Lectures on
Topics In The Theory of Infinite Groups

By

B.H. Neumann

Notes by

M. Pavman Murthy

Tata Institute of Fundamental Research, Bombay
1960
(Reissued 1968)

Preface

As the title of this course of lectures suggests, my aim was not a system- 1
atic treatment of infinite groups. Instead I have tried to present some of the methods and results that are new and look promising, and that have not yet found their way into the books of Kurosh, Specht, Zassenhaus, Marshall Hall, Jr. The contents of Chapters 8, 10, 11, 12 were mostly still unpublished at the time of the lectures; those of Chapters 8 and 12 have recently appeared. All through the lectures I have drawn attention to the numerous problems that still defy our efforts at solution. The Theory of Groups is still very much alive today.

This course was delivered during the monsoon term, 1959, and extended over 36 lectures. I enjoyed every one of them. I am profoundly grateful to Professor K. Chandrasekharan for inviting me to spend this term at the Tata Institute of Fundamental Research. I also wish to record my gratitude to Mr. Pavman Murty, who took the notes and prepared them for circulation.

B.H. Neumann.
The University,
MANCHESTER, 13,
ENGLAND.
December, 1959.

Contents

Chapter 1

Introduction, Definitions and Notations

1 Abstract Algebras

In this chapter we shall derive certain properties of groups and fix certain 2
notations.

Let E be any set and Ω a set of functions defined on the *Cartesian products*

$$E^o = \{\phi\}, E, E^2, \ldots E^n, \ldots$$

with values in E, where ϕ denotes the empty set and

$$E^n = \left\{(x_1, \ldots, x_n) \middle| x_i \in E, i = 1, \ldots n\right\}.$$

The pair (E, Ω) is called an *algebraic system* or an *abstract algebra*. E is called the *carrier* of the algebra (E, Ω) and the elements of Ω are called *operators*.

If $\omega \in \Omega$ is a function on E^n with values in E, we say that ω is in *n-ary operator* . Thus if ω is an n-ary operator, then

$$\omega(x_1, \ldots, x_n) \in E, \text{ for all } (x_1, \ldots, x_n) \in E^n.$$

A *nullary operator* is a function on the set $\{\phi\}$ with value in E. Thus if ω is a nullary operator then it is a function with the argument ϕ and with value in E. We denote this value by $\in \{ \}$.

We shall use the terms *unary* and *binary* operators for 1-ary and 3
2-ary operators respectively.

2 Groups

We are here interested in a particular class of algebraic system called groups.

Definition. A group (G, Ω) is an algebraic system with G as its carrier and Ω consisting of a nullary operator $\in$, an unary operator L and a binary operator π, related by the following laws:

(1) $\pi\,(x, \pi\,(y, z)) = \pi\,(\pi\,(x, y), z)$, for every $x, y, z \in G$ (Associative Law);

(2) $\pi\,(x, L(x)) = \in \{\ \}$, for every $x \in G$;

(3) $\pi\,(x, \in \{\ \}) = x$, for every $x \in G$.

We shall for convenience write,

$$\begin{aligned} \pi(x,y) &= xy, \\ L(x) &= x^{-1}, \\ \in \{\} &= 1. \end{aligned}$$

In this notation, it is customary to call xy the product elements x and y. The above three laws read as follows when written multiplicatively.

(1′) $x(yz) = (xy)z$, (Associative law)

(2′) $xx^{-1} = 1$,

(3′) $x1 = x$.

4 Because of (3′) we say that 1 is a *right neutral* element. Similarly as suggested by (2′)x^{-1} is a *right inverse* of x. For the sake of brevity we shall identify the group (G, Ω) with its carrier G and refer to G as a group through this chapter.

If a group G in addition to the above three laws satisfies

(4) $\pi\,(x, y) = \pi\,(y, x)$, for all $x, y \in G$ (Commutative law)

or

(4′) $xy = yx$ (in the multiplicative notation)

then G is an *abelian group* (or a *Commutative group*).

For the abelian group it is sometimes convenient to use the following additive notation

$$\begin{aligned} \pi(x, y) &= x + y \\ L(x) &= -x \\ \in \{\,\} &= 0. \end{aligned}$$

3 Some elementary properties of groups

(1) In the definition of a group the associative law is formulated for products of three elements of G. One can prove by induction on the number of factors that the corresponding law holds for products of any finite number of factors; in other words, the product will be independent of the way in which the brackets are inserted. The brackets are, therefore, irrelevant and will later on usually be omitted. The proof of the general associative law is straight forward and we omit it.

(2) The right neutral element $'t'$ is also a left neutral element; in other **5**
words,

$$1x = x, \text{ for all } x \in G.$$

Proof. From law (3′), it follows that

$$11 = 1,$$

then

$$\begin{aligned} 1(xx^{-1}) &= xx^{-1} && \text{from } (2'), \\ (1x)x^{-1} &= xx^{-1} && \text{from} (1'). \end{aligned}$$

□

Therefore,

$((1x)x^{-1})(x^{-1})^{-1} = (xx^{-1})(x^{-1})^{-1}$, where $(x^{-1})^{-1}$ is the right inverse of x^{-1}.

An application of the associative law gives,

$$(1x)(x^{-1}(x^{-1})^{-1}) = x(x^{-1}(x^{-1})^{-1}),$$

and therefore

$$(1x)1 = x1 = x.$$

Finally, by another application of the associative law,

$$1(x1) = 1x = x$$

This proves (2).

6 (3) The right inverse x^{-1} is also a left- inverse of x; in other words,

$$x^{-1}x = 1, \text{ for all } x \in G.$$

Proof. $(x^{-1}x)x^{-1} = x^{-1}(xx^{-1}) = x^{-1}1 = x^{-1}$.

Therefore,

$$((x^{-1}x)x^{-1})(x^{-1})^{-1} = x^{-1}(x^{-1})^{-1} = 1,$$
$$(x^{-1}x)(x^{-1}(x^{-1})^{-1}) = x^{-1}(x^{-1})^{-1} = 1.$$

Hence, $(x^{-1}x)1 = 1$,

$$x^{-1}x = (x^{-1}x)1 = 1.$$

This proves (3). □

We say that 1 is a (two-sided) neutral element or unit element, now that it is both left neutral and right neutral. Similarly x^{-1} is an inverse of x.

(4) There is only one right neutral element in G. For let n be any right neutral element. An application of (2) immediately gives

$$n = 1n = 1.$$

This, in particular proves that 1 is the only neutral element of G.

(5) The equation $ax = b$, with $a, b \in G$, has the unique solution $x = a^{-1}b$, in G. It is easy to verify that $a^{-1}b$ is a solution of the above equation. Now if x and y are two solutions of the equation, we have

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1y = y.$$

This proves the uniqueness. **7**

Thus in a group the left cancellation law holds. Dually it follows that the right cancellation law also holds. As a consequence of (5), x^{-1} is the only inverse of x and also x is the inverse of x^{-1}

4

We note that we have defined groups by postulates of the from "for all $x, y, z, \ldots, a$ certain equation is true". This does not mean that we have made no existential assumptions; but all existential assumptions have gone into the general algebraic frame work; that is to say, they are of the form "there is a nullary operator $\in$, a unary operator L", and so on. A class of algebraic systems that is singled out, like that of groups, by postulates of the form "for all $x, \ldots$, the equation $\cdots$ holds" is said to be *equation-ally defined*, or a *variety* of algebraic systems. Thus groups, as we have defined them, form a variety. Not all important and interesting classes of algebraic systems form varieties; thus e.g. the class of fields is not a variety. This will be shown later.

5 The multiplication of subsets of groups and its relation to the lattice operations

Let (E, Ω) be an algebraic system, $\omega \in \Omega$, an n-ary operator, $X_1, \ldots, X_n$, n subsets of the carrier E. We define the set

$$\omega(X_1, \ldots, X_n) \subseteq E \text{ by}$$
$$\omega(X_1, \ldots, X_n) = \left\{\omega(X_1, \ldots, X_n) \middle| x_i \in X_i, i = 1, \ldots, n\right\}.$$

8 Let G be a group, D, E and F subsets of G. Correspondingly we have

$$EF = \left\{ef \middle| e \in E, f \in F\right\},$$
$$E^{-1} = \left\{e^{-1} \middle| e \in E\right\}.$$

We denote the set $E\{f\}$ by Ef and similarly $\{e\}F$ by eF. Also we identify $\{e\}\{f\}$ with element ef.

Using the associativity of the multiplication of the elements of G it is easy to verify that the same holds for the multiplication of sets. In other words,

$$D(EF) = (DE)F, \text{ for } D, E, F \text{ subsets of } G.$$

Let $F \subseteq G$, $\{D_i\}_{i \in I}$ be a family of subsets of G; then

(1) $(\cup D_i)F = \cup D_i F$.

Proof. Let $g \in (\cup D_i)F$; then

$$g = df \text{ with } d \in \cup D_i,\ f \in F; \text{ now}$$
$$d \in D_j \text{ for some } j \in I; \text{ hence}$$
$$g = df \in D_j F \subseteq \cup D_i F,$$

and thus, as g was arbitrary,

$$(\cup D_i)F \subseteq \cup D_i F.$$

9 Conversely, if $g \in \cup D_i F$, then

$$g \in D_j F \text{ for some } j \in I;$$

thus
$$g = df \quad \text{with} \quad d \in D_j,\ f \in F,$$

Hence $d \in \cup D_i$, and therefore

$$g = df \in (\cup D_i)F, \text{ and again as } g \text{ was arbitrary},$$

$$\cup D_i F \subseteq (\cup D_i)F.$$

Combining this with the above inclusion we have the required equality.

In particular, we have

$$(D \cup E)F = DF \cup EF, \text{ for } D, E, F \subseteq G.$$

□

A similar straightforward verification shows that

(2) $(\cup D_i)F \subseteq \cap D_i F$.

In particular, we have

$$(D \cap E)F \subseteq DF \cap EF.$$

The following example demonstrates that in general inclusion cannot be replaced by equality in (2).

Take G to be the additive group of integers, and

$$E = \{1\}, D = \{-1\}, F = G, \text{then}$$
$$(D \cap E)F = \phi, \quad DF \cap EF = G.$$

10

6 Subgroups

Let $S \subseteq G$, and

(1) $\in \{\,\} \in S$,

(2) $L(s)S$, for every $s \in S$,

(3) $\pi(s,t) \in S$, for every $s,t \in S$.

It is obvious that S is a group with the set of operators $\Omega = \left\{ \in, L, \pi \right\}$. We call S, a *subgroup* of G. It should be noted that by definition a subgroup is non-empty. If a subgroup S of G is a proper subset of G, we call it a *proper subgroup*.

Hereafter the notation "$S \leq G$" will be used for "S is a subgroup of G". When S is a proper subgroup of G, we shall write "$S < G$".

The definition of a subgroup is immediately seen to be equivalent to the following conditions.

(1′) $1 \in S$,

(2′) $S^{-1} \subseteq S$,

(3′) $SS \subseteq S$.

These three conditions can be replaced by the apparently weaker condition given in the following simple theorem.

Theorem 1. *The subset S of the group G is a subgroup if, and only if*

(i) $S \neq \phi$,

(ii) $SS^{-1} \subseteq S$.

11 Condition (ii) means that for any $s, t \in S$, the "right quotient" $st^{-1} \in S$: we then say that S is *closed* under right division. Similarly closure under left division can be defined.

Proof. The 'only if' part of the theorem is trivial. We proceed to prove the 'if' part. Since $S \neq \phi$, there is an element $x \in S$, and therefore by hypothesis

$$xx^{-1} = 1 \in S.$$

Now, for any $x \in S$,

$$1x^{-1} = x^{-1} \in S.$$

Further, if $x, y, \in S$, then by what we have just proved

$$y^{-1} \in S$$

and therefore,

$$xy = x(y^{-1})^{-1} \in S.$$

This proves that S is a subgroup. □

Also, by symmetry it follows that a non-empty subset of G, closed under left division is a subgroup.

In the above theorem instead of right or left division, we can also take their transposes. In other words, a non-empty subset S of G is a subgroup if and only if it is closed under one of the following four binary operations.

(1) $\varphi(x, y) = xy^{-1}$, (2) $\varphi^*(x, y) = y^{-1}x$,
(3) $\psi(x, y) = x^{-1}y$, (4) $\psi^*(x, y) = yx^{-1}$.

Graham Higman (Higman and Neumann, 1952) has suggested a **12**
more general problem which stands unsolved in the case of non-abelian groups.

Problem. Let φ be a binary operator (expressible in terms of ε, L, π and two variables) with the property that $S \subseteq G$ is a subgroup if only if

(1) $S \neq \phi$

(2) $\varphi(x, y) \in S$, for all $x, y \in S$.

What forms can φ take?

In the case of abelian groups it is proved that the only possibilities are the above four functions (which in this case reduce to only two functions, right and left division).

Nothing is known in the case of non-abelian groups.

Chapter 2

Generators and Relations

1

In this chapter we shall show how to construct the smallest subgroup 13
containing a given set of elements of group. The concept of relation will also introduced.

As an immediate consequence of the theorem of the last chapter, we have

Theorem 1. *The intersection of an arbitrary family of subgroups of a groups is a subgroup.*

Let G be a group and E a subset of G. The subgroup

$$gp(E) = \bigcap_{E \subseteq S \subseteq G} S$$

is the subgroup *generated by* E. We call E a set of *generators* of $gp(E)$. Since a subgroup by definition is non-empty, it follows that

$$gp(\phi) = \{1\}.$$

We call $\{1\}$ the *trivial subgroup* of G.

If X is any set, we denote by $|X|$ its cardinal.

If $E \subseteq G$ and $|E| < \mathfrak{X}_\circ$, then $gp(E)$ is *finitely generated*. Similarly, $gp(E)$ is countably generated if $|E| \leq \mathfrak{X}_\circ$.

If $|E| = 1$, then $gp(E)$ is a *cyclic group*.

We shall now construct $gp(E)$, given $E \subseteq G$. We construct a non- **14**
decreasing sequence of sets inductively. Put $E_1 = E \cup \{1\}$.

Having defined $E_1, \ldots, E_n$ define $E_{n+1} = E_n E_n^{-1}$ write $S = \bigcup_{n=1}^{\infty} E_n$. It is immediately seen that

$$E_1 \subseteq S.$$

Also, if T is an arbitrary subgroup of G containing E, then

$$E_1 \subseteq T.$$

If $E_n \subseteq T$, then also $E_{n+1} \subseteq T$.

It follows that

$$S \subseteq T \tag{1}$$

and thus

$$S \subseteq gp(E) = \bigcap_{E \subseteq T \leq G} T.$$

We now prove that S is a subgroup. S is non-empty and all the $E_n's$ contain 1. If $f \in E_n$, then

$$f.1^{-1} = f \in E_{n+1}.$$

Therefore $E_n \subseteq E_{n+1}$. Thus $\{E_n\}$ is a non-decreasing sequence of sets. Let $x, y, \in S$; so that $x \in E_m$, $y \in E_n$ for some m, n. Put $p = \max(m, n)$. Then, $x \in E_p, y \in E_p$ and hence $xy^{-1} \in E_{p+1} \subseteq S$. This proves that S is closed under right division. Therefore S is a subgroup
15 containing E. Thus, $gp(E) \subseteq S$, and combining this with (1), we get

$$S = gp(E).$$

2

The above construction shows that any element of E has a 'representation' in terms of elements of E as

$$w(e_1, \ldots, e_n) = e_1^{m_1} e_2^{m_2} \cdots e_n^{m_n}, m_i = \pm 1, e_i \in E, i = 1, \ldots, n.$$

Such expressions are called *words*. It is not assumed that differently indexed e_i are different. Different words may represent the same element. For example, $abb^{-1}c^{-1}$ and ac^{-1} are different words representing the same element ac^{-1}. The word containing no e at all is the *empty word*. This represents the unit element, and we therefore denote it (somewhat ambiguously) by 1. It is easy to see that any element of G that can be represented by a word in the elements of E is in $gp(E)$. Thus we have,

Theorem 2. *The subgroup $gp(E)$ consists of all the elements of G represented by the 'words' formed by the element of E.*

3

Cyclic groups are the simplest types of groups which one comes across. The theorem below gives the structure of subgroups of a cyclic group.

Theorem 3. *If G is cyclic, all subgroups of G are cyclic.*

Proof. Let $\{a\}$ be a generator of G. Then,

$$gp(\{a\}) = gp(a) = C.$$

□

Let S be a subgroup of G. If $= \{1\}$, it is cyclic as claimed. If **16**
$\{1\} < S \leq G$, then there is an element $a^k \in S$, $a^k \neq 1$; also, $a^{-k} \in S$. Let N be the set of positive integers defined by

$$N = \left\{ n \middle| a^n \in S \right\}$$

Since $k \in N$ or $-k \in N$, $N \neq \phi$. Denote by m the least positive integer in N. We claim that a_m is a generator of S.

Trivially,

$$gp(a_m) \leq S.$$

If $c = a^\ell \in S$, then $|\ell| \geq m$. Write

$$\ell = mq + r, 0 \leq r < m$$

Then $a^r = a^\ell a^{-mq} \in S$, and therefore $r = 0$. Hence $c = a^{mq} \in gp(a^m)$. Thus,

$$S \leq gp(a^m)$$

Combining this with the above inequality, we have

$$S = gp(a^m)$$

and the theorem is proved.

4

In this context, we ask the following question

17 **Problem.** What groups can be subgroups of two-generator groups?

A partial answer to this problem will be given now. It will be completely soled in the subsequent chapters.

Theorem 4. *Countably generated groups are countable.*

Let $G = gp(E)$, where E is countable. Let $E = \{e_1, e_2, \ldots\}$. We have seen that $gp(E)$ consists of all the elements represented by 'words' in $e_1, e_2, \ldots$.

If g is an element of G which can be represented by a word w in $e_1, e_2, \ldots$, then g can be written in the form

$$g = w = e_{i_1}^{m_1} e_{i_2}^{m_2} \cdot e_{i_\ell}^{m_\ell},$$

where the i_j are positive integers and m_i are integers, positive, zero, for negative. Note that different $w's$ can represent the same element. Corresponding to each m_i, we define

$$m_i^+ = \max(m_i, 0),$$
$$m_i^- = \max(-m_i, 0).$$

If $m_i \geq 0$, then $m_i^+ = m_i$, $m_i^- = 0$. If $m_i < 0$, then $m_i^+ = 0$, $m_i^- = -m_i$. Thus at most one of m_i^+, m_i^- is non-zero.

We now construct *a* $1-1$ mapping γ of the set of all $w's$ into the set of positive integers. This will prove that $gp(E)$ is countable.

