it again follows that

$$x_{0,0} + x_{0,1} = k_1 \quad ; \quad x_{1,0} + x_{1,1} = k - k_1 \ ;$$

$$x_{0,0} + x_{1,0} = k_2 \quad ; \quad x_{0,1} + x_{1,1} = k - k_2 \ .$$

$x_{\beta,\gamma}$ is the number of times that (β, γ) occurs with $\alpha_i = \alpha + \ell p^2$. Since A contains no repeated element $x_{\beta,\gamma}$ is 0 or 1. Therefore $0 \leqslant k \leqslant 4$, $0 \leqslant k_i \leqslant 2$ and $0 \leqslant k - k_i \leqslant 2$. Further if any k_i or $k - k_i$ is 0, both x's in this equation are 0 and a solution is unique, and if any k_i or $k - k_i$ is 2, both x's in this equation are 1 and a solution is unique. Under these conditions a^{p^2} is a period of A. The only other possibility is that $k_1 = k_2 = k - k_1 = k - k_2 = 1$. Therefore k = 2. There are now two possible solutions: $x_{0,0} = x_{1,1} = 1$, $x_{0,1} = x_{1,0} = 0$ and

$x_{0,0} = x_{1,1} = 0, x_{0,1} = x_{1,0} = 1$. bc is a period of either of the pairs of elements of A arising in this way. Thus if all elements arise in pairs of these kinds bc is a period of A. It may therefore be assumed that certain pairs α_i arise in this way and that other elements arise, as above, in sets of p with a^{p^2} as period. Thus there are at least 3p elements in A. Therefore B cannot have $2p^3$, $4p^2$ or $2p^2$ elements. Therefore B has 2p or 4p elements. If B has 4p elements then A has p^2 elements and from

$$\left(\sum_{i=1}^{p^2} x^{\alpha_i}\right)\left(\sum_{i=1}^{4p} x^{\lambda_i}\right) \equiv 4\left(1+x+\dots+x^{p^3-1}\right)\left(\mathrm{mod}\,(x^{p^3}-1)\right),$$

it can be shown, as in Theorem 3.2, that no two numbers α_i are equal. This contradicts the case k = 2 used above. Therefore the only possibility remaining is that A have $2p^2$ elements and B 2p elements. From the case k = 2, i.e. a number $\alpha_i = \alpha$ arising twice, it follows that λ_i cannot arise four times, as this would give an exponent arising eight times in $(\sum x^{\alpha_i})(\sum x^{\lambda_i})$. Therefore any exponent λ_i occurs twice and the numbers $\mu_i + \nu_i$ corresponding to it are 0 and 1 (modulo 2). Thus the corresponding pair of elements in B can be of one of the forms $a^\lambda, a^\lambda b; a^\lambda, a^\lambda c; a^\lambda bc, a^\lambda b; a^\lambda bc, a^\lambda c$. If $\alpha_i = \alpha$ arises twice then the elements in A, to give no repeated element in AB, are easily verified to be only of the form $a^\alpha, a^\alpha bc$ or $a^\alpha b, a^\alpha c$. Thus if every α_i occurs twice bc is a period of A. From

$$\left(\sum_{i=1}^{2p^2} x^{\alpha_i}\right)\left(\sum_{i=1}^{2p} x^{\lambda_i}\right) \equiv 4\left(1+x+\dots+x^{p^3-1}\right)\left(\mathrm{mod}\,(x^{p^3}-1)\right)$$

and $F_{p^3}(x) \mid \sum_{i=1}^{2p^2} x^{\alpha_i}$ it follows that $F_{p^2}(x)$ or $F_p(x)$ divides

$\sum_{i=1}^{2p^2} x^{\alpha_i}$ and that the other of these two polynomials divides $\sum_{i=1}^{2p} x^{\lambda_i}$. If $F_{p^2}(x)$ divides $\sum_{i=1}^{2p^2} x^{\alpha_i}$ then $F_{p^3}(x)\, F_{p^2}(x) = (1+x^p+\dots+x^{p^2-p})$ divides $\sum_{i=1}^{2p^2} x^{\alpha_i}$. Since $\sum_{i=1}^{2p^2} x^{\alpha_i}$ has degree less than p^3 it follows that the other factor has degree less than p. Therefore this factor has non-negative coefficients and the sum of its coefficients is two. If one coefficient is two every number α_i occurs twice and A is periodic. If each coefficient is one every number α_i occurs once only and A is periodic. From

$$\Big(\sum_{i=1}^{2p^2} (\rho^p)^{\alpha_i}(-1)^{\beta_i}\Big)\Big(\sum_{i=1}^{2p} (\rho^p)^{\lambda_i}(-1)^{\mu_i}\Big) = 0$$

it follows that $F_{p^2}(x)$ divides $\sum_{i=1}^{2p^2} x^{\alpha_i}(-1)^{\beta_i}$ or $\sum_{i=1}^{2p} x^{\lambda_i}(-1)^{\mu_i}$.

If $F_{p^2}(x)$ divides $\sum_{i=1}^{2p^2} x^{\alpha_i}(-1)^{\beta_i}$ then $F_{p^3}(x)\, F_{p^2}(x)$ divides $\sum_{i=1}^{2p^2} x^{\alpha_i}(-1)^{\beta_i}$. The degree of the remaining factor is again less than p. It follows again that every α_i occurs once only or that every α_i occurs precisely twice and so that A is periodic. It may therefore be assumed that $F_{p^2}(x)$ divides $\sum_{i=1}^{2p} x^{\lambda_i}$ and $\sum_{i=1}^{2p} x^{\lambda_i}(-1)^{\mu_i}$. Each number λ_i occurs twice. Therefore the numbers λ_i are congruent to 0, 0, p, p, ..., p^2-p, p^2-p modulo p^2. Therefore the corresponding coefficients in the second polynomial are equal. Thus the pairs of numbers μ_i are either always both 0, or are always 0 and 1. In the first case the corresponding numbers ν_i are 0 and 1 and c is a period of B. In the second case, from the four possibilities stated previously, only

a^{λ}, $a^{\lambda}b$ and $a^{\lambda}bc$, $a^{\lambda}c$ are possible. Therefore b is a period of B.

This completes the proof.