18 We write $\gamma(1) = 1$. If $e_{i_1}^{m_1}\ e_{i_2}^{m_2} \cdot e_{i_\ell}^{m_\ell}$, then define $\gamma(w) = 2^{i_1} 3^{m_1^+} 5^{m_1^-} 7^{i_2}$ $11^{m_2^-} 13_2^{m^-} \dots p_{3\ell}^{m_\ell^-}$ where p_n denotes the n^{th} prime when the set of all positive primes is arranged in increasing order.

The numbers $\gamma(w)$ are called *Gödel numbers*.

Since every positive integer can be written as a product of prime powers uniquely, it follows that every positive integer is the Gödel number of *at most one* word; hence γ is $1-1$. Therefore the set of words in E, and also $gp(E)$, is countable.

Remark. This theorem can also be proved by making use of the construction we have given for $gp(E)$. That is to say,

$$gp(E) = \bigcup_{n=1}^{\infty} E_n,$$

where $E_1 = E \cup \{1\}$, $E_{n+1} = E_n E_n^{-1}$. If E is countable, so is E_1. If E_n is countable, so is E_{n+1} because $|E_{n+1}| \le |E_n^{-1}|\,|E_n^{-1}| = |E_n|^2$. Therefore all the $E_n's$ are countable, and so is their union $gp(E)$.

Corollary. *Necessary for a group to be embeddable in a two-generator group is that it be countable*

5

Let $G = gp(E)$ be a group with E as the set of generators. Then every element of G can be represented by a 'word' formed of some finite number of elements of E. We denote by $w(e_1, \dots, e_n)$ a word consisting 19
of the 'letters' $e_1, \dots, e_n$ only (not necessarily all). Let $w(e_1 \dots, e_n)$, $v(e_1^1, \dots, e_m^1)$ be two words in E. We say that

$$w(e_1, \dots, e_n) = v(e_1^1, \dots, e_m^1)$$

is a *relation* in G, if this equation holds when $w(e_1, \dots, e_n)$ and $v(e_1^{'}, \dots,$ $e_n')$ are considered as elements of G. Without loss of generality we can write the above relation in the form

$$w(e_1, \ldots, e_n) = v(e_1, \ldots, e_n).$$

In the subsequent pages $\underline{e}$ will stand for $(e_1, \ldots, e_n)$. We say that

$$w(\underline{e}) = u(\underline{e})$$

is a *trivial relation* if it follows from the group axioms and does not depend upon the particular group under consideration. For example,

$$e_1 e_2 e_2^{-1} e_3 e_4 e_4^{-1} = e_1 e_3 e_5 e_5^{-1}$$

is a trivial relation. A relation of the the type

$$e_1 e_2 = e_2 e_1,$$

if valid, is a non-trivial relation.

Let

$$w(e_1, \ldots, e_n) = e_1^{m_1} e_2^{m_2} \cdot e_n^{m_n}, m_i = \pm 1, e_i \in E, i = 1, \ldots, n$$

and $$v(f_1, \ldots, f_r) = f_1^{\ell_1} f_2^{\ell_2} \cdots f_r^{\ell_r}, f_i \in E, \ell_i = \pm 1, i = 1, \ldots, 2$$

20 be two words. By the *product* of the words w and v (taken in this order), we mean the word

$$v = w(e_1, \ldots, e_r) v(f_1, \ldots, f_r) = e_1^{m_1} e_2^{m_2} \cdots e_n^{m_n} f_1^{l_1}, \ldots, f_1^{l_r}$$

similarly the *inverse* of w is defined to be the word

$$w^{-1} = e_n^{-m_n} \cdots e_2^{-m_2} e_1^{-m_1}.$$

We now state certain elementary properties of relations which are immediate from the definitions given above.

(1) $v(\underline{e}) = v(\underline{e})$ is a trivial relation.

(2) If $u(\underline{e}) = v(\underline{e})$ is a relation, then so is $v(\underline{e}) = u(\underline{e})$.

(3) If $u(\underline{e}) = v(\underline{e})$ and $v(\underline{e}) = w(\underline{e})$ are relations, then so is $u(\underline{e}) = w(\underline{e})$.

(4) If $u(\underline{e}) = v(\underline{e})$ is a relation, then so is $u^{-1}(\underline{e}) = v^{-1}(\underline{e})$

(5) If $u(\underline{e}) = v(\underline{e})$ and $u'(\underline{e}) = v'(\underline{e})$ are relations then so is $u(\underline{e})u'(\underline{e}) = v(\underline{e})v'(\underline{e})$

(6) For any word $u(\underline{e})$,

$$u(\underline{e})u^{-1}(\underline{e}) = 1$$

is a trivial relation.

6

In what follows, we shall abbreviate $v(\underline{e})$ as v for convenience, when confusion is not possible. 21

we say that a relation

$$u^* = v^*$$

follows from (or is a consequence of) relations $u_1 = v_1, \ldots, u_r = v_r$, if it can be derived from these by a finite chain of applications of (1) - (6). We say that two relations $u = v$ and $u' = v'$ are equivalent if each follows from the other in the above sense.

Example. Every relation $u = v$ is equivalent to a relation of the form

$$w = 1.$$

We can in fact prove this with

$$w = uv^{-1}.$$

Suppose that $u = v$ is true. Then by (4), we have

$$u^{-1} = v^{-1}$$

An application of (2) gives

$$v^{-1} = u^{-1}$$

Also by (1),

$$u = u$$

is a relation. 22

Multiplying these two relations using (5), we get

$$uv^{-1} = uu^{-1}$$

By (6),
$$uu^{-1} = 1$$

is a relation. By the transitivity of relations ((3)), we have

$$uv^{-1} = 1.$$

Similarly we can prove that $uv^{-1} = 1$ implies that $u = v$.

Let $G = gp(E)$ be a group. Consider the set of relations valid in G. Let R be a set relations in the elements of E such that all relations in the elements of E follow from R.

We then say that R is a set of *defining relations* of the group with respect to the system to generators E. The group G is completely determined by E and R. We write

$$G = gp(E; R)$$

We call (E, R) a *presentation* of G.

G is *finitely presented* if there is some presentation $(E; R)$ of G with $|E| < \mathcal{N}_0$ and $|R| < \mathcal{N}_0$. Similarly a countably *presented* group is defined.

It is easy to see that all finite groups are finitely presented. An infinite cyclic group is also finitely presented.

23 There exist groups which are finitely generated but not finitely presented. Examples will be given later.

The following problem about finitely presented groups is unsolved.

Problem. What groups can be embedded in finitely presented groups? [1]

Not all countable groups can be embedded in finitely presented groups. But I know of no example of a countable group of which it can be proved that it cannot be embedded in a finitely presented group.

---

[1]* *note added November 1959.* A very significant advance towards a solution of this problem has recently been made by GRAHAM HIGMAN (unpublished). He has determined all finitely generated subgroups, and a large class of not finitely generated subgroups, of finitely presented groups.

7 The Word Problem for groups

In this section we give a brief account of what is known as the "Word Problem". This problem arose with the development of mathematical logic. A precise statement of the problem entirely depends upon a precise definition of the concept of a "procedure" (also, "algorithm", "rule", "effective procedure", "recurrive procedure", "computational procedure" of "process"), which was given by Church, Turing, Kleene and Post (see Kleene (1952)).

The Word Problem for groups

Given a group presentation $(E; R)$ of a group G, to give a "procedure" to decide, for any two words u^*, v^* in the elements of E, whether

$$u^*(e) = v^*(e)$$

is a consequence of the relations R. Here, roughtly speaking a "proce- **24**
dure" is a set of rules or instructions that could be so formulated as to be programmed for an automatic computer with the data E, R and u^*, v^* (suitably coded) and the computer so programmed as to answer by a somehow cased "follows" or "does not follow".

A similar problem can be formulated for other algebraic systems. Markov and Post have proved the insolubility of the word problem in associative systems. Turing (1950) proved the insolubility of the word problem for semi-groups with cancellations. (A semi-group with cancellation is an algebraic system with an associative binary operator, with the property)

$$\begin{aligned} &ax = bx \text{ implies } a = b, && \text{and} \\ &ya = yb \text{ implies } a = b, && \text{for all } x, y, a, b, \in S). \end{aligned}$$

The solubility of the word problem for groups has been proved in special cases. Magnus (1932) has constructed a procedure to solve the word problem for an arbitrary group with a single defining relation. Similarly V. A. Tartakovski (1949) - (1952), H. Sheik (1956) and

J. L. Britton (1956), (1957) have given solutions for the word problem in special classes of groups. However, the question of the existence of a procedure for the solution of the word problem for groups in general remained open until Novikov (1952), (1955), (1958) proved that in general the word problem for groups is not soluble. Later, Boone (1954) (1955) (1957) (1958) (1959) and Britton (1958) gave different proofs for the insolubility of the word problem for groups.

We conclude this chapter with a precise statement of the insolubility of the word problem for groups.

Theorem (Novikov, Boone, Britton). *There is a finite presentation* $(E; R)$ *such that the word problem is insoluble in the group*

$$G = gp(E; R),$$

in the sense that to every effective procedure M *that purports to solve the word problem for* G*, there is a word* $w_M(\underline{e})$ *such that the equation*

$$w_M(\underline{e}) = 1$$

defeats the procedure.

Chapter 3

Homomorphisms of Groups

1

We shall, in the this chapter introduce the concepts of homomorphism, isomorphism and other important mappings of a group into another group. 26

Let G and H be any two groups. A mapping φ if G into H is a *homomorphism* if it preserves the group operations. On the face of it φ has to satisfy

(i) $(\in \{\ \})^{\varphi} = \in \{\ \}$

(ii) $(l(g))^{\varphi} = l(g)^{\varphi}$, for every $g \in G$

(iii) $(\pi(g, g'))^{\varphi} = \pi(g^{\varphi}, g'^{\varphi})$, for all $g, g' \in G$.

To make the notation less clumsy, we have used the same symbols $\in, l, \pi$ for the operators of the groups G and H. These three conditions written in the multiplicative notation read as follows.

(a) $1^{\varphi} = 1$ (we use the same symbol '1' for the neutral elements of both G and H)

(b) $(g^{-1})^{\varphi} = (g^{\varphi})^{-1}$

(c) $(gg')^{\varphi} = g^{\varphi} g'^{\varphi}$

The definition of homomorphism given here is capable of generalisation, and thus we can speak of a homomorphism of an algebraic system into another. But, here we shall confine our attention to groups. In the case of groups conditions (a) and (b) are contained in (c). Thus we have

27 **Theorem 1.** *A mapping φ of a group G into a group H is a homomorphism if and only if it satisfies* (c).

Proof. If φ is a homomorphism of G into H, then trivially φ satisfies (c). □

Now, let φ be a mapping of G into H satisfying (c). We first observe that in a group the natural element is the only idempotent element. (An element x is *idempotent* if it satisfies the equation $x^2 = x$.) For if x is any idempotent element of a group, then

$$xx = x = x1;$$

therefore,
$$x = 1.$$

Now,
$$1^\varphi 1^\varphi = (11)^\varphi = 1^\varphi.$$

Therefore 1^φ is idempotent and hence the neutral element of H. Similarly

$$g^\varphi (g^{-1})^\varphi = (gg^{-1})^\varphi = 1^\varphi;$$

hence
$$(g^{-1})^\varphi = (g^\varphi)^{-1}.$$

Thus φ is a homomorphism of G into H.

28 Let X, Y be any two sets and θ a mapping of X into Y; further let $E \subseteq X$, $F \subseteq Y$. We define

$$E^\theta = \left\{ e^\theta \middle| e \in E \right\}$$
$$F^{\theta^{-1}} = \left\{ e \middle| e \in X, e^\theta \in F \right\}$$

The following two propositions are easy to verify.

Let φ be a homomorphism of a group G into another group H.

(A) If $S \leq G$, then $S^{\varphi} \leq H$

(B) If $T \leq H$, then $T^{\varphi^{-1}} \leq G$.

In particular,

$$\{1\}^{\varphi^{-1}} = N \leq G.$$

The subgroup $N \leq G$ is uniquely de terminal by φ and is called the *kernel* of the homomorphism.

A homomorphism φ or G into H is an *epimorphism* if it maps G *onto* H; in other words, if

$$G^{\varphi} = H.$$

A homomorphism φ of G onto H is a *monomorphism* if it is one-to-one (briefly $1-1$), i. e. $x^{\varphi} = y^{\varphi}$ implies $x = y$, for all $x, y \in G$. A homomorphism which is both an epimorphism and monomorphism is an *isomorphism*.

(C) If φ is an isomorphism of G onto$H$, then the inverse mapping φ^{-1} **29**
of φ exists and is an isomorphism of H onto G.

Proof. The equation

$$g^{\varphi} = h, \text{ with } g \in G, h \in H,$$

has one and only one solution in G. We define

$$h^{\varphi^{-1}} = g, \text{ if } g^{\varphi} = h.$$

The mapping φ^{-1} is 'onto', because for any $g \in G$, we have

$$(g^{\varphi})^{\varphi^{-1}} = g.$$

Also, if

$$\begin{aligned} h^{\varphi^{-1}} &= h'^{\varphi^{-1}}, \text{ with } h, h' \in H, \text{ and} \\ g^{\varphi} &= h,\ g'^{\varphi} = h', \text{ then} \\ g &= g', \quad \text{and therefore} \\ h &= g^{\varphi} = g'^{\varphi} = h'. \end{aligned}$$

Hence φ^{-1} is one-to-one. □

Now, let $h, h' \in H$, with $h = g^{\varphi}$, $h' = g'^{\varphi}$, then $(hh')^{\varphi^{-1}} = (g^{\varphi} g'^{\varphi})^{\varphi^{-1}} = gg' = h^{\varphi^{-1}} h'^{\varphi^{-1}}$. Hence φ^{-1} is an isomorphism of H onto G. It is easy to see that φ^{-1} is the two-sided inverse of φ, in other words; the composite mappings $\varphi\ \varphi^{-1}$ and $\varphi^{-1}\ \varphi$ are the identity mappings of G and H respectively.

30 We say that two groups G and H are *isomorphic* if there is an isomorphism φ of G onto H. We then write

$$G \cong H.$$

Let G, H and K be any three groups and φ and ψ be homomorphism of G into H and H into K respectively. Then we have

(D) The composite mapping $\varphi\psi$ of G into K is a homomorphism.

For let $g\ g' \in G$; then

$$(gg')^{\varphi\psi} = ((gg')^{\varphi})^{\psi} = (g^{\varphi} g'^{\varphi})^{\psi} = (g^{\varphi})^{\psi} = (g'^{\varphi})^{\psi} = g^{\varphi\psi} = g^{\varphi\psi}$$

In (D), if φ and ψ are isomorphisms then so is $\varphi\psi$. This is easy to verify.

It follows from the above considerations that isomorphism is an equivalence relation on the class of all groups. Thus, we have

(R) $G \cong G$;

(S) $G \cong H$ implies $H \cong G$;

(T) $G \cong G$ & $H \cong K$ implies $G \cong K$.

Let G be a group. A homomorphism of G into itself is an *endomorphism*. An isomorphism of G onto itself is an *automorphism*.

The product of two homomorphisms, or more generally, the product of two mapping is defined only under certain restrictions, viz. that the
31 range of the first mapping is contained in the domain of the second. This is, however, always the case for mapping of a set into itself.

By mere computation one can verify the associativity of the multiplication of mappings whenever the multiplication is defined.

Thus the set of all endomorphisms of a group G is closed under an associative binary operation and therefore forms an algebraic system called *semi-group*.

Now consider the set of all automorphisms of a group G. Trivially the identity mapping L belongs to this set and under the multiplication of automorphisms it acts as an unit element. By what we have already proved automorphism possesses a right inverse (in fact it is the two sided inverse) and the multiplication is associative.

Thus we have,

Theorem 2. *The set of all automorphisms of a group G forms a group.*

Let φ be an endomorphism of G possessing a left inverse θ and a right inverse ψ. Then φ is an automorphism and $\theta = \psi$. For if,

$$x_1^{\varphi} = x_2^{\varphi}, \text{ with } x_1, x_2 \in G$$

then,
$$(x_1^{\varphi})^{\theta} = (x_{\alpha}^{\varphi})^{\theta}$$

i.e.,
$$x_1 = x_1^{\varphi\theta} = x_2^{\varphi\theta} = x_2.$$

Therefore φ is 1-1. Further for any $x \in G$, we have **32**

$$(x^{\psi})^{\varphi} = x^{\psi\varphi} = x.$$

Therefore, φ is 'onto' and hence an automorphism. This, in turn, proves that $\theta = \psi$.

Thus we have proved that the automorphisms of G are precisely the endomorphisms having a left inverse and right inverse. But an endomorphism which is not an epimorphism may possess a left inverse which is not a right inverse. Similarly an endomorphism which is not a monomorphism can have a right inverse which not a left inverse.

Let X be any set. A mapping π of X into itself is a *permutation* if it is 1-1 and 'onto'. Thus every automorphism of a group G is a permutation of G.

With the usual techniques, we can verify the following:

Theorem 3. *The set of all permutations on X form a group with the composite of permutations as the binary operation.*

2 Equivalence relations and congruences

Let G and H be any two sets, not necessarily groups, φ, a mapping of G into H. We introduce an equivalence relation '$\sim$' as follows:

$$g \sim g' \text{ if and only if } g^{\varphi} = g'^{\varphi}.$$

It is immediate that '$\sim$' satisfies the following conditions:

33 (R) $g \sim g$;

(S) $g \sim g'$ implies $g' \sim g$, for all $g, g' \in G$;

(T) $g \sim g', g' \sim g''$ implies $g \sim g''$, for all $g, g', g'' \in G$.

Hence '$\sim$' is an equivalence relation.

Now let G and H be groups and φ a homomorphism of G into H. Then '$\sim$' in addition to R, S, T also satisfies the following condition:

$$g \sim g_1, g' \sim g'_1 \text{ implies } gg' \sim g_1 g'_1.$$

For

$$g^{\varphi} = g_1^{\varphi}, g'^{\varphi} = g_1'^{\varphi}.$$

Therefore,

$$(gg')^{\varphi} = g^{\varphi}\, g'^{\varphi} = g_1^{\varphi}\, g_1^{\varphi} = (g_1\, g'_1)^{\varphi}.$$

Further

$$g \sim g_1 \text{ implies } g^{-1} \sim g_1^{-1}$$

For $$g^{\varphi} = g_1^{\varphi} \text{ implies } (g^{-1}) = (g_1^{-1})^{\varphi}$$

Such an equivalence relation is called a *congruence*.