COROLLARY. A group G of type $\{p^2, 2, 2\}$, where p is an odd prime, is good.

Proof. This follows from the preceding theorem and Theorem 4 of (1, p.263).

CHAPTER V

Introduction

In his paper (5, p.161) Hajós gives a method which, he claims, will give all factorisations of good groups. In this chapter it is pointed out that a correction is needed in his work. The corrected method is then stated and a complete proof is given, since Hajós has not given full details of his proof. In the next part a result of Hajós on the infinite cyclic group and Theorem 3.2 are used, together with the above method, to give all factorisations of the infinite cyclic group in which the number of elements in one factor is a power of a prime. In this part of the work the integers are used as the representation of the infinite cyclic group and the additive notation is used. The necessary changes in the various definitions and results which are needed are assumed to be made to fit in with this notation. The first result of this chapter is a consequence of the work of de Bruijn on bad groups and of most of the results in Chapters II, III and IV of this thesis.

Factorisation of Good Groups

THEOREM 5.1 A group G is bad if and only if it possesses a proper subgroup H admitting of factorisations $H = AB = AC$ where A is non-periodic and B and C have no periods in common.

Proof. By Theorem 2.1 a group G with this property is bad.

Further, by the results of Chapters 3 and 4, the only bad groups are those which follow from the Theorems quoted or proved in Chapter II. In Theorem 2.2 the subgroup K is shown to have the required property. In Theorem 1 of (1, p.260) $H = AC_1 = AC_2$ and it is shown that A is non-periodic while C_1 and C_2 have no period in common. In Theorem 2 (1, p.261) it is easily verified that $H = AH_1 = AH_2$, that A is non-periodic and that H_1 and H_2 have no common period. In Theorem 3 (1, p.262) it is easily verified that $K = AV_1 = AV_2$, that A is non-periodic and that V_1 and V_2 have no common period. It only remains to show that the group H of type $\{2, 2, 2, 2, 2\}$ admits of such factorisations. Using the notation of (1, p.262) it can be verified that A as given, $B_1 = (e, s, t, st)$ and $B_2 = (e, u, v, uv)$ are such that $H = AB_1 = AB_2$ with A non-periodic and B_1 and B_2 having no common period.

This completes the proof.

The open question stated at the end of the "Remark" in (1, p.261) is answered in the negative by Theorem 4.3 where it was shown that a group of type $\{2^2, 2, 2, 2\}$ is good. Theorem 2.2 gives the necessary requirements for a group to be bad containing subgroups of the type in question.

LEMMA 5.2 If a subset A of a group G is periodic then the set of all periods of A, together with the identity e form a subgroup H of G and there is a subset C of A such that $A = HC$.

Proof. Let H be the set of all periods of A, together with e. Then, if g and h are elements of H,

$$(gh)\,A = g\,(hA) = g\,A = A.$$

Therefore gh is an element of H. It follows that H is a subgroup of G. Let a_1 be any element of A. Then ha_1 is in A for all elements h in H. Therefore $Ha_1 \subseteq A$. If $Ha_1 \neq A$ let a_2 be any element of A not in Ha_1. Then $Ha_2 \subseteq A$ and Ha_1 and Ha_2 have no element in common. For, if $h_1 a_1 = h_2 a_2$ with h_1 and h_2 in H, then $a_2 = h_2^{-1} h_1 a_1$ is in Ha_1, which is not so. If $H(a_1, a_2) \neq A$ then let a_3 be any element of A not in $H(a_1, a_2)$. As above $Ha_3 \subseteq A$ and $H(a_1, a_2)$ and Ha_3 have no element in common. Continuing in this way, since A has only a finite number of elements, there exists $(a_1, a_2, \ldots, a_m)$ such that $H(a_1, \ldots, a_m) = A$.

THEOREM 5.3 If G is a good group then all factorisations $G = AB$ of G are given by

$$A = K_1 . K_2 \circ K_3 . \ \ldots \ \overset{\cdot}{\circ} K_m ,$$

$$B = K_1 \circ K_2 . K_3 \circ \ \ldots \ \underset{\cdot}{\circ} K_m ,$$

where, in each factor, the bracketing is from the left, i.e. there are $(m - 1)$ brackets before K_1 and one each after $K_2, \ldots, K_m$, and for each j, $j = 1, 2, \ldots, m$, $H_j = K_j K_{j+1} \ldots K_m$ is a subgroup of G, $H_2 = G$, and K_1 has one element only.

Proof. The proof is by induction on the order of G. Let G be of prime order. Then the only subgroups are G and (e) and the only factorisations are $G = gG$, where g is an element of G. But if $n = 2$, $K_2 = G$ and $K_1 = g_1$, which is the only possibility with K_2 strictly containing K_1, then $A = g_1 G = G$ and

$B = g_1 \circ G = g_1 g_2 = g$, where g is any element of G, as required.

Let G be a good group of order n. It is assumed that the theorem is true for groups of order less than n. By Theorem 4 of (1,p.263) all subgroups of G are good. Any quotient group of G by a subgroup H is isomorphic to some subgroup of G and so is good. Let AB = G. Then A or B is periodic. Since G is abelian it may be supposed that A is periodic. Let H be the set of periods of A, together with the identity e. Then, by Lemma 5.2, H is a subgroup of G and there is a subset C such that A = HC.

Then G = AB = HCB. Therefore CB is a set of coset representatives for G / H. Let $\bar{b}$ and $\bar{c}$ denote the cosets corresponding to b and c. Let $\bar{B}$ and $\bar{C}$ be the subsets of cosets corresponding to B and C respectively. Then $\bar{B}.\bar{C} =$ G / H. But G / H is good and of smaller order than G. Therefore there exist subsets $K_1H/H, K_2H/H, \ldots, K_mH/H$ such that $(K_jH/H)\ldots(K_mH/H) = H_j/H$ is a subgroup of G / H for each $j, j = 1,2,\ldots,m$, $H_2/H = G / H$ and such that

$$\bar{B} = (K_1H/H) \underset{\cdot}{\circ} (K_2H/H) \overset{\cdot}{\circ} (K_3H/H) \underset{\cdot}{\circ} \ldots \cdot (K_mH/H),$$

$$\bar{C} = (K_1H/H) \overset{\cdot}{\circ} (K_2H/H) \underset{\cdot}{\circ} (K_3H/H) \overset{\cdot}{\circ} \ldots \circ (K_mH/H).$$

The notation is used to indicate that if a circle occurs in the product for $\bar{B}$, then a dot occurs in the corresponding position in the product for $\bar{C}$ and vice versa. The circle occurs in the last position in the product for $\bar{C}$, since, if a dot occurred here, every element of K_m would be a period of A. Since $\bar{B}$ and $\bar{C}$ are subsets of cosets it follows that $\mathcal{B} = (K_1 \underset{\cdot}{\circ} K_2 \dot{\circ} K_3 \underset{\cdot}{\circ} \dots \cdot K_m) \circ H$ and $C = (K_1 \dot{\circ} K_2 \underset{\cdot}{\circ} K_3 \dot{\circ} \cdots \circ K_m) \circ H$ where this notation is used to indicate that B is one of the possible sets indicated and so also is C. Then

$$A = ((K_1 \dot{\circ} K_2 \underset{\cdot}{\circ} K_3 \dot{\circ} \cdots \circ K_m) \circ H).H = K_1 \dot{\circ} K_2 \underset{\cdot}{\circ} \cdots \circ K_m . H$$

Let $H = K_{m+1}$. Then

$$A = K_1 \dot{\circ} K_2 \underset{\cdot}{\circ} K_3 \dot{\circ} \cdots \circ K_m . K_{m+1},$$

$$\mathcal{B} = K_1 \underset{\cdot}{\circ} K_2 \dot{\circ} K_3 \underset{\cdot}{\circ} \cdots \cdot K_m \circ K_{m+1}.$$

Furthermore $K_j \dots K_m . K_{m+1} = H_j$, if $j = 1, 2, \dots, m$ and H_j is a subgroup of G and $H_2 = G$. $K_{m+1} = H$ and so is a subgroup of G.

This completes the proof.

In his statement of the theorem Hajós said that the sets K_j were themselves subgroups of G. That this need not be so is seen by considering any group of type $\{p^\lambda\}$, where p is a prime and $\lambda \geqslant 2$. Then $G = (e)$. G is the only product of subgroups equal to G. Thus the only factorisations given by the method of Hajós are G = gG, which are clearly not the only possible factorisations.

In the result as stated each K_j is a set of coset representatives for H_j by H_{j-1}, $j = 2, \dots, m$. Since all sets of coset representatives for quotient groups of finite abelian groups have been determined, the method does give all factorisations of the group. The subgroups H_j can be any chain of subgroups such that $G = H_2 \supset H_3 \supset \dots \supset H_m \supset (e)$. The order of A, in the statement of the theorem, will be the product of the orders of K_1, K_2, K_4, ... etc., and the order of B will be the product of the orders of K_1, K_3, K_5, ... etc.

Hajós (4, 160-1) has shown that if in a factorisation of the set I of integers one of the factors is finite then the other is periodic. Thus if A and B are sets of integers such that A + B = I in the sense that every integer d can be expressed uniquely as $a + b = d$ with $a \in A$ and $b \in B$, and the number of elements of A is finite, then there exists an integer $n > 0$ such that, if $b \in B$, then $b + n \in B$. As before it may be assumed that 0 is in A and B. If the number of elements of A is finite it may be assumed that 0 is the least element in A. If n is a period of B and B_n denotes the set of integers b in B such that $0 \leqslant b < n$ then B is the union of the sets $B_n + k$ where k is $0, \pm 1, \dots$

Let A + B = I, where the number of elements in A is a power of a prime. Consider $A + B_n$ added modulo n Every integer d such that $0 \leqslant d < n$ occurs in A + B. Let $a_1 \in A$ and $b_1 \in B$ be such that $a_1 + b_1 = d$. Then there exists an element $b \in B_n$ such that $b \equiv b_1$ (mod n). Therefore $a_1 + b \equiv d$ (mod n). No two elements of $A + B_n$ can be congruent modulo n. For if $a_2 + b_2 \equiv a_3 + b_3$ (mod n) with $0 \leqslant b_2 < n$, $0 \leqslant b_3 < n$ and so $a_2 \neq a_3$, it follows that there exists an integer k_2 such that $a_2 + (b_2 + k_2 n) = a_3 + b_3$ which is not possible since $b_2 + k_2 n$ is in B. Therefore $A + B_n \equiv I_n$, modulo n, where I_n is the set of integers between 0 and n-1 considered modulo n and thus is a cyclic group of order n. It follows by Theorem 3.2 that A or B_n is periodic.

If B_n is periodic with period m, then $m < n$ and m is a period of B. It may be assumed that A is periodic. If m is a period of A then $A \equiv A_m + (0, m, \ldots, (\frac{n}{m}-1)m)$ (modulo n) where A_m is the set of elements of A congruent modulo n to numbers less than m. Then it can be shown that $A_m + B_n \equiv I_m$ (modulo m). The number of elements of A_m is a divisor of the number of elements in A and so is also the power of a prime. Thus again Theorem 3.2 can be applied and one factor or the other is periodic. The argument can now be repeated and this is precisely the condition necessary for the proof of Theorem 5.3 to go through. Thus, in additive notation, the formulae of Theorem 5 3 give all sets A and B_n (modulo n). Letting n run through all multiples of the order of A all such factorisations are obtained.

As shown above the method also gives all factorisations of a finite cyclic group in which the number of elements in one factor is a power of a prime. If the number of elements in A is a power of a prime and

$$A = K_1 . K_2 \circ K_3 . \ldots$$

then since the order of A is the product of the orders of $K_2, K_4,$ ..., etc., the orders of $K_2, K_4, \ldots$ must be powers of this prime and so there is a restriction on the orders of alternate quotient groups in the chain $G = H_1 = H_2 \supset H_3 \supset \ldots \supset H_m \supset (e)$.

CHAPTER VI

Introduction

When Hajós discovered that not all groups are good, i.e. that there exist groups G and factorisations $AB = G$ in which neither A nor B is periodic, he put forward the following conjecture - if G is a group and $G = AB$ then one or other of the factors, say B, is quasi-periodic. Such a set B is said to be quasi-periodic if there exists an integer m greater than 1 and elements g_i such that $B = B_1 + B_2 + \dots + B_m$ and $AB_i = g_i AB_1$ where the elements g_i form a subgroup of G.