Definition. Let G be a group and '$\sim$' an equivalence relation satisfying the condition.

$$g \sim g', g_1 \sim g'_1 \text{ implies } gg_1 \sim g'g'_1$$

34 Then we call '∼' a congruence. Strictly speaking we should also demand that

$$g \sim g' \text{ implies } g^{-1} \sim g'^{-1}.$$

But in the case of groups our definition implies this. For if,

$$g \sim g', \text{ then}$$
$$g' \sim g$$

Now,

$$g^{-1} \sim g^{-1}$$

and therefore

$$g'\, g^{-1} \sim gg^{-1} = 1.$$

Again,

$$g'^{-1} \sim g'^{-1}.$$

Therefore

$$g^{-1} = g'^{-1}(g'g^{-1}) \sim g'^{-1}1 = g'^{-1}.$$

Let X be any set, φ a mapping of X into another set Y. We have seen that φ induces an equivalence relation '∼' in X. Every equivalence relation splits X into disjoint *blocks*. Let '∼' be any equivalence relation in X. Define, for $g \in X$

$$[g] = \left\{x \in XE \middle| x \in g\right\}.$$

Then clearly either

$$[g] \cap [h] = \phi,$$

or

$$[g] = [h].$$

Conversely every partition of X into blocks gives rise to an equivalence relation. To see this we have only to define "$x \sim y$ if and only if x, y belong to the same block". 35

Now let G be a group and '∼' a congruence relation in G. That is to say,

$$g \sim g_1, h \sim h_1 \text{ implies } gh \sim g_1\, h_1, \text{ for } g, h, g_1, h_1 \in G.$$

In this case the block $[gh]$ depends only on $[g]$ and $[h]$ and not on the particular element g and h. For if

$$[g] = [g']$$

and
$$[h] = [h']$$

then
$$[gh] = [g'h'].$$

This follows easily from the definition of a congruence in a group.

Now we shall prove that the product of $[g]$ and $[h]$ is again a block. In other words,

$$[g][h] = [gh]$$

Let, $p \in [gh]$, then $p \sim gh$. But

$$g^{-1} \sim g^{-1}.$$

Therefore

$$g^{-1}p \sim g^{-1}(gh) = h$$

36 Thus

$$p = g(g^{-1}p), \text{ with } g \in [g], g^{-1}p \in [h]$$

Hence

$$p \in [g][h]$$

thus

$$[gh] \subseteq [g][h]. \tag{1}$$

Conversely if $x =\in [g][h]$, then

$$x = g'h', \text{ with } g' \in [g], h' \in [h]$$

Hence

$$g'h' \sim gh, \quad \text{and}$$

therefore
$$x = g'h' \in [gh].$$

This gives

$$[g][h] \subseteq gh. \tag{2}$$

Combining this with (1) we have

$$[g][h] = [gh]$$

This multiplication of blocks turns the set of blocks into a group. We have

$$[1][g] = [1g] = [g]$$

Similarly 37

$$[g][1] = [g1] = [g],$$
$$[g][g^{-1}] = [gg^{-1}] = [1],$$
$$[g^{-1}][g] = [g^{-1}g] = [1]$$

The above equations prove the following theorem.

Theorem 4. *The books associated with a congruence in a group G from a group*

We denote this group by $G/\sim$. The block $[l]$ is the neutral element of this group and $[g^{-1}]$ is the inverse of $[g]$. We call $G/\sim$ the *quotient group* (also the *factor group*) with respect of the congruence '$\sim$'

The notion of congruence, as well as the notion of the quotient algebra with respect to a congruence, can be defined much more generally than for groups, namely for arbitrary algebraic systems.

In the case of groups, the book $[l]$ plays an important part. In fact we shall see that it completely determines the congruence associated with it.

We one define an epimorphism θ of G onto $G \sim$. Write

$$g^{\theta} = [g]$$

The equation

$$[gh] = [g][h]$$

demonstrates that θ is a homomorphism. Obviously θ is onto $G/\sim$ and 38
therefore θ is an epimorphism.

Consider now

$$\{[1]\}^{\theta^{-1}} = \left\{x \in G \middle| x^{\theta} = [1]\right\} = \left\{x \in G \middle| [x] = [1]\right\}.$$

We see from this that

$$\{[1]\}^{\theta-1} = [1] \text{ (considered as a set).}$$

Thus $[l]$ is the kernel of θ and we denote it by N.

Definition. Let $S \leq G$; then the set S_g is called a *right coset* of S. Similarly left cost coset is defined

We shall now prove that every block, with respect to a certain congruence is a right coset of the kernel of the epimorphism induced by the congruence under consideration.

Let '$\sim$' be a congruence in G and θ the corresponding epimorphism of G onto $G/\sim$, and again

$$N = [1] = [1]^{\theta^{-1}}.$$

Then

$$[g] = Ng;$$

for let $x \in Ng$; then

$$x = ng \quad \text{with} \quad n \in N.$$

39 Now,

$$n \sim 1, g \sim g, \quad \text{give}$$
$$ng \sim 1g = g$$

i.e.,
$$x = ng \in [g]$$

Therefore

$$Ng \subseteq [g]$$

Conversely if $x \in [g]$, then

$$x \sim g, g^{-1} \sim g^{-1} \text{ imply}$$

$$xg^{-1} \sim gg^{-1} = 1$$

Therefore $\quad x = (xg^{-1})g \in Ng.$

Thus

$$[g] \subseteq Ng, \text{ and it follows that}$$
$$[g] = Ng, \text{ as claimed}$$

Similarly

$$[g] = gN$$

Hence

$$Ng = [g] = gN.$$

Thus we have proved the following theorem. **40**

Theorem 5. *Let '$\sim$' be a congruence in G. The mapping θ of G into $G/\sim$ defined by*

$$g^{\theta} = [g] \text{ with } g \in G$$

is an epimorphism with kernel $N = [1]$. Further every element of $G/\sim$ is a right coset (left coset) of N. Also N commutes with every elements of G.

Let $\mathscr{R}$ be the set of all congruences in G. Every $\sim\in\mathscr{R}$ in a $1-1$ manner determines the associated natural epimorphism. Let $\mathscr{M}$ denoted the set of all such associated natural epimorphisms. Also every $\theta \in \mathscr{M}$ determines uniquely a kernel N. Let $\mathscr{N}$ be the of all such kernels. By the above theorem every $N \in \mathscr{N}$ determines completely all the blocks and therefore uniquely determines the associated congruences which in turn determines the natural epimorphism. The consideration above prove the following theorem.

Theorem 6. *There is a 'natural' 1-1 correspondence between $\mathbb{R}, \mathscr{M}$ and $\mathscr{N}$.*

Because of the above theorem we shall write G/N for $G/\sim$ where N is the kernel determined by $\sim$.

3 Factorisation of a homomorphism

We shall now show that every homomorphism of a group onto another can be factorised "canonically".

Theorem 7. *Let G and H be any two groups, φ a homomorphism of*
41 *G into H. Then φ can be factorised in the from $\varphi = \theta\psi$, where θ is the* canonical epimorphism *(or natural epimorphism) of Gonto $G/\sim$ $(= G/N)$, $\sim$ being the congruence determined by φ, and where ψ is a monomorphism of $G/\sim$ into H.*

Proof. Define ψ on $G/\sim$ with values in H by

$$[g]^{\psi} = g^{\varphi}$$

Let

$$[g] = [g']$$

then $$g \sim g'$$

and therefore $$g^{\varphi} = g'^{\varphi}.$$

This proves that ψ is a defined mapping. Further,

$$\begin{aligned}([g][h])^{\psi} &= ([gh])^{\psi} = (gh)^{\varphi}\\ &= g^{\varphi}h^{\varphi} = [g]^{\psi}[h]^{\psi}, \text{ for all } g, h \in G.\end{aligned}$$

Also ψ is 1-1. For if

$$\begin{aligned}&[g]^{\psi} = [h]^{\psi}, \text{ with } g, h \in G, \text{ then}\\ &g^{\varphi} = h^{\varphi}; \text{ that is}\\ &g \sim h \text{ and}\end{aligned}$$

42 therefore

$$[g] = [h].$$

Thus ψ is a monomorphism of $G/\sim$ into H. Now,

$$g^{\theta\psi} = [g]^{\psi} = g^{\varphi}, \text{ for all } g \in G.$$

Therefore

$$\varphi = \theta\psi$$

Hence the theorem. □

4 Normal subgroups

We now proceed to characterise the kernels of the homomorphisms of a group G. We have already seen that the kernel determined by a congruence in G commutes with all the elements of G. We shall prove that the kernel of any homomorphism of G has this property. The following establishes this.

Theorem 8. *Let G and H be any two groups, φ a homomorphism of G into H. Then the kernel of φ is also kernel N associated with the congruence '$\sim$' determined by φ.*

Proof.

$$\begin{aligned}\{1\}^{\varphi^{-1}} &= \left\{x \middle| x^{\varphi} = 1\right\} \\ &= \left\{x \middle| x^{\varphi} = 1^{\varphi}\right\} = \left\{x \middle| x \sim 1\right\} \\ &= [1] = \left\{1\right\}^{\theta^{-1}} = N.\end{aligned}$$

Thus the kernel of any homomorphism of the group G into H commutes with all the elements of G. **43**

□

We now make the following definition.

Definition. Let $N \leq G$. Then is a *normal subgroup* (also self-conjugate or invariant) of G (notation $N \triangle G$) if

$$Ng = gN \text{ for all } g \in G.$$

Thus the kernel of a homomorphism of G into H is a normal subgroup

Let $N \triangle G$. Define $x \sim y$ if and only if $xy^{-1} \in N$. A straight forward verification shows that '$\sim$' is a congruence relation in G. Further,

$$[1] = \left\{x \middle| x \sim 1\right\} = \left\{x \middle| x \in N\right\} = N$$

Hence we have

Theorem 9. *Every normal subgroup $N \triangle G$ determines a congruence '$\sim$' in G with*

$$[1] = N.$$

Corollary. *If $N \triangle G$, then N is the kernel of some homomorphism of G.*

Proof. We have only to consider the natural epimorphism θ of G onto $G/\sim = G/N$. Theorem 6 and Theorem 9 together imply □

Theorem 10. *Let $\mathscr{C}$ be the set of all congruences in G, $\mathscr{N}$ the set of all*
44 *normal subgroup of G. Then there is a $1-1$ mapping α of $\mathscr{C}$ onto $\mathscr{N}$, in a natural way.*

Proof. Define α as

$$\alpha(\sim) = \left\{x \middle| x \sim 1\right\} = [1] = N, \text{ for all } \sim \in \mathscr{C}$$

α serves our purpose. □

5 The graph of a binary relation

Let E be any set and '$*$' a binary relation in E. With every such relation there is associated a set $R \subseteq E \times E$, namely

$$R = \left\{(x, y) \middle| x * y, x \in E, y \in E\right\}.$$

The subset R is called the graph of the binary relation. Conversely to every $R \subseteq E \times E$ there is a binary whose graph is R; and this correspondence is $1-1$. We shall usually identify the binary relation '*' with its graph and refer to R itself as the binary relation. In particular, with this identification, an equivalence relation in E will be subset of $E \times E$. We shall now interpret the reflexive, symmetric and transitive laws in terms of the subset of the product set $E \times E$. We call the subset $\triangle \subseteq E \times E$, defined by

$$\triangle = \left\{(x, x) \middle| x \in E\right\}$$

the *diagonal* of $E \times E$.

Let $R \subseteq E \times E$, $S \subseteq E \times E$ be two binary relations in E. Then

$$R^{-1} = \Big\{(x, y) \Big| (y, x) \in R\Big\}$$

is the inverse of the relation R. By the *product* of the relations R and S 45
we mean the relation

$$RS = \Big\{(x, z) \Big| \exists y, y \in E, (x, y) \in R, (y, z) \in S\Big\}.$$

Let R be a binary relations in E. Then R is reflexive if and only in $\triangle \subseteq R$; also R is symmetric if and if $R^{-1} \subseteq R$; finally R is transitive if and only if $R^2 (= RR) \subseteq R$.Thus R is equivalence relation if and only if it has all three properties:

(R) $\triangle \subseteq R$,

(S) $R^{-1} \subseteq R$,

(T) $R^2 \subseteq R$.

It is immediate from the above definitions that

$$R\triangle = \triangle R = R, \text{ for all } R \subseteq E \times E.$$

Further the symmetric and transitive laws are in the equivalent to $R - R^{-1}$ and $R^2 = R$, respectively. The following fact is formally analogous to Theorem 1 of Chapter 1; we omit the proof.

Theorem 11. *$R \subseteq E \times E$ is an equivalence relation if and only if*

(1) $R \neq \phi$

(2) $RR^{-1} \subseteq R$.

6 The graph of a congruence in a group

Let G be a group. Before considering the congruences in a group, we shall introduce a group structure on the product set $G \times G$ in a natural 46
way. Define the unit element of $G \times G$ to be (1,1) with $1 \in G$, the inverse of (g, h) to be (g^{-1}, h^{-1}) and the product of (g, h) and (g', h') to be

$$(g, h)(g', h') = (gg', hh'), \text{ with } g, g', h, h' \in G.$$

It is easily seen that this turns $G \times G$ into a group. We call this group *the direct square* of G. In fact we can define the direct product of any family of groups. We shall have occasion to return to this topic later (See Chapter 6).

Let $R \subseteq G \times G$ be a congruence in G. Since

$$\triangle \subseteq R,$$

it follows that

$$(1, 1) \in R.$$

If

$$(g, h) \in R \text{ and } (g', h') \in R \text{then}$$
$$g \sim h \text{ and } g' \sim h'.$$

Therefore

$$gg' \sim hh'; \text{ that is}$$
$$(gg', hh') \in R.$$

Thus

$$(g, h)(g', h') = (gg', hh') \in R.$$

47 Further if $(g, h) \in R$, then

$$g \sim h \text{ and therefore}$$
$$g^{-1} \sim h^{-1}; \text{ that is}$$
$$(g^{-1}, h^{-1}) \in R.$$

Thus we have proved that R is a subgroup of $G \times G$, that is in symbols

$$R \leq G \times G.$$

Conversely reversing the above arguments we can prove that if R is an relation and $R \leq G \times G$, then R is a congruence in G. Thus we have following theorem.

Theorem 12. *The equivalence relation $R \subseteq G \times G$ is a congruence in G if and only if $R \leq G \times G$*

7 The lattice of congruences and normal subgroups

Let R, S be two binary relations in E. By the *intersection* of relations R and S, we mean the relation whose graph is $R \bigcap S$. The following theorem is an immediate consequence of the definition of an equivalence relation.

Theorem 13. *The intersection of any family of equivalence relations in E is an equivalence relation.*

Let S be any binary relation in E. Then
$R = R(S) \bigcap_{S \subseteq R_i} R_i$ is the equivalence relation *generated by S* where 48
R_i runs all the equivalence relations containing S. In particular,

$$R(\phi) = \triangle$$

is the *identity relation*.

In general, the union of two equivalence relations need not be an equivalence relation. We make the following definition.

Definition. Let $\{R_i\}_{i \in I}$ be a family of equivalence relations. The *join* of $\{R_i\}_{i \in I}$ is the equivalence relation generated by $\bigcup_{R_i}$.

The discussion above, leads to the following theorem.

Theorem 14. *The set of all equivalence relation in E is a lattice on $E \times E$ with "$\subseteq$ in EXE" as the partial order.*

In this case, the 'cap' and 'cup' operations are the set intersection and the 'join' as we have defined above.

Let us turn to groups. Let G be a group. Similar to Theorem 13, we have for congruences the following theorem.

Theorem 15. *The intersection of any family of congruences in G is again a congruence.*

Thus we can now speak of *the congruence generated by a binary relation* in G. As in the case of equivalence relations we can similarly define the join of a family of congruences in G. Note, however, that "join" means different things according as we deal with the lattices of equivalence or of congruences.

49 Analogous to Theorem 14 is the following theorem.

Theorem 16. *The set R of all congruences in a group G is a lattice on $G \times G$ with "$\subseteq$ in $G \times G$" as the partial order.*

Of course, the 'cap' and the 'cup' operations again are the set intersection and the join. The lattice of congruences of a group have important properties. But we shall not discuss them here. We only mention that the lattice of congruences of a group G is not a sub-lattice of the lattice of equivalence relations.

Let us now consider the set $\mathscr{N}$ of all normal subgroups of G. We shall show that $\mathscr{N}$ is a lattice with set inclusion as the partial order. For this we need to following theorem, the proof of which is straightforward; and we omit it.

Theorem 17. *The intersection of a family $\{N_i\}_{i\in I}$ of normal subgroups is a normal subgroup.*

We can now speak of the normal subgroup generated by a subset of G. An an immediate consequence of this theorem we have

Theorem 18. *The set $\mathscr{N}$ of all normal subgroups of G is a lattice with inclusion as the partial order.*

Here again the 'cap' operations is the intersection and the 'cup' operation is the "join", where the join of a family of normal subgroups is the normal subgroup generated by the union of the groups of this family.

We have already need (Theorem 10) that there is natural 1-1 map-
50 ping λ of the set of all congruences in G onto $\mathscr{N}$. In fact this mapping is a lattice isomorphism of $\mathscr{R}$ onto $\mathscr{N}$. To prove this we have only to show that this mapping λ preserves the partial order.

Let $R \subseteq R'$ with $R, R' \in \mathscr{R}$, and $R^\lambda = N$, $R^\lambda = N'$. Then,

$$N = \left\{x \middle| (x, 1) \in R\right\} \subseteq \left\{x \middle| (x, 1) \in R'\right\} = N'$$

Thus we have,

Theorem 19. *The lattice $\mathscr{R}$ and $\mathscr{N}$ are isomorphic.*

8 Extension of a mapping of a set of generators of a group to a homomorphism

Let $G = gp(E)$ and $H = gp(F)$ be groups and φ an arbitrary mapping of E into F. Under what conditions can φ be extended to a homomorphism of G into H? In other words, when can a homomorphism ψ of G into H exists, with

$$e^\psi = e^\varphi, \text{ for all } e \in E?$$

Further if such a mapping ψ exists, is it unique? The mapping φ induces, in a natural way, a mapping φ^* on the set of all words in E with values in H; namely

$$\begin{aligned} &(w(\underline{e}))\varphi^* = w(\underline{e}^\varphi), \text{ where} \\ &\qquad \underline{e}^\varphi = (e_1, \ldots, e_n)^\varphi = (e_1^\varphi, \ldots, e_n^\varphi), e_i \in E, i = 1, \ldots, n. \end{aligned}$$

In general φ^* need not be a well define mapping of G. For an element 51
of G may have more than one word representation it and it is bot always true that the images by φ^* of all these words are the same elements of H. Whenever φ^* induces a mapping on G, we shall denote the induced mapping also by φ^*.