No fundamental result on quasi-periodicity is proved in this thesis. But it is shown that the factorisations of groups of one of the types which have been shown to be bad in it, namely those of type $\{p^\lambda, 2, 2\}$, where p is an odd prime, do indeed possess this property.

The Quasi-periodicity of certain Types of Groups

THEOREM 6.1 If a group G is good and $G = AB$ then one of the factors is quasi-periodic.

Proof. Since G is good one of the factors, say A, is periodic. Then, by Lemma 5.2, there exists a subgroup H greater than (e) such that $A = HC$. Let the elements of H be $g_1, \dots, g_m$, with $g_1 = e$. Let $A_j = g_j C$ for $j = 1, \dots, m$. Then

$A_j B = g_j CB = g_j A_1 B$ for $j = 1, \ldots, m$ and H is a subgroup with $m > 1$, as required.

THEOREM 6.2 If G is a group of type $\{p^\lambda, 2, 2\}$ where p is an odd prime and $AB = G$ then one of the factors is quasi-periodic.

Proof. Let a, b and c be generators of G of orders p^λ, 2 and 2 respectively. Let ρ be a primitive root of unity of order p^λ. Let

$$A = \sum a^{\alpha_i} b^{\beta_i} c^{\gamma_i} \ ; \ B = \sum a^{\lambda_i} b^{\mu_i} c^{\nu_i}.$$

It is not necessary to specify the numbers of elements in A and B.

From $AB = G$ it follows that

$$(\sum \rho^{\alpha_i})(\sum \rho^{\lambda_i}) = (\sum \rho^{\alpha_i}(-1)^{\beta_i})(\sum \rho^{\lambda_i}(-1)^{\mu_i}) =$$
$$= (\sum \rho^{\alpha_i}(-1)^{\gamma_i})(\sum \rho^{\lambda_i}(-1)^{\nu_i}) = (\sum \rho^{\alpha_i}(-1)^{\beta_i+\gamma_i})(\sum \rho^{\lambda_i}(-1)^{\mu_i+\nu_i}) = 0.$$

Therefore $F_{p^\lambda}(x)$ divides $\sum x^{\alpha_i}$ or $\sum x^{\lambda_i}$, $\sum x^{\alpha_i}(-1)^{\beta_i}$ or $\sum x^{\lambda_i}(-1)^{\mu_i}$, $\sum x^{\alpha_i}(-1)^{\gamma_i}$ or $\sum x^{\lambda_i}(-1)^{\nu_i}$, and $\sum x^{\alpha_i}(-1)^{\beta_i+\gamma_i}$ or $\sum x^{\lambda_i}(-1)^{\mu_i+\nu_i}$.

It may be assumed, without loss of generality, that $F_{p^\lambda}(x)$ divides $\sum x^{\alpha_i}$. Then if the exponent α occurs precisely t times in $\sum x^{\alpha_i}$ so also do the exponents $\alpha + p^{\lambda-1}, \alpha + 2p^{\lambda-1}, \ldots, \alpha + (p-1)p^{\lambda-1}$, where $0 \leqslant \alpha < p^{\lambda-1}$. From $(\sum x^{\alpha_i})(\sum x^{\lambda_i}) \equiv 4(1 + x + \cdots + x^{p^\lambda - 1}) (\mathrm{mod}\,(x^{p^\lambda} - 1))$, it follows that $F_{p^\mu}(x) \mid \sum x^{\alpha_i}$ or $\sum x^{\lambda_i}$ where $1 \leqslant \mu \leqslant \lambda$, but that it does not divide both as $p^{\lambda+1}$ does not divide $4p^\lambda$. Therefore $F_{p^\lambda}(x)$ does not divide $\sum x^{\lambda_i}$.

Suppose that $F_{p^\lambda}(x)$ divides two of the other polynomials derived from B. Since any two of b, c and bc generate the subgroup of type $\{2, 2\}$, it may be assumed without loss of generality that $F_{p^\lambda}(x)$ divides $\sum x^{\lambda_i}(-1)^{\mu_i}$ and $\sum x^{\lambda_i}(-1)^{\nu_i}$. Then if $0 \leq \alpha < p^{\lambda-1}$ the coefficients of $x^{\alpha}, x^{\alpha+p^{\lambda-1}}, \dots, x^{\alpha+(p-1)p^{\lambda-1}}$ in each polynomial are equal. If the coefficient is even then the number of α's occurring is even. If the coefficient is odd then the number of α's occurring is odd. Let some coefficient be odd, then x^{α} occurs once or three times and so do $x^{\alpha+p^{\lambda-1}}, \dots, x^{\alpha+(p-1)p^{\lambda-1}}$. Let $\alpha_i = \beta$ occur in $\sum x^{\alpha_i}$. Then $\alpha+(p-1)p^{\lambda-1}+\beta$ occurs as an exponent in the product $(\sum x^{\alpha_i})(\sum x^{\lambda_i})$ as $(\alpha+(p-1)p^{\lambda-1})+\beta$, $(\alpha+(p-2)p^{\lambda-1})+(\beta+p^{\lambda-1}), \dots, \alpha+(\beta+(p-1)p^{\lambda-1})$. Thus it occurs at least p times and if more than p times, from exponents occurring three times in $\sum x^{\lambda_i}$, it occurs p + 2k times. If it arises also from even coefficients then it occurs an even number of times from these. But it occurs four times and p + 2k cannot equal four. Therefore every coefficient of x^{α} is even. If the coefficient is not zero then $x^{\alpha}, x^{\alpha+p^{\lambda-1}}, \dots, x^{\alpha+(p-1)p^{\lambda-1}}$ must each occur at least twice and so, as above, some coefficient in $(\sum x^{\alpha_i})(\sum x^{\lambda_i})$ occurs at least 2p times, which is not possible. Therefore every coefficient is zero. If x^{α} occurs four times then, since the pairs (μ_i, ν_i) occurring with $\lambda_i = \alpha$ must be distinct, they are (0,0) (0,1) (1,0) and (1,1). If x^{α} occurs twice then the numbers μ_i are 0 and 1 and the numbers ν_i are 0 and 1. It follows that bc is a period of B. Therefore, by Theorem 6.1, B is quasi-periodic.