Suppose now, that φ can be extended to a homomorphism ψ of G into H. Let $g = w(\underline{e}) \in G$. Then

$$g^\phi = (w(\underline{e}))^\psi = w(\underline{e}^\psi) = w(\underline{e}^\varphi).$$

This shows that φ^* induces a mapping on G and that ψ coincides with φ^*. Conversely let φ^* induce a mapping on G. If $g = w(\underline{e})$, $h = u(\underline{e})$, then $g^{\varphi^*} = w(\underline{e}^\varphi)$, $h^{\varphi^*} = u(\underline{e}^\varphi)$; and $(gh)^{\varphi^*} = (w(\underline{e})u(\underline{e}))^{\varphi^*} = w(\underline{e}^\varphi)u(\underline{e}^\varphi) = g^{\varphi^*}h^{\varphi^*}$. Hence φ^* is a homomorphism of G into H. Thus we have proved the following theorem.

Theorem 20. *The mapping φ can be extended to a homomorphism of G into H if and only if φ^* induces a mapping on G. Further, there can be only one such extension and this then coincides with φ^*.*

Let φ be a mapping of E into H and φ^* the mapping induced by φ on the set of all words in E. Suppose φ^* induces a mapping on G. Let

$$u(\underline{e}) = v(\underline{e})$$

be a relation in G. Suppose φ^* induces a mapping on G, we have

$$(u(\underline{e}))^{\varphi^*} = (v(\underline{e}))^{\varphi^*};$$

that is

$$u(\underline{e}^{\varphi}) = v(\underline{e}^{\varphi})$$

52 is a relation valid in H.

Conversely suppose every relation

$$u(\underline{e}) = v(\underline{e})$$

in G leads to a valid relation

$$u(\underline{e}^{\varphi}) = v(\underline{e}^{\varphi}) \text{ in } H.$$

Now if x is any element in G, say

$$x = u(\underline{e}).$$

Then

$$x^{\varphi^*} = (u(\underline{e}))^{\varphi^*} = u(\underline{e}^{\varphi}).$$

If also

$$x = v(\underline{e})$$

then

$$x^{\varphi^*} = (v(\underline{e}))^{\varphi^*} = v(\underline{e}^{\varphi})$$

But

$$u(\underline{e}) = v(\underline{e}) \quad (= x)$$

53 is a relation in G. Therefore

$$u(\underline{e}^{\varphi}) = v(\underline{e}^{\varphi})$$

is valid relation in H; that is φ^* induces a well-defined mapping on G. Hence by Theorem 20, we have

Theorem 21. *A mapping φ of of E into H can be extended to a homomorphism of $G = gp(E)$ into H if and only if every relation*

$$u(\underline{e}) = v(\underline{e}) \text{ in } G$$

leads to a relation

$$u(\underline{e}^{\varphi}) = v(\underline{e}^{\varphi}) \text{ in } H.$$

Since every relation can be derived from the defining relations, we have the following corollary.

Corollary ven Dyck (1882). *Let $G = gp(E)$ and $H = gp(F)$, and let φ be a mapping of E into F. Then φ can be extended to a homomorphism of G into K if and only if every defining relation of the form*

$$u(\underline{e}) = v(\underline{e})$$

turns into a valid relation

$$u(\underline{e}^{\varphi}) = v(\underline{e}^{\varphi})$$

between the elements of F upon applying.

Chapter 4

Free Groups

1

In this chapter we shall consider an important class of groups called "free groups". Let E be a set of generation of a group F. We call F a free groups if $F = gp(E; \varphi)$. In other words, a free groups is one which, in a particular set of generations, does not have any defining relations and hence it is without non-trivial relations. An infinite cyclic group is a free group with one generator. An immediate consequence of Von Dyck's theorem is: **54**

Theorem 1. *Every mapping of the generation set E of a free group $F = gp(E; \varphi)$ onto a group H can be extended to a homomorphism of F into H.*

2 Normal words

We now proceed to find what the elements of a free group look like. We make the following definition

Definition. (i) The empty word '1' is a normal word

(ii) the words $e_{i_1}^{m_1} e_{i_2}^{m_2} \cdots e_{i_\lambda}^{m_\lambda}$ is a normal word if

(a) $m_i = \pm 1$, $i = 1, \ldots, \lambda$

(b) $i_j = i_{j+1} \Rightarrow m_j = m_{j+1}$.

It is clear from this definition that a normal word is one which cannot
55 be "cancelled down" to a shorter word. The number of letters in a word w is the *length* if the word w and is denoted by $\lambda(w)$. We put $\lambda(1) = 0$.

The following theorem shows that any word can be cancelled down to a unique normal word.

Theorem 2. *Every word is trivially equal (i.e. equal by a trivial relation) to a normal word and this normal word is unique.*

Proof. We prove the first part of the theorem by induction on the length. Let $G = gp(E)$ be a group and let $w(e)$ be a word in E, with $\lambda(w) = n$. When $n = 0$, by definition w is the empty word and hence normal. Thus the theorem is true for $n = 0$. Assume that every word v, with $\lambda(v) < n$, is 'trivially equal' to a normal word. Let [1] $w = e_{i_1}^{m_1} e_{i_2}^{m_2} \cdots e_{i_n}^{m_n}$ and thus $\lambda(w) = n$. □

If w is normal, there is nothing to prove. If w is not normal, then there is a positive integer j such that $i_j = i_{j+1}, m_j = -m_{j+1}$. Put $u = e_{i_1}^{m_1} e_{i_2}^{m_2} \cdots\ e_{i_{j-1}}^{m_{j-1}}, u' = e_{i_{j+2}}^{m_{j+2}} \cdots e_{i_n}^{m_n}$. Then $w \equiv ue_{i_j}^{m_j} e_{i_{j-1}}^{m_{j+1}}, u'$. It is immediate that $w \equiv ue_{i_j}^{m_j} e_{i_{j-1}}^{m_{j+1}}, u' = uu' \equiv v$ is a trivial relation. But $\lambda(v) = n - 2$. Therefore induction hypothesis, there is a normal word w' such that $v = w'$ is a trivial relation. Since $w = v$ is also a trivial relation
56 it follows by transitivity that $w = s'$ is a trivial relation. This proves the first part of the theorem.

We say that word v is obtained from the word u by an *'elementary reduction'* if there is a 'letter' e in u such that $u \equiv u' e^m e^{-m} u''$ and

$$v \equiv u' u'', m = \pm 1.$$

To prove the uniqueness we required the following two lemmas.

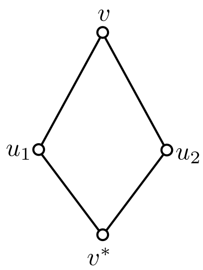
Lemma 1. *Two words v, v' are trivially equal (i.e. $v = v'$ is a trivial relation) if and only if there is a finite sequence of words $v = v_0$, $v_1, \ldots, v_n = v'$, such that for every $i(1 \leq i \leq n)$, either v_{i+1} is got from v_i by elementary reduction or v_i is got from v_{i+1} by elementary reduction.*

[1] We use $\equiv$ for equality of words, $=$ for equality of group elements

Lemma 2. *(The "Diamond Lemma"). If u_1 and u_2 are obtained from the same word v by elementary reduction, then either $u_1 \equiv u_2$, or each can be reduced by an elementary reduction to one and the same word v^*.*

Proof. Let

$$v = e_{i_1}^{m_1} e_{i_2}^{m_2} \cdots e_{i_n}^{m_n},$$
$$i_j = i_{j+1}, m_j = -m_{j+1},$$
$$i_k = i_{k+1}, m_k = -m_{k+1},$$



and u_1 obtained by omitting $e_{i_1}^{m_1} e_{i_{j+1}}^{m_{j+1}}$ from v, and u_2 by omitting $e_{i_k}^{m_k} e_{i_{k+1}}^{m_{k+1}}$, where we may without loss of generality suppose that $j \leq k$.

Then if $j = K$, then $u_1 \equiv u_2$ (trivially). □ 57

If $j = k - 1$, then $e_{i_j}^{m_j} e_{i_{k+1}}^{m_{k+1}} = e^m$, say, and

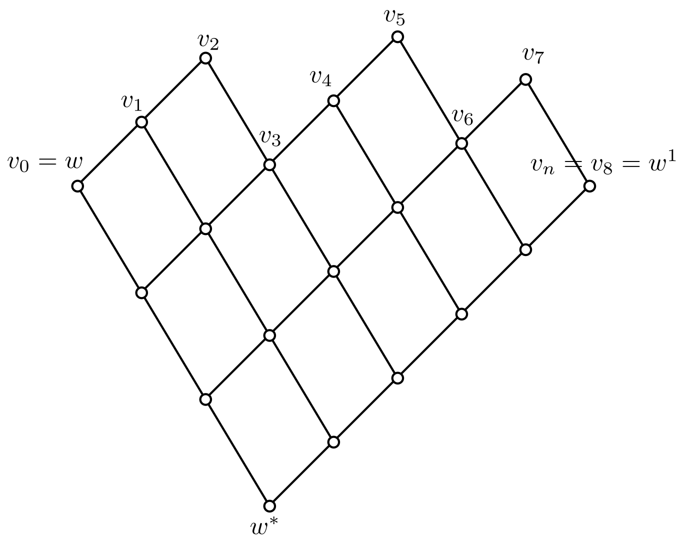
$$u_1 \equiv e_{i_1}^{m_1} \cdots e_{i_{j-1}}^{m_{j-1}} \; e^m \; e_{i_{k+2}}^{m_{k+2}} \cdots e_{i_n}^{m_n} \equiv u_2.$$

Finally, if $j < k - 1$, put

$$v^* = e_{i_1}^{m_1} \cdots e_{i_{j-1}}^{m_{j-1}} e_{i_{j+2}}^{m_{j+2}} \cdots e_{i_{k-1}}^{m_{k-1}} e_{i_{k+2}}^{m_{k+2}} \cdots e_{i_n}^{m_n}.$$

Then v^* is obtained from u_1 by the elementary reduction that deletes $e_{i_k}^{m_k} e_{i_{k+1}}^{m_{k+1}}$ and from u_2 by similarly deleting $e_{i_j}^{m_j} e_{i_{j+1}}^{m_{j+1}}$.

We now give an intuitive argument to show that if two normal words are trivially equal, then they are identical. Let w, w' be two words such that $w = w'$ is a trivial relation. By lemma 1, there exists words $w = v_0, v_1, \ldots, v_n = w'$ such that either v_{i+1} is obtained from v_i by elementary reduction or vice versa, for $i = 0, 1, \ldots, n$. In the following figure we write v_{i+1} above v_i and connect it to v_i if v_{i+1} is obtained from v_i by elementary reduction.



58 A glance at the above figure shows that by several applications of the diamond lemma, we descend down to a word w^*, which is trivially equal to w and w', or w and w' are identical. Now if w and w' are normal words which are trivially equal, then they have to be identical as further descent is not possible.

59 A formal proof of the above lemma can be found in M.H.A Newman (1942).

Corollary. *If $G = gp(E)$, then every element $g \in G$ has a representation $g = w(\underline{e})$ where w is normal.*

In particular in a free group, every element is representative by one and only one normal word. This follows from the fact that in a free group there are no non-trivial relations.

3

Let G be any group with $G = gp(E; R)$ and $F = gp(E^0, \varphi)$ a free group such that $|E^0| = |E|$. There is a mapping φ of E^0 onto E which is one-one. By Von Dyck's theorem φ can be extended to an epimorphism φ^* of F onto G.

Let $N = \{1\}^{\varphi*^{-1}}$ be the kernel of φ^*. Then $N\Delta F$. Let $f \in F$. Then $f = w(\underline{e}^0)$. Without loss of generality we can assume that w is a normal word. We have

$$f^{\varphi^*} = w(\underline{e}) = g \in G$$

where
$$e^0 = (e_1^0, \ldots, e_n^0)$$
$$e^0 = (e_1, \ldots, e_n) \text{ and } e_i = e_i^{\circ\varphi}.$$

Now $f \in N$ if and only if $g = 1$; i.e., $f \in N$ if only if $w(\underline{e}) = 1$ is a relation in G. Since any relation of G can be written in the form $w = 1$, it follows that N completely determines the relation in G. Hence N is called the *relation group* of G.

Further 60

$$g \cong F/N.$$

Thus we have the following theorem.

Theorem 3. *Every group is an epimorphic image of a free group and hence is isomorphic to a quotient group of a free group.*

If a set of defining relation R of G is given we can say something more about the structure of N. Let $R = \{f_i \equiv w_i(\underline{e}) = 1 \mid i \in I\}$ be a set of defining relations of G. Without loss of generality we can assume that all $w_i(\underline{e})$ are normal words. We claim that N is the normal closure in F of $\{f_i'\}_{i\in I}$, where $f_1' = w_i(\underline{e^0})$. That is to say N is the normal subgroup of F containing $\{f_1'\}_{i\in I}$. In other words, if $R' = \{f_1'\}_{i\in I}$, then

$$N = \bigcap_{R' \subseteq M\Delta F} M$$

Since $R' \subseteq N\Delta F$, we have $N' \subseteq N$, where N' denotes the normal closure of R'. Consider now the quotient F/N'. All the defining relations $w_i = 1, i \in I$ of G, are satisfied in F/N' as $R' \subseteq N'$. Hence any relation $w = 1$ satisfied in G is also satisfied in F/N'. Let $f \equiv w(e^0) \in N$. Then $w(e) = 1$ is a relation in G and therefore $w(e^0)N' = N'$. i.e., $w(e^0) \in N'$. Hence $N \subseteq N'$.

In virtue of the reversed inclusion which we already have, this proves that $N = N'$.

The following theorem gives a method of construction for N'. 61

Theorem 4. *Let G be any group, $S \subseteq G$. Then the normal closure T of S in G is the totality of all elements t of the form*

$$t = g_1^{-1} s_1^{m_1} g_1 g_1^{-1} s_2^{m_2} g_2 \cdots g_\lambda^{-1} s_\lambda^{m} g_\lambda,$$

where $m_i = \pm 1, \lambda$ arbitrary, g_i, s_i are arbitrary elements of G and S respectively.

Proof. Let T denote the totality of such elements. Trivially T is contained in the normal closure of S. To complete the proof of the theorem, we have only to show that $T \Delta G$. That T is closed under right division is easy to verify, so that $T \leq G$. If $g \in G$, then

$$\begin{aligned} g^{-1} t g &= g^{-1} g_1^{-1} s_1^{m_1} g_1 g_2^{-1} s_2^{m_2} g_2 \cdots g_\lambda^{-1} s_\lambda^{m} g_\lambda g \\ &= (g_1 g)^{-1} s_1^{m_1} (g_1 g)\,(g_1 g)\,(g_2 g)^{-1} s_2^{m_2} (g_2 g) \cdots (g_\lambda g)^{-1} s^{m} (g_\lambda g) \in T \end{aligned}$$

for arbitrary $t \in T$. Therefore $T \Delta G$. Hence the theorem. Determining to our N, we see that N consists of all elements of the form

$$t_1^{-1} w_{i_1}^{\pm 1} t_1 t_2^{-1} w_{i_2}^{\pm 1} t_2 \cdots t_\lambda^{-1} w_{i_\lambda}^{\pm 1}, \text{ where}$$

$t'_\lambda s$ are arbitrary and $w_{i_k} \in R'$. □

4 Dual property of free groups

Theorem 5. *If a group G is epimorphically mapped on a free group F, then G contains a free subgroup isomorphic to F, and in fact mapped*
62 *isomorphically onto F by the restriction to it of the epimorphism of G.*

Proof. Let φ be an epimorphism of G onto F. Let $F = gp(E, \varphi)$. Then $e^{\varphi^{-1}}$ is a non-empty for every $e \in E$. Choose an e_1 from $e^{\varphi^{-1}}$. Denote by E_1 the set of all such $e'_1 s$. Let $F_1 = gp(E_1)$. We claim that the restriction φ_1 of φ to F_1 ia an isomorphism of F_1 onto F. That the mapping φ_1 is an epimorphism is obvious, by our choice of $e'_1 s$. Now if $g \in F$, let $w(\underline{e})$ he a normal word representing g. Then $g^{\varphi_1} = (w(\underline{e}))^{\varphi_1} = (w(\underline{e}))^{\varphi} = (w(\underline{e}_1^{\varphi})) = w(\underline{e}) = 1$ if and only if w is the empty word, as F is a free group. Hence the kernel of φ_1 consists of the neutral elements alone and therefore φ_1 is an isomorphism. Since any group isomorphic to a free group is also free, our theorem follows. □

Theorem 6. *Free groups generated by sets of the same cardinality are isomorphic.*

Proof. Let E and E^0 be two sets such that $|E| = |E^0|$, $F = gp(E, \phi)$ and $F^0 = gp(E^0, \phi)$. Let ψ be a one-one mapping of E^0 onto E. Extend it to an epimorphism of F^0 onto F. We shall also denote this extended mapping by ψ. □

Now $(w(c^\circ))^\psi = w(e) = 1$ if and only if w is an empty word. This follows because we can without loss of generality take w to be a normal word. hence $w(e^0) = 1$. Therefore ψ is an isomorphism of F^0 onto F.

This shows that the structure of a free group depends only on the **63**
cardinality of its set of generators. We call $|E|$ the rank of the free group $gp(E, \phi)$. A free of rank zero is the trivial group $\{1\}$. Free groups of rank 1 are finite cyclic groups.

It is natural to ask if free groups of different ranks are in fact different. The following theorem answer this question.

Theorem 7. *Free groups of different ranks are not isomorphic.*

To prove this theorem we need the following lemma, the proof of which we shall give later.

Lemma. *To every cardinal number n there is group G_n that can be generated by a set of cardinal n elements, but by no set of strictly smaller cardinal.*

Proof of the theorem. Let

$$F_n = gp(E_n, \phi), |E_n| = n,$$
$$F_m = gp(E_m, \phi), |E_m| = m$$

where n and m may be infinite cardinals. Choose G_n of the above lemma. Then there is a epimorphism ψ of F_n onto G_n. Assume that there is an isomorphism φ of F_m onto F_n. Then $\varphi\psi$ is an epimorphism of F_m onto G_n. Therefore $E_m^{\varphi\psi}$ generates the group G_n. Hence we have $m = |E_m| \geq |E_m^{\varphi\psi}| \geq n$ using the isomorphism φ^{-1}, we similarly get $n \geq m$. Hence $m = n$. Differently put, F_m and F_n are not isomorphic if $m \neq n$. Hence the theorem.

Proof of the lemma. For every cardinal n, we shall construct a G_n with
64 the desired property. Let M be any set with $|M| = m$. Consider the set G of all finite subsets of M. We turn G into a group by defining the binary operation as the symmetric difference. That is to say, for every $S, T \in G$.

$$ST = (S - T) \bigcup (T - S)$$

We take the empty set ϕ as the unit element and each S as its own inverse. For we have

$$S\phi = \phi S = S \text{ and } SS = \phi, \text{ for every } S \in G.$$

The verification of the associativity of this multiplication is easy and therefore we omit it. Hence the multiplication defined in G, makes G a group. We claim that this group G is generated by the set of one-element subsets of M, $E = \left\{\{x\} \middle| x \in M\right\}$. For if $S = \left\{a_1, a_2, \ldots, a_k\right\}$, it is easily seen that $S = \{a_1\}\{a_2\} \cdots \{a_k\}$. Further for every S, $T \in G$, we have $ST = TS$. Therefore G is commutative. We shall show that no set of cardinal $< m$ generates G. Let E^0 be a set of generators of G with $E^0 = n$, say. Then every elements $x \in G$ can be written as

$$x = s_1^{m_1} S_2^{m_2} \cdots S_k^{m_k} \text{ with } m_i = \pm 1, S_i \in E^0, i = 1, \ldots, k.$$

But in G, we have $S = S^{-1}$, for every $S \in G$. Therefore every $x \in G$, can be written as

$$x = S_1 S_2 \cdots S_k \text{ with district generators } S_i \in E^0.$$

65 Further, since G is commutative it follows that every finite subset of E^0 determines only one element of G. Thus to every element $x \in G$, we can associated a finite subset of E^0. This shows that $|G| \leq$ cardinal of the set of all finite subsets of E^0. But we know that if X is any set and F the set of all finite subset of X. Then

$$|F| = 2^X \text{ if } |X| < \mathcal{N}_0$$

and

$$|F| = X \text{ if } |X| \geq \mathcal{N}_0$$

Thus if m is finite, we have, from the above inequality, that $2^m \leq 2^n$, and therefore $m \leq n$. If m is infinite and n is finite, we have $m \leq 2^n$, which is impossible. Hence if m is infinite, n must also be infinite, and again conclude that $m \leq n$. Hence the group G cannot be generated by a set of cardinals strictly smaller than m. This establishes the lemma.

Chapter 5

Identical Relations and Varieties of Groups

1

In the preceding chapter we have seen that an arbitrary mapping from a set generators of a free group into any other group can be extended to a homomorphism. In fact this property completely characterises the free groups. In order to generalise this notion of being "free", we introduce certain classes of groups called *varieties* of groups **66**

While proving that the free groups of different ranks are not isomorphic we have come across an example of a group G in which the equation $x^2 = 1$ holds for all x in G. Such equations are called *identical relations* or *laws*.

Definition. A law or identical relation is a relation of the form

$$u(\underline{\mathrm{X}}) = v(\underline{\mathrm{X}})$$

where u and v are words in $\underline{\mathrm{X}} = (X_1, \dots, X_n)$. We say that the law $u(\underline{\mathrm{X}}) = v(\underline{\mathrm{X}})$ holds in a group G if the equation $u(\mathrm{f}) = v(\mathrm{f})$ holds when we substitute arbitrary elements $g_1, \dots, g_n$ of G for the "variables" $X_1, \dots, X_n$. For instance if $u(\underline{\mathrm{X}}) = X_1 X_2$ and $v(\underline{\mathrm{X}}) = X_2 X_1$, then in an abelian group the law $u(\underline{\mathrm{X}}) = v(\underline{\mathrm{X}})$ holds.

The following fundamental relations can be easily verified

(1) If $u \equiv v$, then $u = v$ is a law.

(2) If $u = v$, is a law then so is $v = u$.

67 (3) If $u = v$ and $v = w$ are laws, then so is $u = w$.

(4) If $u = v$ is a law, then so is $u^{-1} = v^{-1}$.

(5) If $u = v$ and $u' = v'$ are laws, then $uu' = vv'$ is a law.

(6) $XX^{-1} = 1$ and $X^{-1}X = 1$ are laws.

(7) If $u(\underline{X}) \equiv u(X_1, \ldots, X_n) = v(X_1, \ldots, X_n) \equiv v(\underline{X})$ is a law and $Y_1(\underline{Z})$, $\ldots Y_n(\underline{Z})$ are words in variables $Z_1, \ldots, Z_p$ then $u(Y_1(\underline{Z}), \ldots, Y_n(\underline{Z}))$ $= v(Y_1(\underline{Z}), \ldots, Y_n(\underline{Z}))$ is a law.

The rule (7) is a called the *substitution rule*.

[If we assume $XX^{-1} = 1$ and (7) we can derive the law $X^{-1}X = 1$. For put $Y = X^{-1}$. Then $YY^{-1} = 1$ is a law. i.e. $X^{-1}(X^{-1})^{-1} = X^{-1}X = 1$ is a law.]

These rules can be used can be used to derive from given laws that are valid in a group further laws that “follow” from the given laws.

Example. If $X^2 = 1$ is a law in a group, then so is

$$XY = YX$$

Proof. The law $XY = YX$ is equivalent to $X^{-1}Y^{-1}XY = 1$. Now

$$\begin{aligned} X^{-1}Y^{-1}XY &= X^{-1}Y^{-1}XX^{-1}Y^{-1}XX^{-1}X^{-1}XYXY \\ &= (X^{-1}Y^{-1}X)^2(X^{-1})^2(XY)^2 \end{aligned}$$

Applying (5) and (7) we have $X^{-1}Y^{-1}XY = 1$, i.e. $XY = YX$ is a law. □

It is easily seen (as for relations) that every law $u(\underline{X}) = v(\underline{X})$ is equivalent to a law $w(\underline{X}) = 1$; and it is often convenient to write all laws in this from.

2 Varieties

Throughout this chapter we shall assume that the set of variables $\left\{X_1, X_2, \ldots\right\}$ is countable. This is just for convenience and not a real restriction.

Let L be a set of laws invariables $\left\{X_1, X_2, \ldots\right\}$. The class of all groups satisfying the laws of L is called *variety*. We call this the variety *defined* by L and denote it by $V_{=L}$ as it clearly depends on L. For example if L consists of the single law $X_1^{-1}X_2^{-1}X_1X_2 = 1$, then $V_{=L}$ is the class of all abelian groups.

A variety may be defined by different sets of laws. For instance if $L = \left\{X_1^2 = 1\right\}, L' = \left\{X_1^2 = 1, X_1^{-1}X_2^{-1}X_1X_2 = 1\right\}$, then $V_{=L} = V_{=L'}$.

It is easily seen that if $L \subseteq L'$, then $V_{=L'} \subseteq V_{=L}$. We say that a variety $\underset{=}{V}$ is *finitely based* if there exists a finite set of laws defining $\underset{=}{V}$.

In this context there are still some undecided questions.

Problem. Are all varieties of groups finitely based?

Let $\underset{=}{C}$ be a class of groups, and consider the “least variety” to which all groups of $\underset{=}{C}$ belong: this is the variety defined by all those laws that are (simultaneously) valid in all groups in $\underset{=}{C}$. We can take, as the simplest case $\underset{=}{C}$ to consist of just a single group G.

Problem. If $\underset{=}{V}$ is the least variety to which the finite group G belongs, is $\underset{=}{V}$ necessarily finitely based?

Even this problem is not solved in general; only if G is further as- **68**
sumed to be nilpotent is the answer known to be positive [R.C. Lyndon 1952]; of. also *p*.163.

Let $V_{=L}$ be a variety, without loss of generality we can assume that all laws in L are of the form $w = 1$, where w is a normal word in the variables $X_1, X_2, \ldots$. Let E be any set with $|E| = n$. Let R be the set of all relations of the form $w(e_1, \ldots, e_m) = 1$ with e_i arbitrary elements of E and $w(X_1, \ldots, X_m) = 1$ a law in L and $m \le n$. Consider the group $F_L = gp(E; R)$. Now, if G is a group in the variety $V_{=L}$, then any mapping φ

of E into G is extendable to a homomorphism φ^* of F_L into G. For if $w(e_1,\dots,e_n) = 1$ is a relation in R, then $w(X_1,\dots,X_n) = 1$ is a law in L; and therefore, since $G \in V_{=L}, w(e_1^{\varphi},\dots,e_n^{\varphi}) = 1$ is a relation in G. Thus the set R of defining relations in F_L go over to relations in G upon applying φ

Therefore, by von Dyck's theorem the mapping φ is extendable to a homomorphism φ^* of F_L into G. Thus in a way, this is a generalisation of free groups, We call F_L a *free group of* $V_{=L}$ (reduced free or relatively free) of rank n. It is easy to see that F_L itself is a member of $V_{=L}$ and it depends upon n. In particular if L is the empty set we get the free group in the ordinary sense (in this context called *absolutely free groups)*.

3 Burnside conjectures

69 Let L be the set consisting of the single law $X^n = 1$. We denote the corresponding $V_{=L}$ by $B_{=n}$. Group of $B_{=n}$ are called groups of *exponent* n. We call B_n the *Burnside variety* after W. Burnside (1852-1927). There is a problem connected with this known as the Burnside conjectures (Burnside *W.*1902). We first state the original conjecture, now known as the Full Burnside Conjecture; and afterwards a weaker form, the so-called Restricted Burnside Conjecture. *Full Burnside Conjecture*. Every finitely generated group in $B_{=n}$, that is of finite exponent n, is finite. Let $B_{d,n}$. denote a d generator free group of $B_{=n}$. The Full Burnside Conjecture is equivalent to saying that $|B_{d,n}| < \mathscr{N}_\circ$, for every positive integer d for every group with d generators and exponent n is an epimorphic image of $B_{d,n}$.

The following problem is weaker than the above conjecture.

Restricted Burnside Conjecture.

There is a bound $\beta(d,n)$ such that every finite d generator group of exponent n has order $\leq \beta(d,n)$. This conjecture is an easy consequence of the full Burnside conjecture. For if the full conjecture is true, then $B_{d,n}$ is finite and we can take $\beta(d,n) = |B_{d,n}|$. The present state of knowledge of the Burnside conjecture is for from complete. The following are the results so far obtained in this direction. In the following d denotes the number of generators, n the exponent. We abbreviate the Restricted Burnside

Conjecture and the full Burnside conjecture RBC and FBC respectively. 70

d	n	RBC	FBC	REMARKS
all	2		true	Trivial. In fact $\|B_{d,2}\| = 2^d$.
all	3		true	Burnside (1902). The order of $B_{d,3}$ was given by Levi and van der Waerden (1933). $\|B_{d,3}\| = 3^{\binom{d}{1}+\binom{d}{2}+\binom{d}{3}}$.
all	4		true	Sanov(1940). The order of $B_{d,4}$ is not known.
2	5	true	unsolved	Kostrikin (1955).
all	5	true	unsolved	G.Higman (1956).
all	6	true		P. Hall and G. Higman (1956).
all	6		true	M. Hall, Jr. (1959).
all	12	true	unsolved	P. Hall and G. Higman (1956).
all	all prime	p true	-	Kostrikin(1959).
all	pq (p, q different primes)	true	unsolved	follows form a combination of Kostrikind (1959), Hall and Higman(1956)
all	4p (p, a prime)	true	unsolved	
2	≥	72	not true	Novikov(1959).

4 A consequences of the result of Novikov (1959) and Kostrikin (1959)

Using the result of Novikov and Kostrikin, we shall derive an interesting 71
consequence. As the Burnside conjecture is not true for $d = 2, n \geq 73$, it follows that $B_{2,73}$, the 2 generator free group of $B_{=73}$, is infinite. But 73 is a prime, and therefore by Kostrikin's result, there exists a maximal finite 2 generator group of exponent 73. Let us denote this

group by $B^*_{2,73}$. We know that $B^*_{2,73}$ is an epimorphic image of $B_{2,73}$ and therefore is isomorphic to a quotient group of $B_{2,73}$. Thus $B^*_{2,73} \cong B_{2,73}/N, N\Delta B_{2,73}$. Therefore N is an infinite normal subgroup of finite index in $B_{2,73}$. We now state the following theorem without proof.

Theorem (0, Schreier (1972); see Kurosh (1956) pp.36-37). *A subgroup of finite index of a finitely generated group is finitely generated.*

By this theorem N is finitely generated. Now, it is known that a finitely generated group contains a maximal normal subgroup. (B.H. Neumann 1937[b]). Let M be a maximal normal subgroup in N. Then it is easily seen that N/M is simple; that is to say, N/M does not contain any proper non-trivial normal subgroup. We assert that the group N/M is infinite. To prove this we quote another theorem with out proof.

Theorem (R. Baer 1953**).** *If a finitely generated group contains a proper subgroup of finite index it also contains a characteristic (for definition see section 6 of this chapter) proper subgroup of finite index.*

72 If N/M is finite, by the above theorem, there exists a characteristic proper subgroup K of finite index in N. It follows that K is a normal subgroup of $B_{2,73}$ and is of finite index in $B_{2,73}$. Therefore $B_{2,73/K}$ is a finite group of exponent 73, whose order exceeds that of $B^*_{2,73}$. This is impossible. Therefore N/M is infinite. Thus we arrive at in infinite group N/M which is simple, finitely generated and of exponent 73.

5

We return to the considerations of section 2. Let $V_{=L}$ be a variety determined by a set of laws L. Without loss of generality we can assume that every law of L is of the form $w(X_1, \dots, X_n) = 1$ where $w(X_1, \dots, X_n)$ is a normal word in the variables $X_1, X_2, \dots$. We denote by F_n the free group generated by the variables $X_1, X_2, \dots, X_n$ and by F the free group generated by all the variables $X_1, X_2, \dots$. That is to say,

$$F_n = gp\left(\left\{X_1, \dots, X_n\right\}, \phi\right), \; F_\omega = gp\left(\left\{X_1, X_2, \dots\right\}, \phi\right)$$

By F we shall mean either F_n or F_ω. With every $V_{=L}$ we associate a subgroup W of F in the following way. Define

$$\left\{ W = w(X_1, \ldots, X_m) \middle| \begin{matrix} w(X_1, \ldots, X_m) = 1 \\ w(X_1, \ldots, X_m) \in^F \end{matrix} \text{ valid in all group } of \ \stackrel{V}{=} L \right\}$$

That W is a group is easy to verify.

Now let F_L be a free group of $V_{=L}$ with E as the set of generators and of the same rank as F. Consider some one-one mapping φ of X onto E, where X denotes the set of generators of F. We can extend φ to an epimorphism φ^* of F onto F_L. The kernel of φ^*, by the definition of F_L, is precisely the group W we have defined above. Therefore W is a normal subgroup of F and F_L is isomorphic to F/W. The substitution rule which we have for laws in a group gives some more information about W. If $w(x_1, X_2, \ldots, X_m) \in W$, and $Y_1(\underline{X}), \ldots, Y_m(\underline{X}) \in F$, then also $w(Y_1(\underline{X}), \ldots, Y_m(\underline{X})) \in W$. **73**

We make the following definition.

Definition. Let E be any set, $S \subseteq E$ and η a mapping of $E \to E$. We say that the subset S admits the mapping η if $S^\eta \subseteq S$.

Theorem 1. *The subgroup $W \leq F$ admits all endomorphisms of F.*

Proof. Let η be any endomorphism of F and $X_i^\eta = Y_i(\underline{X})$. If $w(X_1, \ldots, X_m)$ is in W, then

$$\begin{aligned} \Big(w(X_1, X_2, \ldots, X_m)\Big)^\eta &= w(X_1^\eta, \ldots, X_m^\eta) \\ &= w(Y_1(X), \ldots, Y_m(X)) \in W. \end{aligned}$$

Therefore $W^\eta \subseteq W$. This proved the theorem. □

Let G be any group. For every $t \in G$, we define the mapping φ_t of G onto itself such that

$$x^{\varphi_t} = t^{-1}xt \text{ for all } x \in G.$$

now $(xy)^{\varphi_t} = t^{-1}xyt = (t^{-1}xt)(t^{-1}yt) = (x)^{\varphi_t}y^{\varphi_t}$ for all x and y in G. **74**

Therefore φ_t is an endomorphism of G. But

$$x^{\varphi_t\varphi_{t-1}} = (t^{-1}xt)^{\varphi_t} = t(t^{-1}xt)t^{-1} = x = x^{\varphi_t{}^{-1}\varphi_t}.$$

Thus $\varphi_t\varphi_{t^{-1}} = \ell = \varphi_{t^{-1}}\varphi_t$; in other every φ_t has a two sided inverse. Thus φ_t is an automorphism of G. We call φ_t an *inner automorphism* of G. An automorphism which is not an inner automorphism is called an *outer automorphism*.

Let us denote by A_I the set of all inner automorphisms of G. It is easy to see that A_I is a group. There is a natural mapping φ of G onto A_I defined by $s^\varphi = \varphi_s$ for all s in G. This mapping φ is easily seen to be an epimorphism. Then kernel Z of φ consists precisely of those elements of G which commute with every element of G. [For proofs see Kurosh (1955), Ch. 4, §12]. We call Z the center of G. By the definition of inner automorphisms it follows that $N\Delta G$ if and only if N admits all inner automorphisms of G.

A subgroup $H \leq G$ is *characteristic* in G if it admits all automorphisms of G. Similarly a subgroup $H \leq G$ is *fully invariant* in G if it admits all endomorphisms of G. By the definition of full invariance it follows that the subgroup W in Theorem 1 is fully invariant in F. Every fully invariant subgroup of G is trivially characteristic in G and every characteristic subgroup of G is normal in G. We remark that the centre
75 z of a group G is a characteristic subgroup. For if $a \in Z$, then $ax = xa$ for every x in G. Therefore

$$a^\top x^\top = (ax)^\top = (xn)^\top = x^\top a^\top$$

for every automorphism $\top$ of G. Now since $x^\top$ runs through all the elements of G it follows that $a^\top$ is in Z and therefore Z is a characteristic subgroup of G. In general the centre of a group is not a fully invariant subgroup. [See Kurosh (1955), ch. 4 15].

One can easily verify that the intersection of an arbitrary family of characteristic (fully invariant) subgroups of a group is a characteristic (fully invariant) subgroup. Thus we can talk of characteristic (fully invariant subgroup generated by a set of elements and also of the lattice of characteristic (fully invariant) subgroups of a group.

In general a characteristic subgroup is not a fully invariant subgroup. [See Neumann and Neumann (1951)]. The following is an unsolved problem in this direction.
Unsolved problem. Is there a characteristic subgroup of a free group F of infinite rank which is NOT fully invariant in F?