The other cases to be considered are that in which $F_{p^\lambda}(x)$ divides one polynomial arising from B and that in which $F_{p^\lambda}(x)$

divides every polynomial arising from A.

Let $F_{p^\lambda}(x)$ divide $\sum x^{\alpha_i}$, $\sum x^{\alpha_i}(-1)^{\beta_i}$, $\sum x^{\alpha_i}(-1)^{\gamma_i}$ and $\sum x^{\alpha_i}(-1)^{\beta_i+\gamma_i}$. Suppose that the exponent α occurs k times among the exponents α_i. Then so also does the exponent $\alpha + l p^{\lambda-1}$. The coefficientsof $x^{\alpha}, x^{\alpha+p^{\lambda-1}}, \dots, x^{\alpha+(p-1)p^{\lambda-1}}$ in $\sum x^{\alpha_i}(-1)^{\beta_i}$, $\sum x^{\alpha_i}(-1)^{\gamma_i}$ and $\sum x^{\alpha_i}(-1)^{\beta_i+\gamma_i}$ are equal in each polynomial. Therefore there are k_1 exponents $\beta_i = 0$ k_2 exponents $\gamma_i = 0$ and k_3 exponents $\beta_i+\gamma_i$ congruent to 0 modulo 2 corresponding to $\alpha_i = \alpha + l p^{\lambda-1}$ for each l. Let the pair (β,γ) occur $x_{\beta,\gamma}$ times among the pairs (β_i,γ_i) occurring with $\alpha_i = \alpha + l p^{\lambda-1}$. Then the following equations arise.

$$x_{0,0} + x_{0,1} = k_1 \quad ; \quad x_{1,0} + x_{1,1} = k - k_1 \; ;$$

$$x_{0,0} + x_{1,0} = k_2 \quad ; \quad x_{0,1} + x_{1,1} = k - k_2 \; ;$$

$$x_{0,0} + x_{1,1} = k_3 \quad ; \quad x_{0,1} + x_{1,0} = k - k_3 \, .$$

But adding the equations involving $x_{\beta,\gamma}$ and subtracting $x_{0,0} + x_{0,1} + x_{1,0} + x_{1,1} = k$ it is seen that these equations have a unique solution. Therefore the same pairs (β_i, γ_i) arise with $\alpha_i = \alpha + l p^{\lambda-1}$ for all l. It follows that $a^{p^{\lambda-1}}$ is a period of A. Therefore, by Theorem 6.1, A is quasi-periodic.

In the remaining case it may be assumed that $F_{p^\lambda}(x)$ divides $\sum x^{\alpha_i}$, $\sum x^{\alpha_i}(-1)^{\beta_i}$, $\sum x^{\alpha_i}(-1)^{\gamma_i}$ and $\sum x^{\lambda_i}(-1)^{\mu_i+\nu_i}$.

Then using the same notation as in the previous paragraph the first four equations above are obtained. But no result concerning k_3 arises. It is shown that a unique solution holds in all but one of the possible cases. Since no element occurs twice in A, $x_{\beta,\gamma}$ is equal to 0 or 1 and so $0 \leqslant k \leqslant 4$, $0 \leqslant k_1 \leqslant 2$, $0 \leqslant k_2 \leqslant 2$. Then

$$x_{0,0} + x_{0,1} = k_1 \quad ; \quad x_{1,0} + x_{1,1} = k - k_1 \ :$$

$$x_{0,0} + x_{1,0} = k_2 \quad ; \quad x_{0,1} + x_{1,1} = k - k_2 \, .$$

If $k = 0, 1, 3, 4$ then some k_i or some $k-k_i$ is equal to 0 or 2. Therefore the two numbers $x_{\beta,\gamma}$ in the corresponding equation are both 0, if k_i or $k-k_i = 0$, and both 1 if k_i or $k-k_i = 2$. Substituting these results into the other equations a unique solution is obtained for any such fixed set k, k_1 and k_2. If $k = 2$ and some k_i or $k-k_i$ is 0 or 2 the solution is unique as above. But if $k = 2$, $k_1 = k_2 = 1$ then $x_{0,1} = x_{1,0}$ and $x_{0,0} = x_{1,1}$ but $x_{0,1} = x_{1,0} = 1, x_{0,0} = x_{1,1} = 0$ and $x_{0,1} = x_{1,0} = 0, x_{0,0} = x_{1,1} = 1$ are both possible solutions. To the first solution correspond the elements $a^{\alpha + l_1 p^{\lambda-1}} b$, $a^{\alpha + l_1 p^{\lambda-1}} c$ and to the second correspond the elements $a^{\alpha + l_3 p^{\lambda-1}}$, $a^{\alpha + l_3 p^{\lambda-1}} bc$. If only these types occur then bc is a period of A and, by Theorem 6.1, A is quasi-periodic. However for certain α these types may occur and for other α different values of k, k_1 and k_2 may give rise to different types. In this case A need not be periodic.

Such a set A is now split up into p disjoint subsets. Let A_j be the set of elements $a^{\alpha_i} b^{\beta_i} c^{\gamma_i}$ such that $(j-1) p^{\lambda-1} \leqslant \alpha_i < j p^{\lambda-1}$.