Theorem 2. *The relation "characteristic" and "fully invariant" are transitive; that is to say, if $K \leq H \leq G$ with K characteristic (fully invariant) in H and H characteristic (fully invariant) in G then K is characteristic (fully invariant) in G.*

Proof. Let α be an automorphism of G; α' the restriction of α to H. **76**
Then, because H is characteristic in $G, H^{\alpha} \leq H$. Applying the automorphism α^{-1} to H, we have $H^{\alpha-1} \leq H$. Therefore $H = (H^{\alpha-1})^{\alpha} \leq H^{\alpha}$. Hence we have $H^{\alpha} = H$. i.e. $H^{\alpha'} = H$. Therefore α' is an automorphism of H. Now since K is characteristic in H, we have $K^{\alpha} = K^{\alpha'} \leq K$. hence K is characteristic in G. □

The proof in the case of full invariance is similar and actually even easier and we omit it.

The transitivity is not true for the relation "normal". In other words if $K \Delta H \Delta g$, in general it is not true that $K \Delta G$. For example take for G the symmetric group S_4 of permutations on four letters or the alternating group A_4. Let

$$H = V_4 = \Big\{1, (12)(34), (13)(24), (14)(23)\Big\} \quad \text{and}$$
$$K = \Big\{1, (12)(34)\Big\}.$$

We know that $H \Delta G$, and $K \Delta H$. Now $(123) \in A_4$. $(123)^{-1} = (132)$ and $(123)^{-1} K (123) = \Big\{1, (14)(23)\Big\} \neq K$. Therefore K is not normal in G.

We say that $H \leq G$ is *accessible* (or *subnormal*) in G (notation $H \Delta\Delta G$) if there exists subgroups $H_0 = H, H_1, \ldots, H_n = G$, such that $H_0 \Delta H_1 \Delta H_2 \cdots \Delta H_n$.

The accessible subgroups of finite group were introduced by H. Wielandt (1939) and further studied by H. Wielandt and recently by **77**

B. Huppert. It is easy to verify that the intersection of two and hence the intersection of a finite number of accessible subgroups is an accessible subgroup. The intersection of an infinite number of accessible subgroups need not be an accessible subgroup.

If a group G has a composition series [Kurosh (1955), $CH.5, \S 16$] then the join of any two accessible groups is again an accessible group (Wielandt (1939)). The following is an unsolved problem.

Unsolved problem. Is the join of two accessible subgroup of an infinite group (without composition series) accessible?

7 Verbal Subgroups

Let L be any set of words [1] in the variables $X_1, X_2, \ldots$ and G a group. Consider the set,

$$S = \left\{ w(g_1, \ldots, g_n) \middle| w(x_1, \ldots, x_n) \in L, g_i \in G i = 1, 2, \ldots n \right\}$$

This is not in general a subgroup of G. We call $H = gp(S) \leq G$, the word *subgroup* or a *verbal subgroup* defined by L.

Theorem 3. *Every verbal subgroup H of a group G is fully invariant.*

Proof. Let η be an endomorphism of G and the verbal subgroup H be defined by L. It is enough to prove that $S^\eta \subseteq S$, for every endomorphism η of G, where S is the set of generators of H as defined above. Now if $w(g_1, \ldots, g_n) \in S, w(X_1, \ldots, X_n) \in L_\eta$, then $\left\{ w(g_1, \ldots, g_n) \right\}^\eta =$
78 $w(g_1^\eta, \ldots, g_n^\eta) \in S$. Therefore $S^\eta \subseteq S$; this is true of every endomorphism of G. Hence H is fully invariant in G. The converse of this theorem is not true in general; but happens to be in the case of free group. □

Theorem 4. *Every fully invariant subgroup of a free group is verbal.*

[1]This is a slight change of notation - earlier L stood for a set of laws = 1, now only for the set of their left-hand sides.

Proof. Let W Be a fully invariant subgroup of a free group F. Let L be the set of all normal words that occur in W. If $Y_1(\underline{X}), \ldots, Y_n(\underline{X}) \in F$, where $\underline{X} = (X_1, \ldots, X_n)$ and $X_i \in X$, and where X denotes the set of variables as well as the set of generators of F, then the mapping defined by

$$X_i^\eta = Y_i(\underline{X}),\ i = 1, \ldots, n,$$

can be extended to an endomorphism of F which also we denote by η. Now if $w(X_1, \ldots, X_n) \in L$, then $w(X_1, \ldots, X_n)^\eta = w(Y_1(\underline{X}), \ldots, Y_n(\underline{X})) \in W$ as W is fully invariant in F. Therefore

$$S = \left\{ w(Y_1(Y_1(\underline{X}), \ldots, Y_n(\underline{X})) \,\middle|\, w(X_1, \ldots, X_n) \in L, Y_i(\underline{X}) \in F, i = 1, 2, \ldots n \right\}$$

is contained in W. But clearly also $W \subseteq S$. Thus $S = W$, and also $gp(S) = W$. Hence the theorem. ◻

It follows that the intersection of any arbitrary family of verbal subgroup of a free group is a verbal subgroup. In general in an arbitrary group this is not true [B.M. Neumann (1937^a)]. It is easy to verify that the join of two verbal subgroups of a group is a verbal subgroup.

8

We shall now give an important example of a verbal subgroup. Let G be any group. Let L consist of the single word $X_1^{-1}X_2^{-1}X_1X_2 = [X_1, X_2]$. The verbal subgroup G' of G defined by L is called the *commutator subgroup* or *derived subgroup* of G. **79**

Evidently the commutator subgroup of an abelian group is the trivial group. For any group it is easily seen that the quotient group G/G' is abelian [Kurosh (1955)].

Theorem 5. *Let W be a verbal subgroup, defined by a set L of words, of the free group F. Then the quotient group F/W is the free group of* *the variety $V_{=L}$ defined by the laws $w(\underline{X}) = 1$, for all $w(\underline{X}) \in L$ and it has the same rank as F.*

Proof. Now F_L, the corresponding free group of the variety $V_{=L}$, is isomorphic to F/W^*, where W^* consists of all $w(X_1, \ldots, X_n)$ such that $w(X_1, \ldots, X_n) = 1$ is a law in all the groups of V_L. We also know that W^* is fully invariant in F. If $w(X_1, \ldots, X_n)$ is in L, then $w(Y_1(\underline{X}), \ldots, Y_n(\underline{X}))$ $\in W^*$ for arbitrary $Y_i(\underline{X}) \in F$. Therefore $W \leq W^*$. Now $F/W \in V_{=L}$. Therefore, if $w(X_1, \ldots, X_n) \in W^*$ then the law $w(X_1, \ldots, X_n) = 1$ holds in F/W. In other words $w(X_1, \ldots, X_n) \in W$. Therefore $W^* \leq W$; we get $W = W^*$. Hence the theorem. □

Theorem 6. *Every verbal subgroup W of a free group F is the fully invariant closure of the set L (i.e. the fully invariant subgroup generated by L) of words consisting of either one or no word of the from X_1^k and*
80 *apart from that "commutator words" i.e. words contained in the derived group F'.*

Proof. We have already remarked that the quotient group F/F' is abelian. Therefore every $w \in W$ can be written as $w = X_1^{k_n} \cdot X_n^{k_n} w'$ with $w' \in F'$. Let η be the endomorphism of F defined by $X_1^{\eta} = X_1, X_i^{\eta} = 1$ for $i \neq 1$. Since W is fully invariant in F it follows that $w^{\eta} = X_1^{k_1} w'^{\eta} = X_1^{k_1}$. Similarly η_i defined by $X_i^{\eta_i} = X_1$ and $X_j^{\eta_i} = 1$ for $j \neq i$, generates an endomorphism of F and therefore $w^{\eta_i} = X_1^{k_i} w'^{\eta_i} = X_1^{k_i}$, since $w'^{\eta_i} = 1$. Let $gp(X_1^k) = gp(X_1) \cap W$. Then k/k_i for $i = 1, 2, \ldots n$. If Π_i is the endomorphism defined by $X_1^{\Pi_i} = X_i, X_j^{\Pi_i} = 1$ for $i \neq j$, then $(X^k)^{\Pi_i} = X_i^k \varphi W$. Let L be the set consisting of X_1^k and all the $w's$ that occur when each $w \in W$ is written as $w = X_1^{k_1} \cdots X_n^{k_n} w'$. It is easily seen that any invariant subgroup of F that contains L also contains W. But W itself is fully invariant in F. Hence W is the fully invariant closure of L. When $k = 0$, L is a subset of W'. □

Corollary B.M. Neumann, 1937[1]**.** *If $k \neq 1$, then the reduced free groups of the variety are non-isomorphic for different ranks. [If $k = 1$, the free groups of the variety are all the trivial groups.]*

Chapter 6

Group-theoretical Constructions

1 The Cartesian product and the direct product of a family of groups

Let $\{G_i\}_{i \in I}$ be a family of group indexed by a non-empty set I. Let T 81
denote the set of all functions on I with values in G_i. Consider the set P defined by

$$P = \left\{ f \in T \,\middle|\, f(i) \in G_i \text{ for all } i \in I \right\}.$$

We turn P into a group by introducing the following multiplication: If $f, g \in P$. Then

$$fg = h, \text{ where } h(i) = f(i)g(i), \text{ for all } i \in I.$$

It is easy to see that $h \in P$. We take the function $e \in P$, defined by

$$e(i) = 1_i \text{ for every } i \in I$$

(where 1_i is the unit element of G_i) as the unit element. For,

$$ef = fe = f, \text{ for all } f \in P.$$

For every $f \in P$, we take the function f^{-1} defined by

$$f^{-1}(i) = (f(i))^{-1}, \text{ for every } i \in I,$$

as the inverse of f. It is easy to verify that $f^{-1} \in P$ and $ff^{-1} = f^{-1}f =$
82 e, for every $f \in P$. We have only to verify the associative law. Let $f, g, h \in P$. We have

$$\begin{aligned}((fg)h)(i) &= (fg)(i)h(i) = (f(i)g(i))h(i) = f(i)(g(i)h(i)) \\ &= f(i)(gh)(i) = (f(gh))i,\end{aligned}$$

for every $i \in I$. Therefore for all $f, g, h, \in P$,

$$(fg)h = f(gh).$$

This proves that P is a group. We call P the *Cartesian product* (unrestricted, full, or strong direct product) of $\left\{G_i\right\}_{i\in I}$.

Consider now the set P^* defined by

$$P^* = \left\{f \,\middle|\, f \in P \text{ and } \left|\left\{i \,\middle|\, f(i) \neq 1_i\right\}\right| < \chi_0\right\}.$$

That is to say, P^* consists precisely of all $f \in P$ with $f(i) = 1_i$ except for a finite number of indices i. It is easy to see that P^* is a subgroup of P. The subgroup P^* is known as the *direct product* (restricted or weak direct product) of $\left\{G_i\right\}_{i\in I}$. If $|I| < \chi_0$, then $P = P^*$; that is to say, the concepts of the Cartesian product and the direct product coincide when the index set is finite. The two products we have just defined are important, and they occur frequently in the group theory.

Hereafter, we shall denote all the unit elements that occur by 1; unless is a possibility of confusion.

Consider now, for every $i \in I$, the set

$$H_i = \left\{f \,\middle|\, f \in P \text{ and } f(j) = 1 \text{ for all } j \neq i\right\}.$$

83 We claim that $H_i \Delta P$ and that $H_i \cong G_i$. Let $f, g \in H_i$. Then $f(j) =$

$1, g(j) = 1$, for $j \neq i$. Therefore, $f^{-1}g(j) = f^{-1}(j)g(j) = (f(j))^{-1}g(j) = 1^{-1}1 = 1$, for all $j \neq i$. Hence $f^{-1}g \in H_i$, and therefore $H_i \leq P$. In fact $H_i \leq P^* \leq P$. Now, let $f \in P, h \in H_i$. Then

$$(f^{-1}hf)(j) = (f(j))^{-1}h(j)f(j) = (f(j))^{-1}1f(j) = 1, \text{ for } j \neq i.$$

Therefore $H_i \Delta P$. Consider now the mapping $\prod_i$ of P onto G_i defined by

$$f^{\prod_i} = f(i), \text{ for every } f \in P.$$

We have, for arbitrary $f, g \in P$,

$$(fg)^{\prod i} = (fg)(i) = f(i) = f(i)g(i) = f^{\prod_i}g^{\prod_i}.$$

Therefore $\prod_i$ is a homomorphism and in fact, clearly, an epimorphism. We call $\prod_i$ the projection of P onto G_i. Let us now restrict $\prod_i$ to the subgroup H_i. We shall denote this restricted mapping also by $\prod_i$. We claim that $\prod_i$ is an isomorphism of H_i onto G_i. To check that this mapping is 'onto', we have only to observe that for every $a \in G_i$, the function $h_a \in H_i$ defined by

$$h_a(j) = 1 \text{ for } j \neq i, \text{ and } h_a(i) = a$$

is mapped on a by $\prod_i$. Obviously, the kernel of $\prod_i$ in H_i is trivial, and therefore **84**

$$H_i \cong G_i, \text{ for all } i \in I.$$

Thus we have in P isomorphic copies of the groups G_i. The group P is something called the *internal Cartesian product* of $\{H_i\}_{i \in I}$, and the *external Cartesian product* of $\{G_i\}_{i \in I}$.

It is easy to see that for $i \neq j$, every element of H_i commutes with every element of H_j.

We have already seen that $H_i \Delta P^*$, for all $i \in I$. We assert now that P^* is the subgroup generated by $\{H_i\}_{i \in I}$ in P. Trivially

$$gp(\{H_i\}_{i \in I}) \leq P^*.$$

Let now $f^* \in P^*$ with $f^*(i_j) = a_j \neq 1, j = 1, \ldots, n$ and $f^*(i) = 1$ for $i \neq i_1, \ldots, i_n$. Define $h_{i_j} \in H_{i_j}.j = 1, \ldots, n$ as follows:

$$h_{i_j}(i_j) = a_j, h_{i_j}(i) = 1 \text{ for } i \neq i_j.$$

Then

$$f^* = h_{i_1} h_{i_2} \cdots h_{i_n} \in gp(\{H_i\}_{i \in I}).$$

Therefore, $P^* = gp(\{H_i\}_{i \in I})$.

The following, theorem and the example we give show that certain properties of the G_i are retained in the direct product, but not in the Cartesian product.

85 We call a group *periodic* if all of its elements are of finite order.

Theorem 1. *The direct product of periodic groups is periodic.*

Proof. Let $f \in P^*$. Let

$$\left\{ i \middle| i \in I, f(i) \neq 1 \right\} = \left\{ i_1, \ldots, i_n \right\}.$$

If m is the least common multiple of the orders of $f(i_1), \ldots, f(i_n)$, then $f^m = 1$. This proves the theorem. □

In general this is not true for Cartesian products P. For example, let $G_i = gp(a_i : a_i^{i+1} = 1), i = 1, 2, 3, \ldots$; that is to say, G_i is a cyclic of order $i + 1$, generated by a_i. Consider $f_0 \in P$ defined by

$$f_o(i) = a_i, i = 1, 2, 3, \ldots$$

For any positive integer m, we have

$$f_0^m(m) = a_m^m \neq 1,$$

therefore f_o is of infinite order.

Let $\{G_i\}_{i \in I}$ be a countable family of countable groups. Then $P^* = gp(\{H_i\}_{i \in I})$ is countably generated, since each H_i, being isomorphic to G_i, is countable. On the other hand, the Cartesian product of a countably infinite family of non-trivial countable groups has the cardinal of the continuum. For it is easily seen that

$$2^{\mathcal{N}_o} \leq |P| \leq \mathcal{N}_o^{\mathcal{N}_o} = 2^{\mathcal{N}_o}.$$

86 We have already remarked that the Cartesian product and the direct product of a family of groups are equal if the index set I is finite. (The

converse is also true if there are no trivial groups in the family.) If $I = \{1, 2, \ldots, n\}$, we denote this product by

$$P = P^* = G_1 \times G_2 \times \cdots \times G_n$$

(Note that the same notation is used for the set product of the G_i; but there is little danger of confusion.)

The following theorems are easy to prove. We shall state them here without proof.

Theorem 2. *If $\{G_i\}_{i\in I}$ and $\{G'_i\}_{i\in I}$ are two families of groups indexed by the same set I, and*

$$G_i \cong G'_i \text{ for every } i \in I,$$

then $P \cong P'$ and $P^* \cong P'^*$ where P, P' denote the Cartesian products of $\{G_i\}_{i\in I}$ and $\{G'_i\}_{i\in I}$ respectively, and P^*, P'^* the corresponding direct products.

Theorem 3. *If $\{I_j\}_{j\in J}$ is a partition of the index set I, and P_j, P^*_j are the Cartesian product and direct product of the family $\{G_i\}_{i\in I_j}$, then the Cartesian product (direct product) of $\{P_j\}_{j\in J}(\{P^*_j\}_{j\in J})$ is isomorphic to the Cartesian product (direct product of $\{G_i\}_{i\in I}$.*

In particular, if $I = \{1, 2, 3\}$, we have

$$G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3.$$

If the G_i are all isomorphic to a group G, then we call P the *Carte-* **87**
sian power of G, and P^* the *direct power* of G. By Theorem 2, we may replace all the G_i by G. Then P will be the set of all functions on I with values in G. We denote this set by G^I. If $f, g \in G^I$, then $fg(i) = f(i)g(i)$. The unit element is the function $e \in G^I$ such that $e(i) = 1$ for all $i \in I$. The inverse of $f \in G^I$ is the function f^{-1} such that $f^{-1}(i) = (f(i))^{-1}$ for all $i \in I$.

When I is a finite set, say $I = 1, 2, \ldots, n$, we write G^n for G^I.

The Cartesian or direct power of a group G does not depend on the index set I, but only on the cardinal of I (See Kuroshm 1955, §17).

2 The splitting extension

In this section we shall give a group-theoretical construction which is more general then the direct product. This construction will be later used in proving certain embedding theorems.

Let G be any group, and $A \Delta G$, with $G/A \cong B$. We call G an *extension* of A by B. We now pose the following question. Given two groups A and B, does there exist an extension of A by B? We assert that the direct product of A and B is one such extension. For, let $G = A \times B$ be the direct product of A and B. According to our definition of the direct product an element of G is a function f on the set $\{1, 2\}$ with values in
88 $A \cup B$, such that $f(1) \in A$, and $f(2) \in B$. We shall denote this function by the pair $(f(1), f(2))$; in other words $(a, b) \in A \times B$ is the function on $\{1, 2\}$ such that $f(1) = a$, $f(2) = b$. Further, if $(a, b), (a', b') \in A \times B$, then

$$(a, b)(a', b') = (aa', bb');$$

the unit element of $A \times B$ is $(1, 1)$ and (a^{-1}, b^{-1}) is the inverse of (a, b) in our new notation. We have seen in the last section that the projection $\prod_2$ of G onto B is an epimorphism with the set $\left\{(a, 1) \middle| a \in A\right\}$ as the kernel. Clearly, the kernel is isomorphic to A in a natural way. If we identify this set with A, we have

$$G/A \cong B.$$

Thus G is an extension of A by B. But in general this is not the only extension of A by B.