Then $A = A_1 + A_2 + \dots + A_p$. Let $g_j = a^{(j-1)p^{\lambda-1}}$. Then $A_j = g_j A_1$, except for those sets in A arising from $k = 2$, $k_1 = k_2 = 1$, as shown above. Let C_j be the subset of A_j arising from this case. Now $F_{p^\lambda}(x)$ divides $\sum x^{\lambda_i}(-1)^{\mu_i+\nu_i}$ and therefore the coefficients of $x^\alpha, x^{\alpha+p^{\lambda-1}}, \dots, x^{\alpha+(p-1)p^{\lambda-1}}$ in this polynomial are equal. As has already been shown from consideration of the exponents in $(\sum x^{\alpha_i})(\sum x^{\lambda_i})$ the coefficient of each x^α in $\sum x^{\lambda_i}(-1)^{\mu_i+\nu_i}$ must be zero. Since $k = 2$, no number λ_i can occur more than twice. Therefore $\lambda_i = \beta$ occurs twice or not at all. If it occurs twice the corresponding numbers $\mu_i + \nu_i$ are 0 and 1 (modulo 2). Then the corresponding elements in B are $a^\beta bc, a^\beta b ; a^\beta bc, a^\beta c ; a^\beta, a^\beta b$ or $a^\beta, a^\beta c$ It is easily verified that the product of any one of these pairs with $a^{\alpha+lp^{\lambda-1}}b, a^{\alpha+lp^{\lambda-1}}c$ or with $a^{\alpha+lp^{\lambda-1}}, a^{\alpha+lp^{\lambda-1}}bc$ is $a^{\alpha+\beta+lp^{\lambda-1}}$, $a^{\alpha+\beta+lp^{\lambda-1}}b$, $a^{\alpha+\beta+lp^{\lambda-1}}c$, $a^{\alpha+\beta+lp^{\lambda-1}}bc$. Therefore $C_j B = g_j C_1 B$. It follows that $A_j B = g_j A_1 B$. The elements $g_1, \dots, g_p$ form a subgroup as required. Therefore A is quasi-periodic.

CHAPTER VII

Introduction

In this chapter extensions of some of the preceding results on finite abelian groups to certain infinite abelian groups are considered. The result of Hajós on the infinite cyclic group has already been mentioned. Results similar to this are proved for groups of type $\{p^{\infty}\}$ and for certain direct sums of groups of this type with finite abelian groups. A generalisation of Theorem 3.2 to such groups is proved. Throughout the chapter it is assumed that one of the factors has a finite number of elements: cases in which both factors are infinite are not considered.

Factorisations of certain Infinite Groups

The group of type $\{p^{\infty}\}$ may be defined multiplicatively as the set of all p^{λ}-th roots of unity, where $\lambda = 0, 1, 2, \ldots$, and p is a prime; see, for example, Kaplansky (7, p.4). Every element of this group has finite order, this being a power of p, and every proper subgroup is finite, being a cyclic group of order p^{λ}, for some fixed integer λ. If a and b are two elements of orders p^{λ} and p^{μ} respectively, where $\lambda > \mu$, then ab has order p^{λ}. For $(ab)^{p^{\mu}} = a^{p^{\mu}} \neq e$. Therefore the order is p^{ν} where $\nu > \mu$. Then $(ab)^{p^{\nu}} = a^{p^{\nu}} = e$. Therefore $\nu \geq \lambda$. But $(ab)^{p^{\lambda}} = e$. Thus $\nu = \lambda$. If a and b have the same order, it is not possible to specify the order of ab without further knowledge of the elements, but it is less than or equal to the order of a and b.

The problem of the factorisation of such a group is similar to that of a finite group and the definitions are carried over from that case.

THEOREM 7.1 If G is a group of type $\{p^\infty\}$, where p is a prime, and $AB = G$, where the number of elements in A is finite, then either A or B is periodic.

Proof. Since the number of elements in A is finite and every element has finite order there exists an integer λ such that the order of every element of A is less than or equal to p^λ. For each positive integer μ let B_μ be the set of all elements of B of order less than or equal to p^μ. Let $B - B_\mu$ denote the remaining elements of B. Let $\mu \geqslant \lambda$. Then no element of order less than or equal to p^μ arises from $A(B - B_\mu)$. Also no element of order greater than p^μ arises from AB_μ. Therefore, since $AB = G$, AB_μ is equal to the set of all elements of G of order less than or equal to p^μ. Thus $AB_\mu = H_\mu$, where H_μ is the subgroup of G of type $\{p^\mu\}$.

Let g be an element of G of order p^μ. Then g generates H_μ. Let $A = \sum g^{\alpha_i}$ and $B_\mu = \sum g^{\beta_i}$. Let $A(x) = \sum x^{\alpha_i}$ and $B_\mu(x) = \sum x^{\beta_i}$. Then

$$A(x) . B_\mu(x) \equiv (1 + x + \dots + x^{p^\mu - 1} \chi \bmod (x^{p^\mu} - 1)).$$

Therefore $F_{p^\mu}(x)$ divides $A(x)$ or $B_\mu(x)$. If $F_{p^\mu}(x)$ divides

$A(x)$ then $g^{p^{\mu-1}}$ is a period of A. Therefore, it may be assumed, that $F_{p^\mu}(x)$ divides $B_\mu(x)$. Thus $g^{p^{\mu-1}}$ is a period of B_μ. But $g^{p^{\mu-1}}$ is of order p. It follows that all powers of $g^{p^{\mu-1}}$, and so all elements of G of order p, are periods of B_μ. This is true for all $\mu \geqq \lambda$. Let b be any element of B. Then, since b has finite order, there exists an integer $\mu \geqq \lambda$ such that b is in B_μ. Therefore if h is any element of G of order p, hb is in B_μ and so in B. It follows that h is a period of B.

THEOREM 7.2 If G is a direct sum of a group of type $\{p^\infty\}$ and a group of type $\{q\}$ where p and q are distinct primes, and $AB = G$, where A has a finite number of elements, then either A or B is periodic.

Proof. Let H be the subgroup of G of type $\{p^\infty\}$ and K the subgroup of type $\{q\}$. Then G is the direct sum of H and K. Thus any element of G can be expressed uniquely as an element of H multiplied by an element of K.

Let $A = \sum h_i k_i$ where the elements h_i are in H and the elements k_i are in K. Since the number of elements in A is finite there exists an integer λ such that every h_i occurring in the expression for A has order less than or equal to p^λ. For each positive integer μ let B_μ denote the set of elements b of B such that the greatest power of p dividing the order b is less than or equal to p^μ. Let $B - B_\mu$ denote the remaining elements of B. For each $\mu \geqq \lambda$, $A(B-B_\mu)$ contains no element whose order is not divisible by $p^{\mu+1}$ and AB_μ contains no element whose order is divisible by $p^{\mu+1}$. Since $AB = G = H.K$ it follows that $AB_\mu = H_\mu.K$ where H_μ is the subgroup of H of type $\{p^\mu\}$. Thus $H_\mu.K$ is a group of type $\{p^\mu, q\}$. By Theorem 4 of (2, p.376) it follows that A or B_μ is periodic. If A is not periodic then B_μ is periodic for every integer μ greater than or equal to λ. Since any power of a period of B_μ is also a period it follows that either every element of G of order p is a period or that every element of G of order q is a period. If g_1 and g_2 are elements of G of orders p and q respectively then, for every $\mu \geq \lambda$, g_1 or g_2 is a period of B_μ. It follows that one of them is a period infinitely many times. Let this element be g_i. Then for any number $\mu \geq \lambda$ there exists a number $\nu \geq \mu$ such that g_i is a period of B_ν. Let b be any element of B. Then b is of finite order. By the above argument there exists $\nu \geq \lambda$ such that b is in B_ν and g_i is a period of B_ν. Therefore $g_i b$ is in B_ν and so is in B. Thus g_i is a period of B.

This completes the proof.

THEOREM 7.3 If G is a direct sum of a group of type $\{2^\infty\}$ and a group of type $\{2\}$ and $AB = G$, where A has a finite number of elements, then either A or B is periodic.

Proof. Let H be the subgroup of type $\{2^\infty\}$ and K the subgroup of type $\{2\}$ such that G is the direct sum of H and K. Let $A = \sum h_i k_i$ where the elements h_i are in H and the elements k_i are in K. Since A has a finite number of elements there exists an integer λ such that every h_i occurring in the expression for A has order less than or equal to 2^{λ}. For each positive integer μ let B_{μ} be the set of elements $b = hk$ of B, where $h \in H$ and $k \in K$, such that the order of h is less than or equal to 2^{μ}. Then, as in the previous theorem, $AB_{\mu} = H_{\mu}.K$ for all $\mu \geqslant \lambda$, where H_{μ} is the subgroup of H of type $\{2^{\mu}\}$. Then by Theorem 4.7 either A or B_{μ} is periodic. If A is not periodic then B_{μ} is periodic for all $\mu \geqslant \lambda$. Since any power of a period of B_{μ} is also a period of B_{μ} it follows that B_{μ} has a period of order two. But in G there are only three elements of order two. Therefore one of these is a period of B_{μ} for an infinite number of μ. As in the previous proof, this element is a period of B.

This completes the proof.

These three theorems show that in the three cases where an arbitrary positive integer λ occurs in the expression for a type of good finite abelian group the integer λ may be replaced by ∞ provided that one of the factors is still finite. In the next theorem it is shown that this is also true for Theorem 3.2.

THEOREM 7.4 If G is the direct sum of groups of type $\{p_i^{\lambda_i}\}$ where $i = 1, \ldots, k$ and the numbers p_i are different primes and the exponents λ_i are positive integers or infinity, $AB = G$ and the number of elements of A is a power of a prime, then either A or B is periodic.

Proof. Let $G = H_1 . H_2 \ldots H_k$ where for each i, H_i is a group of type $\{p_i^{\lambda_i}\}$. Then every element g of G can be expressed uniquely as $g = h_1 h_2 \dots h_k$ where, for each i, h_i is in H_i. Let $A = \sum_j h_{1j} h_{2j} \dots h_{kj}$ where h_{ij} is in H_i for each i. Then, since the number of elements in A is finite, for each i, there exists an integer ν_i such that every h_{ij} in the expression for A has order less than or equal to $p_i^{\nu_i}$. Let $B_{\mu_1,\dots,\mu_k}$ be the set of elements b of B such that $b = h_1 h_2 \dots h_k$ where h_i is in H_i and has order less than or equal to $p_i^{\mu_i}$, where the numbers μ_i are non-negative integers less than or equal to λ_i. Let $B - B_{\mu_1,\dots,\mu_k}$ be the remaining elements of B.

Suppose that $\lambda_i \geqslant \mu_i \geqslant \nu_i$ where μ_i is an integer for i = 1, 2, ..., k. Let H_{i,μ_i} denote the subgroup of H_i of order $p_i^{\mu_i}$. Then $A(B - B_{\mu_1,\dots,\mu_k})$ contains no element of $H_{1,\mu_1} H_{2,\mu_2} \dots H_{k,\mu_k}$ but every element of $A B_{\mu_1,\dots,\mu_k}$ is in $H_{1,\mu_1} H_{2,\mu_2} \dots H_{k,\mu_k}$. Therefore, since AB = G, $A B_{\mu_1,\dots,\mu_k} = H_{1,\mu_1} \dots H_{k,\mu_k}$. Since the numbers p_i are distinct primes $H_{1,\mu_1} \dots H_{k,\mu_k}$ is a finite cyclic group. Since the number of elements in A is a power of a prime and, from above, divides $\prod_{i=1}^{k} p_i^{\mu_i}$ it may be assumed that A has p_1^{ν} elements, where $\nu \leq \lambda_1$.

It is necessary to use the precise result contained in the proof of Theorem 3.2. Let g generate $H_{1,\mu_1} \dots H_{k,\mu_k}$. Let

$$A = \sum g^{\alpha_i} \; ; \; B_{\mu_1,\dots,\mu_k} = \sum g^{\beta_i} \; ;$$

$$A(x) = \sum x^{\alpha_i} \; ; \; B_{\mu_1,\dots,\mu_k}(x) = \sum x^{\beta_i} .$$

Let $\prod_{i=1}^{k} p_i^{\mu_i} = N$ and $\prod_{i=2}^{k} p_i^{\mu_i} = M$. Then the results proved in Theorem 3.2 are as follows. If $F_N(x) \mid A(x)$ then g^{N/p_1} is a period of A: if $F_{p_1^{\mu_1}d}(x) \mid B_{\mu_1,\ldots,\mu_k}(x)$ for every divisor d of M, g^{N/p_1} is a period of $B_{\mu_1,\ldots,\mu_k}$: if $F_{p_1^{\mu_1}u}(x) \mid A(x)$ where $1 \leq u < M$ and u is the greatest divisor of M such that $F_{p_1^{\mu_1}u}(x) \mid A(x)$ then $g^{p_1^{\mu_1}u}$ is a period of $B_{\mu_1\ldots\mu_k}$. It may be assumed that A is not periodic and so that $F_N(x)$ does not divide $A(x)$.