We shall now give another method of constructing an extension of A by B. Let α be a homomorphism of B into the group of automorphisms of A; this is to say $\alpha(b)$ for any $b \in B$ is an automorphism of A, and further $\alpha(bb') = \alpha(b)\alpha(b')$ for all $b, b' \in B$: this is the homomorphism property of α. We take the product *set*

$$G = B \times A = \left\{(b, a) \middle| b \in B, a \in A\right\},$$

and make it a group by introducing the following multiplication:

$$(b, a)(b', a') = (bb', a^{\alpha(b')}a'), \text{ for } b, b' \in B, \text{ and } a, a' \in A.$$

We take (1, 1) as the unit elements of G. (The unit elements of both 89
A and P are denoted by 1.) For

$$(1,1)(b,a) = (1b, 1^{\alpha(b)}a) = (b,a)$$

as $\alpha(b)$, being an automorphism of A, must map 1 on 1; and

$$(b,a)(1,1) = (b1, a^{\alpha(1)}1) = (b,a),$$

since α is a homomorphism and thus $\alpha(1)$ must be the unit be the unit element of the group of automorphisms of A, that is the identity automorphism. The inverse of (b,a) we take as

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

For,

$$(b,a)(b^{-1}, (a^{\alpha(b^{-1})})^{-1}) = (bb^{-1}, a^{\alpha(b^{-1})}((a^{\alpha(b^{-1})})^{-1}) = (1,1).$$

Similarly,

$$(b^{-1}, (a^{\alpha(b^{-1})})^{-1})(b,a) = (b^{-1}b, ((a^{\alpha(b^{-1})})^{-1})^{\alpha(b)}a).$$

But

$$\begin{aligned}((a^{\alpha(b^{-1})})^{-1})^{\alpha(b)} &= ((a^{\alpha(b^{-1})})^{\alpha(b)})^{-1}\\ &= (a^{\alpha(b^{-1})\alpha(b)})^{-1} = ((a^{\alpha(b^{-1}b)})^{-1} = (a^{\alpha(1)})^{-1} = a^{-1}.\end{aligned}$$

Therefore, $(b^{-1}, (a^{\alpha(b^{-1})})^{-1})(b,a) = (1,1)$. We have now only to verify the associative law. Let $(b,a), (b',a')$ and $(b'',a'') \in B \times A$. Then

$$\begin{aligned}((b,a)(b',a'))(b'',a'') &= (ba, a^{\alpha(b')}a')(b'',a'')\\ &= ((bb')b'', (a^{\alpha(b')}a')^{\alpha(b'')}a'')\\ &= (b(b'b''), (a^{\alpha(b')\alpha(b'')}a'^{\alpha(b'')})a'')\\ &= (b(b'b''), a^{\alpha(b'b'')}a'^{(b'')}a'')\\ &= (b,a)(b'b'', a'^{(b'')}a'')\end{aligned}$$

$$= (b, a)((b', a')(b'', a'')).$$

Thus $B \times A$ is a group with the multiplication we have defined. **90**

To show that G is an extension of A by B, we have first to identify A with some subgroup of G. In other words we have to find a suitable monomorphic image of A in G. Consider the mapping $\prod_1$ of A into G defined by

$$a^{\prod_1} = (a, a) \text{ for all } a \in A.$$

Now,

$$(aa')^{\prod_1} = (1, aa') = (11, a^{\alpha(1)}a') = (1, a)(1, a') = a^{\prod_1}a'^{\prod_1}$$

and $a^{\prod_1} = (1, 1)$ if and only if $a = 1$. Therefore $\prod_1$ is a monomorphism of A into G, the monomorphic image the subgroup $\left\{(1, a)\middle| a \in A\right\} \leq G$.

91 We identify A with this monomorphic image; in other words we write a for $(1, a)$, for all $a \in A$.

Similarly, consider the mapping the mapping $\prod_2$ of B into G defined by

$$b^{\prod_2} = (b, a), \text{ for all } b \in B.$$

We have

$$(bb')^{\prod_2} = (bb', 1) = (bb', 1^{\alpha(b')}1) = (b, 1)(b', 1) = b^{\prod_2}b'^{\prod_2}$$

Further $b^{\prod_2} = (1, 1)$ if and only if $b = 1$. Therefore $\prod_2$ is a monomorphism of B into G, and

$$B^{\prod_2} = \left\{(b, a)\middle| b^* \in B\right\} \leq G.$$

We identity B with $B^{\prod_2}$ and write b for (b, a), for all $b \in B$.

Now,

$$ba = (b, a)(1, a) = (b1, 1^{\alpha(1)}a) = (b, a).$$

Therefore every element (b, a) of G can be written as

$$(b, a) = ba, \text{ with } b \in B, a \in A.$$

By the identification we have made, it is easily seen that $A\cap B = \{1\}$. We claim that the representation of a pair (b, a) as a product ba is unique. For if

$$ba = b'a', \text{ with } b, b' \in\in B, a, a' \in A,$$

then $b'^{-1}b = a'a^{-1}$. But $A \cap B = \{1\}$. Hence, 92

$$b'^{-1}b = a'a^{-1} = 1, \text{ i.e }, a = a', b = b'.$$

Consider now the mapping $\prod$ of G onto B defined by

$$(ba)^{\prod} = b.$$

(Note that the uniqueness of the representation ba ensure that $\prod$ is a mapping.) We assert that $\prod$ is an epimorphism of G onto B with A as kernel, For,

$$((ba)(b'a'))^{\prod} = (bb'a^{\alpha(b')}a')^{\prod} = bb' = (ba)^{\prod}(b'a')^{\prod}$$

for all $b, b' \in B, a, a' \in A$.It is easy to see that the kernel of $\prod$ is A and therefore

$$A\Delta G, G/A \cong B.$$

Hence G is an extension of A by B. We call G a splitting extension (split extension or semi-direct product) of A by B.

By the above construction it follows that G depends on the homomorphism α also. In particular, if we take for α the trivial homomorphism, that is, the mapping which maps every element of B onto the identity automorphism of A, it is easy to see that the corresponding splitting extension is the direct product of A and B.

If α is an isomorphism of B onto the group of automorphisms of A, then corresponding splitting extension is known as the *holomorph* of A. 93

We note that in a splitting extension of A by B,

$$b^{-1}ab = a^{\alpha(b)} \text{ for all } a \in A;$$

that is to say, all the automorphism $\alpha(b)$ of A are induced by inner automorphisms of the splitting extension. In particular when G is the holomorph of A, all the automorphisms of A are induced by the inner automorphisms of G.

Not all extensions of A by B are necessarily splitting extensions. Consider the group Q generated by two elements i, j with the defining relations

$$i^{-1}ji = j^{-1}, j^{-1}ij = i^{-1}.$$

This group is known as the *quaternion* group (see Coxeter and Moser, 1957). It is not difficult to prove the order of Q is 8, the element i is four, and the only subgroup of order 2 in Q is $\{1, i^2\}$. Let now $A = gp(i)$. Then the subgroup A being of index 2 in Q is a normal subgroup of Q. Thus Q is an extension of A by a cyclic group of order 2. But the only subgroup of order 2 of Q is $gp(i^2)$, which is contained in A. Therefore Q is not a splitting extension of A. The subgroup $gp(i^2)$ is also normal in Q, as it is the only subgroup of order 2 of Q. But

$$Q/gp(i^2) \cong V_4 = gp(a, b : a^2 = b^2 = 1).$$

94 However, Q contains only one subgroup of order 2, hence cannot contain any subgroup isomorphic to V_4. Therefore Q is not a splitting extension of $gp(i^2)$.

3

The quaternion group Q is a finite group which is presented by two generators and two relations. Let G be a group generated by a minimal set of generators consisting of d elements, and let the number of defining relations in these generators be e. It is not difficult to prove that if $e < d$, then the group G is infinite. Thus for finite groups, one necessarily has $e \geq d$. Obviously the finite cyclic group are examples of finite groups with $e = d = 1$. Some examples of finite groups with $e = d = 2$ can be found in B.H.Neumann (1956).

H.Mennicke (Kiel, Germany now Glasgow) has shown that the following group is finite:

$$G = gp\left(a, b, c : a^b, b^3, b^c = b^3, c^a = c^3\right).$$

It is not difficult to verify that G cannot be generated by generated by fewer than three elements; thus G is an example of a finite group with $e = d = 3$. Later Mennicke and $I.P.$ Macdonald (Manchester) independently have given an infinite sequence if finite groups with $e = d = 3$. (The results of Mennick and Macdonald are to be published in Arch. Math. and Canod J.math., respectively. This suggests the following

Unsolved problem. Are there finite groups with $e = d = 4$ that cannot be generated by fewer than 4 elements? 95

4

Let G be a group, and A, B subgroups of G satisfying the following conditions:

(i) $G = AB$, (ii) $A \cap B = \{1\}$

We call G the *general product* of the subgroups A and B[1].

If G is the general product of its subgroups A and B, then it can also be written as $G = AB$. For,

$$G = G^{-1} = (AB)^{-1} = B^{-1}A^{-1} = BA.$$

Every $g \in G$ can be represented as the product of an element of A and an element of B. Moreover, this representation is unique. For, if $g = ab = a'b'$ with $a, a' \in A, b, b' \in B$, then

$$a'^{-1} = b'b^{-1} \in A \cap B = \{1\}$$

Hence $a'^{-1}a = 1 = b'b^{-1}$, i.e, $a = a', b = b'$.

We have seen (section 2 of this chapter) that if G is a splitting extension of its subgroup A by a subgroup B, then

(i) $G = BA$, (ii) $B \cap A = \{1\}$ and (iii) $A \Delta G$.

We claim that conditions (i), (ii) and (iii) are sufficient in order that G be a splitting extension of A by B. To prove this, we define a mapping 96
α of B into the group of automorphisms of A as follows: for every $b \in B$,

$$a^{\alpha(b)} = b^{-1}ab \text{ for all } a \in A.$$

[1]Note:- In the recent literature it is also often called the Zappa-Szep-Redei product

Since $A\Delta G$, it admits all inner automorphisms of G, and hence $\alpha(b)$ is an automorphism of A. We assert that α is a homomorphism of B into the group of automorphisms of A. For,

$$\begin{aligned} a^{\alpha(bb')} &= (bb')^{-1}a(bb') = b'^{-1}(b^{-1}ab)b' = b'^{-1}a^{\alpha(b)}b' \\ &= (a^{\alpha(b)})^{\alpha(b')} = a^{\alpha(b)\alpha(b')} \end{aligned}$$

for every $a \in A$ and all $b, b' \in B$. Hence

$$\alpha(bb') = \alpha(b)\alpha(b') \text{ for all } b, b' \in B;$$

that is, α is a homomorphism.

The condition (ii) immediately gives $ba = b'a'$ is and only if $b = b', a = a'$. Now, $(ba)(b'a') = bb'b'^{-1}ab'a' = bb'a^{\alpha(b')}a'$. This proves that G is a splitting extension of A by B.

If, decides conditions (*i*), (*ii*) and (*iii*), G also satisfies (*iv*) $B\Delta G$, then G is the direct product of A and B. For,

$$a^{\alpha(b)} = b^{-1}ab = aa^{-1}b^{-1}ab = a[a, b]$$

for all $a \in A, b \in B$. And since $A\Delta G$, $B\Delta G$, we have

$$[a, b] = (a^{-1}b^{-1}a)b = a^{-1}(b^{-1}ab)\, A \cap B = \{1\},$$

i.e., $$[a, b] = 1, \text{ for all } a \in A, b \in B.$$

97 That is $a^{\alpha(b)} = a$ for all $a \in A$; thus $\alpha(b)$ is the identity automorphism of A for every $b \in B$. Therefore, α is the trivial homomorphism, and G is the direct product of A and B.

Conversely if G is the (internal) direct product of its subgroup A and B, then G satisfies (i), (ii), (iii) and (iv).

Then we have

Theorem 4. 1. *G is a splitting extension of A by B if and only if it satisfies conditions (i), (ii) and (iii).*

2. *G is the direct product of A and B if and only if it satisfies conditions (i), (ii), (iii) and (iv).*

5 Regular permutation representations of a group by right multiplications

Let G be a group. We know that the set of all one-one mapping of G onto G, or *permutations* of G forms a group (called the symmetric group) with the composition of mapping as multiplication. We shall embed G in this permutation group; in other words, we shall find a monomorphic image of G in this group.

For every $g \in G$, we define a permutation $\rho(g)$ of G by

$$x^{\rho(g)} = xg, \text{ for all } x \in G.$$

It is easy to verify that $\rho(g)$ is a permutation of G; but this also **98**
follows from the homomorphism property to be moved now. Consider the mapping ρ of G into the group of permutations of G, defined by

$$g^{\rho} = \rho(g) \text{ for all } g \in G.$$

We claim that ρ is a monomorphism. Let $g, h \in G$. Then

$$\begin{aligned} x^{\rho(gh)} &= x(gh) = (xg)h = x^{\rho(g)}h = (x^{\rho(g)})^{\rho(h)} \\ &= x^{\rho(g)}, \text{ for all } x \in G. \end{aligned}$$

Therefore,

$$\rho(gh) = \rho(g)\rho(h), \text{ for all } g, h \in G.$$

Further, $\rho(g) = 1$ means

$$x^{\rho(g)} = xg = x, \text{ for all } x \in G.$$

In particular if we take $x = 1$, we get $g = 1$. Hence ρ is a homomorphism with trivial kernel, that is, a homomorphism. Thus $G \cong \rho(G)$.

We call $\rho(g)$a *right multiplication*, and $\rho(G)$ the regular permutation representation by right multiplications.

In this context, we can realise the holomorph of G as a subgroup of the symmetric group S_G of all permutation of G, namely as the normaliser of $\rho(G)$ in S_G.

6 Wreath Product

99 Let A be an abstract group, and B a permutation group of a set Y. Consider A^Y, the Cartesian power of A; this consists of all functions on Y with values in A. If $f, g \in A^Y$, then

$$fg(y) = f(y)g(y), \text{ for all } y \in Y.$$

We want to represent B as an automorphism group of A^Y. In other words we want to find a homomorphism of B into the group of automorphisms of A^Y. For every $b \in B$, we define a mapping $\alpha(b)$ of A^Y into A^Y by

$$f^{\alpha(b)}(y) = f(y^{b^{-1}}) \text{ for all } y \in Y.$$

We first prove that $\alpha(b)$ is an endomorphism of A^Y. We have

$$\begin{aligned}(fg)^{\alpha(b)}(y) &= (fg)(y^{b^{-1}}) = f(y^{b-1})g(y^{b^{-1}})\\ &= f^{\alpha(b)}(y)g^{\alpha(b)}(y) = (f^{\alpha(b)}g^{\alpha(b)})(y),\end{aligned}$$

for all $y \in Y$. Therefore

$$(fg)^{\alpha(b)} = f^{\alpha(b)}g^{\alpha(b)}, \text{ for all } f, g \in A^Y.$$

Further,

$$\begin{aligned}f^{\alpha(bb')}(y) &= f(y^{(bb')^{-1}}) = f(y^{b'^{-1}b^{-1}})\\ &= f((y^{b'^{-1}})^{b^{-1}}) = f^{\alpha(b)(y^{b'^{-1}})} = (f^{\alpha(b)})^{\alpha(b')}(y)\\ &= f^{\alpha(b)\alpha(b')}(y), \quad \text{for all } y \in Y.\end{aligned}$$

100 Hence $\alpha(bb') = \alpha(b)\alpha(b')$

Again, this is true for all $b, b' \in B$, hence the mapping α of B into the semigroup of endomorphisms of A^Y is a homomorphism. It follows that $\alpha(B)$ is a group, and also that every $\alpha(b)$ is an automorphism of A^Y. (Incidentally, one easily verifies that α is a monomorphism, provided that A is non - trivial).

We now form the splitting extension P of A^Y by B in terms of α. Every element p of P can be written uniquely as

$$p = bf, b \in B, f \in A^Y.$$

if $p' = b'f'$ with $b' \in B$, $f' \in A^Y$ is any other element of P, then

$$pp' = (bf)(b'f') = bb'f^{\alpha(b')}f'$$

We call P the (*Cartesian, full, or unrestricted) wreath product of* A and B write

$$P = AWrB$$

(P. Hall uses the notation $A\overline{\wr}B$, see P. Hall (1954^b).) **101**

Instead of taking the Cartesian power A^Y, we could start with the corresponding direct power of A; we then arrive at a group P^* the *direct (or restricted) wreath product* of A and B, and we write

$$P^* = AwrB.$$

(P. Hall uses the notation $A\overline{\wr}B$. If Y is a finite set, the two wreath products are equal:

$$AWrB = AwrB.$$

Next we shall consider the case when both A and B are abstract groups. We represent B as a permutation group of $Y = B$ by right multiplications and form the wreath product P of A and the permutation group of Y which represents B. We call P the wreath product of the abstract groups A and B. We shall identify every element b of B with the corresponding right multiplication $\rho(b)$ and write b for $\rho(b)$; that is,

$$y^{\rho(b)} = y^b, \text{ for all } y \in B.$$

As before α is the homomorphism of B into the group of automorphism of A^B defined by

$$f^{\alpha(b)}(y) = f(y^{b^{-1}}) = f(yb^{-1}), \text{ for all } y \in B.$$

This is a slight simplification of the notation, and we further simplify it by writing b for $\alpha(b)$. Thus we write

$$f^b(y) = f(yb^{-1}), \text{ for all } y \in B, f \in A^B.$$

(This accords with our usual notation, by which $b^{-1}fb = f^b$).

Every element p of P can be written uniquely as $p = bf$ with $b \in B$, $f \in A^B$; and

$$(bf)(b'f') = bb'f^{b'}f', \text{ for all } b, b' \in B, f, f' \in A^B.$$

102 Thus by this convention of identifying the abstract group B with the group of all right multiplications of B, we form the wreath product of any two abstract groups.

Now suppose both A and B are permutation groups, say of sets X and Y respectively. In this case we can give a particularly simple permutation representation on the product set $X\ Y$ for the wreath product of A and B. To this end, we reverse the order of the factors in the splitting extension P of A^Y by B, that is, we now write the element of P in the form

$$p = fb, f \in A^Y, b \in B.$$

Then multiplication of such products takes the form

$$\begin{aligned}(fb)(f'b') &= fbf' - b^{-1}bb' = ff'^{b-1}bb'\\ &= f^*b^* \quad \text{say},\end{aligned}$$

where $f^* = ff'^{b^{-1}} \in A^Y$ and $b^* = bb' \in B$. For every fb of P, we define a mapping (f, b) of the set $X \times Y$ into itself as follows:

$$(x, y)^{(f,b)} = (x^{f(y)}, y), \text{ for all } (x, y) \in X \times Y.$$

We shall now show that the mapping φ of P into the set of all mapping of $X \times Y$ into itself, defined by

$$(fb)^{\varphi} = (f, b)$$

103 is a monomorphism. Let fb, $f'b' \in P$, with $f, f' \in A^Y, b, b' \in B$.