Let $\tau_1, \ldots, \tau_k$ be integers such that $\lambda_i \geq \tau_i \geq \mu_i$ and $\sum_{i=1}^{k} \tau_i > \sum_{i=1}^{k} \mu_i$. Let $\prod_{i=1}^{k} p_i^{\tau_i-\mu_i} = n$. Let $\prod_{i=2}^{k} p_i^{\tau_i-\mu_i} = m$. Then, as before, it follows that $A\,B_{\tau_1,\ldots,\tau_k} = H_{1,\tau_1} \cdots H_{k,\tau_k}$. Let h generate $H_{1,\tau_1} \cdots H_{k,\tau_k}$ such that $h^n = g$. Then $A = \sum g^{\alpha_i} = \sum h^{n\alpha_i}$ and $B_{\tau_1,\ldots,\tau_k} = \sum h^{\gamma_i}$. Let $A^*(x) = \sum x^{n\alpha_i} = A(x^n)$ and $B_{\tau_1,\ldots,\tau_k}(x) = \sum x^{\gamma_i}$.

Since $F_N(x)$ does not divide $A(x)$ it follows that $F_N(x^n)$ does not divide $A(x^n)$ and so, by Lemma 1.5, $F_{Nn}(x)$ does not divide $A^*(x)$. $\prod_{d|M} F_{p_1^{\mu_1}d}(x)$ divides $B_{\mu_1,\ldots,\mu_k}(x)$ if and only if $F_{p_1^{\mu_1}}(x)$ does not divide $A(x)$. $F_{p_1^{\mu_1}}(x)$ does not divide $A(x)$ if and only if $F_{p_1^{\mu_1}}(x^{p_1^{\tau_1-\mu_1}m})$ does not divide $A(x^n) = A^*(x)$. But, by Lemma 1.6, $F_{p_1^{\mu_1}}(x^{p_1^{\tau_1-\mu_1}m}) = \prod_{d|m} F_{p_1^{\tau_1}d}(x)$. Therefore if $\prod_{d|M} F_{p_1^{\mu_1}d}(x)$ divides $B_{\mu_1,\ldots,\mu_k}(x)$, $F_{p_1^{\tau_1}}(x)$ does not divide

$A^*(x)$. It follows by the results in Lemma 3.2 that $\prod_{d|Mm} F_{p_1^{T_1}d}(x)$ divides $B_{T_1,\ldots,T_k}(x)$ and so that h^{Nn/p_1} is a period of $B_{T_1,\ldots,T_k}$ But $h^{Nn/p_1} = g^{N/p_1}$. Therefore if g^{N/p_1} is a period of $B_{\mu_1,\ldots,\mu_k}$ it is also a period of $B_{T_1,\ldots,T_k}$ for all $T_i \geq \mu_i$ and so is a period of B. If $F_{p_1^{\mu_1}u}(x) | A(x)$ where $1 \leq u < M$ and $u|M$ then $F_{p_1^{\mu_1}u}(x^n) | A(x^n)$. But, by Lemma 1.6, $F_{p_1^{T_1}ud}(x)$ divides $F_{p_1^{\mu_1}u}(x^n)$ for every divisor d of m. If for some divisor c of mM which is not a divisor of u m, $F_{p_1^{T_1}c}(x) | A^*(x)$ then by the results of Theorem 3.2, $F_{p_1^{T_1}lm}(x) | A^*(x)$ where lm is the lowest common multiple of um and c. Then $F_{p_1^{T_1}d}(x) | A^*(x)$ for every divisor d of lm. But $\prod_{d|m} F_{p_1^{T_1}lm}(x) = F_{p_1^{\mu_1}l}(x^n)$ by Lemma 1.6. Therefore $F_{p_1^{\mu_1}l}(x^n)$ divides $A(x^n)$ and so $F_{p_1^{\mu_1}l}(x)$ divides A(x) and from the above u/l. Therefore if u is the greatest divisor of M such that $F_{p_1^{\mu_1}u}(x) | A(x)$ then um is the greatest divisor of mM such that $F_{p_1^{T_1}um}(x) | A^*(x)$. Therefore if $g^{p_1^{\mu_1}u}$ is a period of $B_{\mu_1,\ldots,\mu_k}$, $h^{p_1^{T_1}um}$ is a period of $B_{T_1,\ldots,T_k}$ for all $T_i \geq \mu_i$. But $h^{p_1^{T_1}um} = h^{n p_1^{\mu_1}u} = g^{p_1^{\mu_1}u}$. Therefore $g^{p_1^{\mu_1}u}$ is a period of B.

This completes the proof.

BIBLIOGRAPHY

(1) BRUIJN, N.G. de On the factorisation of finite abelian groups, Indag. Math. Kon. Ned. Akad. Wetensch. Amsterdam, 15 (1953), pp. 258-264.

(2) BRUIJN, N.G. de On the factorisation of cyclic groups, Indag. Math. Kon. Ned. Akad. Wetensch. Amsterdam, 15 (1953), pp. 370-377.

(3) BRUIJN, N.G. de On bases for the sets of integers, Publ. Math. Debrecen, 1 (1950), pp. 232-242.

(4) HAJÓS, G. Über einfache und mehrfache Bedeckung des n - dimensionalen Raumes mit einem Würfelgitter, Math. Zeitschrift, 47 (1941), pp. 427-467.

(5) HAJÓS, G. Sur la factorisation des groupes abéliens. Casopis Pest. Mat. Fys. 74 (1950), pp. 157-162.

(6) HAJÓS, G. Sur le problème de factorisation des groupes cycliques. Acta Math. Acad. Sci. Hungar. 1 (1950), pp. 189-195.

(7) KAPLANSKY, I. Infinite Abelian Groups, University of Michigan Publ. 2 (1954).

(8) RÉDEI, L. Zwei Lückensätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gaussischen Summen, Acta Math. 79 (1947), pp. 273-290.

(9) RÉDEI, L. Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen, Acta Math. Acad. Sci. Hung. 1 (1950), pp. 197-207.

(10) VAN DER WAERDEN, B.L. Moderne Algebra, Vol. I, Berlin (1930).