Then

$$(fb)(f'b') = ff^{b-1}bb' = f^*b^*.$$

Now,

$$(x, y)^{(f,b)(f',b')} = \left(x^{f(y)}, y^b\right)^{(f',b')}$$

$$= \left(\left(x^{f(y)}\right)^{f'(y^b)}, (y^b)^{b'}\right)$$
$$= \left(x^{f(y)^{f'^{b-1}}}(y), y^{bb'}\right)$$
$$= \left(x^{ff'^{b-1}}(y), y^{bb'}\right) = \left(x^{f^*}(y), y^{b^*}\right);$$

and as this is true for all $(x, y) \in X \times Y$ it follows that

$$(b, b)(f', b') = (f^*, b^*),$$

that is,
$$((fb)(f'b')) = (fb)(f'b')$$

This proves that φ is a homomorphism.

It follows that every (f, b) is a permutation of $X \times Y$. We claim that φ is a monomorphism of P into the symmetric group of permutations of $X \times Y$. For if $(f, b) = (f', b')$, then

$$(x, y)^{(f,b)} = (x^{f(y)}, y^b) = (x^{f'(y)}, y^{b'}) = (x, y)^{(f',b')}$$

for all $(x, y) \in X \times Y$. Hence **104**

$$x^{f(y)} = x^{f'(y)} \text{ for all } \quad x \in X$$

Therefore $f(y) = f'(y)$.

Again this holds for all $y \in Y$; thus $f = f'$. Similarly, $y^b = y^{b'}$ for all $y \in Y$; hence $b = b'$. This show that φ is a monomorphism. Thus we have represented P as a group of permutations of $X \times Y$.

In the following, we shall identify the wreath product of the permutation groups A and B (of the sets X and Y respectively), with its representation as a permutation group of $X \times Y$.

The above permutation representation of the wreath product of two permutation groups makes the wreath product associative. In other words, if A, B and C are permutation groups of sets X, Y, and Z respectively, then

$$(A Wr B) Wr C \cong A Wr (B\, Wr\, C).$$

In fact, if we make the natural identification of $((x, y), z) \in (X \times Y) \times Z$ and

$$(x, (y, z)) \in X \times (Y \times Z)$$

with the triplet $(x, y, z) \in X \times Y \times Z$ then $(AWrB)\,Wr\,C$ and $AWr(BWrC)$ become the same permutation group of $X \times Y \times Z$. This will consist of
105 the mapping (F, g, c) where $F \in A^{Y\times Z}, g \in B^{z}, c \in c$ and

$$(x, y, z)^{(F,g,c)} = \left(x^{F(y,z)}, y^{g(z)}, z^{c}\right).$$

Write $P = AWrB, Q = BWrC$. Then

$$P = \left\{(f, b)\middle| f \in A^{Y}, b \in B\right\},$$

and
$$(AWrB)WrC = PWrC = \left\{(\varphi, c)\middle|\varphi \in P^{z}, c \in C\right\}$$

Now, if $\varphi \in P^{z}, \varphi(z)$ is of the form

$$\varphi(z) = (f_z, b_z),\ f_z \in A^{Y}, b_z \in B.$$

Write

$$f_z(y) = F(y, z), b_z = g(z).$$

We have

$$\begin{aligned}
((x, y), z)^{(\varphi,c)} &= \left((x, y)^{\varphi(z)}, z^{c}\right)\\
&= \left((x, y)^{(f_z,b_z)}, z^{c}\right) = \left((x^{f_z(y)}, y^{b_z}), z^{c}\right)\\
&= \left((x^{F(y,z)}, y^{g(z)}), z^{c}\right)\\
&= \left(x^{F(y,z)}, y^{g(z)}, z^{c}\right) \quad \text{(by our identification)}\\
&= (x, y, z)^{(F,g,c)} \quad \text{(say)}.
\end{aligned}$$

Conversely, by retracing the above steps, one can easily see that
106 any triplet of the form (F, g, c) with $F \in A^{Y\times Z}, g \in B^{Z}$ and $c \in C$ is (by our identification) an element of $(AWrB)WrC$. Thus the group $(AWrB)WrC$ consists of all permutations of $X\times Y\times Z$ of the form (F, g, c) with $F \in A^{Y\times Z}, g \in B^{Z}, c \in C$, and

$$(x, y, z)^{(F,g,c)} = \left(x^{F(y,z)}, y^{g(z)}, z^{c}\right)$$

for all $(x, y, z) \in X \times Y \times Z$.

Similarly, we have

$$Q = \left\{(g, c) \middle| f \in B^z, c \in C\right\},$$

and $$AWr(BWrC) = AWrQ = \left\{(F, q) \middle| F \in A^{Y\times Z}, q \in Q\right\}$$

Let $q = (g, c) \in Q$.Then

$$\begin{aligned}(x,(y,z))^{(F,q)} &= (x^{F(y,z)}, (y,z)^q)\\ &= \left(x^{F(y,z)}, (y^{g(z)}, z^c)\right)\\ &= \left(x^{F(y,z)}, y^{g(z)}, z^c\right), \quad \text{again by our identification}\\ &= (x,y,z)^{(F,g,c)}.\end{aligned}$$

Conversely, we can prove that any (F, g, c) is an element of $AWr(B$ $WrC)$. Thus we have proved that

$$(AWrB)WrC = AW(BWrC).$$

Let us now compute the cardinality of the group $(AWrB)WrC$. It is easy to see that

$$|AWrB| = |B||A|^{|Y|}$$

and $$\begin{aligned}|(AWrB)WrC| &= |AWrB|^{|Z|}|C|\\ &= (|B||A|^{|Y|})^{|Z|}|C| = |A|^{|Y||Z|}|B|^{|Z|}|C|\\ &= |AWr(BWrC)| \text{ because of associativity}.\end{aligned}$$

In general the wreath product of two abstract groups as we have defined it is not associative. Let A and B be two abstract groups. Then by definition $AWrB$ is a group with the set $B\times A^B$ as carrier and therefore **107**

$$|AWrB| = |A|^{|B|}|B|.$$

Let now A, B, C be three abstract groups of orders say 2, 3, 5 respectively

$$|A| = 2, |B| = 3, |C| = 5.$$

Then we have

$$|AWrB| = |A|^{|B|}|B| = 2^3 3, \quad \text{and}$$
$$|(AWrB)WrC| = |AWrB|^{|C|}|C| = (2^3 3)^5 5 = 2^{15} 3^5 5$$

on the other hand $|BWrC| = |B^{|C|}|C| = 3^5 5$ and

$$|AWr(BWrC)| = |A|^{|BWrC|}|BWrC| = 2^{3^5 .5} 3^5 5.$$

108 Hence

$$AWr(BWrC) \neq (AWrB)WrC.$$

Thus in general the wreath product of abstract groups is not associative and the wreath products of two groups A and B depends upon the permutation representation we choose for B.

7

We shall later have occasion to use the wreath product of group while certain embedding theorems. As a first illustration of wreath products and their usefulness, we ally them to find the sylow subgroups of finite symmetric groups.

Let A and B be cyclic groups of order 3, say

$$A = gp(a_o : a_0^3 = 1), B = gp(b_0 : b_0^3 = 1).$$

The groups A and B can be regarded as permutation groups on the set $X = \{1, 2, 3\} = Y$ by identifying a_0 and b_0 with the cycle (123); thus

$$1^{a_0} = 2, 2^{a_0} = 3, 3^{a_0} = 1,$$

and similarly for b_0. Write $P = AWrB$. The group P has permutation representation on the set $X \times Y$, since the groups A and B are permutation groups on the set $X = Y\{1, 2, 3\}$.

Now,

$$X \times Y = \{(1, 1), (1, 2), (1, 3), (2, 1)(2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

109 For convenience, we rename these pairs $1, 2, 3, 4, 5, 6, 7, 8, 9$ in the same order; i.e.,

$$\begin{aligned} (1, i) &= i, && (i = 1, 2, 3) \\ (2, j) &= 3 + j, && (j = 1, 2, 3) \\ (3, k) &= 6 + k, && (k = 1, 2, 3) \end{aligned}$$

The group $A^Y = A \times A \times A$ consists of all functions on the set $\{1, 2, 3\}$ with values in A. In our usual notation,

$$P = \{(f, b) | f \in A \times A \times A, b \in B\},$$

where (f, b) is the permutation of $X \times Y$ such that

$$(x, y)^{(f,b)} = (x^{f(y)}, y^b), x \in X, y \in Y.$$

Define $f_i \in A^Y, i = 1, 2, 3$ by

$$f_i(j) = 1 \text{ for } i \neq j, f_i(i) = a_0 (j = 1, 2, 3).$$

Then it is easy to verify that

$$A^Y = gp(f_1, f_2, f_3).$$

Since $(f, b) = (f, 1)(1, b)$ for all $f \in A^Y, b \in B$,we have

$$P = gp((f_1, 1), (f_2, 1), (f_3, 1), (1, b_0)).$$

Now we can easily write down the permutations $(f_1, 1), (f_2, 1)(f_3, 1)$ and $(1, b_0)$. We have 110

$$\begin{aligned} (1, 1)^{(f_1,1)} &= \left(1^{f_1(1)}, 1^1\right) = (2, 1) \\ (2, 1)^{(f_1,1)} &= \left(2^{f_1(1)}, 1^1\right) = (3, 1) \\ (3, 1)^{(f_1,1)} &= \left(3^{f_1(1)}, 1^1\right) = (1, 1) \end{aligned}$$

and $$(i, j)^{(f_1,1)} = (i^{f_1(j)}, j^1) = (i, j), \text{ for } i = 1, 2, 3, j = 2, 3.$$

Thus, in the alternative notation

$$(f_1, 1) = (147).$$

Similarly, $(f_2, 1) = (258), (f_3, 1) = (369)$. Further

$$\begin{aligned}
(1,1)^{(1,b_0)} &= (1^{1(1)}, 1^{b_0}) = & (1,2)\\
(1,2)^{(1,b_0)} &= & (1,3)\\
(1,3)^{(1,b_0)} &= & (1,1),
\end{aligned}$$

and so on. Therefore,

$$(1, b_0) = (123)(256)(789)$$

111 But

$$\begin{aligned}
&(1, b_0)^{-1}(f_1, 1)(1, b_0)\\
&= (321)(654)(987)(123)(456)(789)\\
&= (258) = (f_2, 1)
\end{aligned}$$

Similarly, $(1, b_0)^{-1}(f_2, 1)(1, b_0) = (f_3, 1)$.

Hence the group P is generated by the two permutations $(f_1, 1)$ and $(1, b_0)$; that is, by (147) and (123)(456)(789). We also note that P is here represented as a group of permutations of degree 9, that is, as a subgroup of the symmetric group S_9. The order of the group P is

$$|P| = |A|^{|Y|}|B| = 3^3 3 = 3^4.$$

It is easy to see that $3^4 T 9!$; that is 3^4 is the highest power of 3 dividing the order $9! ofS_9$. Thus P is a ”sylow subgroup” of S_9.

Let G be a finite group, and p a prime. If $p^k T G$, the G has subgroups of order p^k. Such subgroups are called *sylow subgroups.* There are a number of important theorems (known as sylow theorems) about these subgroups. See e.g Kurosh (1956, §54) and Zassenhaus (1958, Ch. IV, p. 135).

The example considered above is a particular case of the following theorem.

112 **Theorem 5** (Kaloujnine, 1948). *The sylow p-subgroup of S_{p^n} is the wreath product*

$$P_n = C_p Wr C_p Wr \cdots Wr C_p (n \text{ times })$$

were $C_p = gp(c_0 : c_0^p = 1)$ is the cyclic group of order p. The group C_p can be regarded as the subgroup generated by the cycle $(12 \cdots p)$ *in S_p.*

Let $X = \{1, 2, \ldots, p\} = X_1 = \cdots = X_n$, and

$$Z = \left\{(x_1, x_2, \ldots, x_n) \middle| x_i \in X_i, i = 1, \ldots, n\right\};$$

that is to say,

$$Z = X_1 \times X_2 \cdots \times X_n = X^n.$$

We rename the elements $(x_1, \ldots, x_n)$ of Z, and write $1 + \sum\limits_{i=1}^{n} (x_i - 1) p^{i-1}$ for $(x_1, \ldots, x_n)$. We note that $|Z| = p^n$. In the new notation, we have $P_n \leq S_{p^n}$.

Since the wreath product is associative (note that we are using permutation groups), we get

$$P_n = P_{n-1} Wr C_p.$$

Therefore $|P_n| = |P_{n-1}|^p |C_p| = |P_{n-1}|^p p$
$= p^{k(n)}$ (say).

Here $k(n)$ is defined by the recurrence relation

$$k(1) = 1, k(n) = pk(n-1) + 1.$$

We shall prove by induction that 113

$$p^{k(n)} \top p^n;$$

For $n = 1$, this is obvious. Assume that

$$p^{k(n-1)} \top p^{n-1};$$

Now,

$$p^n = \left(\prod_{r=1}^{p^{n-1}} r\right)\left(\prod_{r=1}^{p^{n-1}}(p^{n-1}+r)\right)\left(\prod_{r=1}^{p^{n-1}}(2p^{n-1}+r)\right)\cdots\left(\prod_{r=1}^{p^{n-1}}((p-1)p+r)\right)$$

We have $p^s \top (mp^{n-1}+r)$ if and only if $p^s \top r$, $m < p-1, 1 \leq r \leq p^{n-1}$. Therefore,

$$p^{k(n-1)} \top \prod_{r=1}^{p^{n-1}}(mp^{n-1}+r) \text{ for } m < p-1.$$

But $p^{k(n-1)+1} \top \prod_{r=1}^{p^{n-1}}((p-1)p^{n-1}+r)$, since the last term of this product is p^n. Hence $(p^{k(n-1)})^p p = p^{k(n)} \top p^n$; for all n, Thus P_n is a sylow subgroup of S_{p^n}. It is not difficult to use this result to compute the sylow subgroups of any symmetric group S_m.

Chapter 7

Varieties of Groups (Contd.)

1

Let $\underline{\underline{V}}$ be a variety defined by a set of laws L, that is $\underline{\underline{V}}$ consists of all 114
groups in which the laws of L hold. If $G \in \underline{\underline{V}}$ and $H \leq G$, then $H \in \underline{\underline{V}}$. Let G' be any epimorphic image of G; that is, there is an epimorphism φ of G onto G'. Now if

$$w(X_1, \ldots, X_n) = 1$$

is a law in $\underline{\underline{V}}$, then it is also a law in G'. For, let $g'_1, \ldots, g'_n$ be arbitrary elements of G'. Because φ is an epimorphism, there exist elements $g_1, \ldots, g_n \in G$ such that

$$g_i^{\varphi} = g'_i, 1, \ldots, n.$$

Now,

$$\begin{aligned} &(w(g_1, \ldots, g_n))^{\varphi} = 1 = w(g_1^{\varphi}, \ldots, g_n^{\varphi}) \\ \text{i.e.,} \quad &w(g'_1, \ldots, g'_n) = 1; \text{ thus} \\ &w(X_1, \ldots, X_n) = 1 \end{aligned}$$

is a law in G. Therefore

$$G' \in \underline{\underline{V}}$$

Let $\{G_i\}_{i\in I}$ be an arbitrary family of groups of $\underset{=}{V}$. We assert that the 115
cartesian product P of $\{G_i\}_{i\in I}$ is in the variety $\underset{=}{V}$. Consider

$$f^* = w(f_1, \ldots, f_n) \in P,$$

where $f_1, \ldots, f_n$ are arbitrary elements of P and

$$w(X_1, \ldots, X_n) = 1,$$

is a law in L. Then

$$f^*(i) = w(f_1(i), \ldots, f_n(i)) = 1, \text{ for all } i \in I, \text{ since}$$
$$f_1(i), \ldots, f_n(i) \in G_i \text{ and } G_i \in \underset{=}{V}. \text{ Therefore}$$
$$f^* = w(f_1, \ldots, f_n) = 1p \text{ that is}$$
$$w(X_1, \ldots, X_n) = 1,$$

is a law in P. That is

$$P \in \underset{=}{V}.$$

Hence we have prove

Theorem 1. *Every variety is closed under the operations of forming subgroups* (S), *epimorphic maps* (Q) *and cartesian products* (R).

Theorem 1, enables us to make new groups of a variety $\underset{=}{V}$ by using there which we already know. A variety in general is not closed under the operation of "wreathing".

116 The converse of the above theorem is also true. Before proceeding to prove the converse we wish to remark that many of the concepts which we have introduced for groups can be generalised to abstract algebraic system in a natural way. For example, we can speak of a subalgebraic system of an algebraic system, a homomorphism of an algebraic system in to another, the cartesian product of a family of algebraic systems. Note that the concept of direct product cannot in general be introduced in the theory of algebraic system, as we may not have an analogue of the neutral element of a group. Thus proofs of Theorem 1 and Theorem 2 can easily be carried over to abstract algebraic systems.

Theorem 2. *A class of groups closed under the operations Q, R, S is a variety.*

We first prove two lemmas.

Let $\underline{\underline{G}}$ be a class of groups. We form the closure $\underline{\underline{C}}$ of $\underline{\underline{G}}$ under the operations Q, R, S. Let $\underline{\underline{V}}$ be the least variety containing $\underline{\underline{G}}$. By Theorem 1 $\underline{\underline{V}}$ is closed under the operations Q, R, S. Therefore

$$\underline{\underline{C}} \subseteq \underline{\underline{V}}.$$

Lemma 1. There is a group G^* with the following properties:

(i) $G^* \in \underline{\underline{C}}$

(ii) Every law $w(\underline{X}) = 1$

valid in G^*, is valid in every group of $\underline{\underline{G}}$ (and is hence a law of $\underline{\underline{V}}$).

Proof. Consider the class $\underline{\underline{F}}$ of all finitely generated groups of $\underline{\underline{C}}$. We **117**
split $\underline{\underline{F}}$ into disjoint classes $\underline{\underline{H}}_\alpha$ of mutually isomorphic groups, that is any two groups of $\underline{\underline{F}}$ are isomorphic if and only if they belong to the same $\underline{\underline{H}}_\alpha$. From each $\underline{\underline{G}}_\alpha$ we choose a group H_α and form the cartesian product G^* of $H_\alpha s$. Since each $H_\alpha \in \underline{\underline{C}}$, and $\underline{\underline{C}}$ is closed under the operations Q, R, S, we have

$$G^* \in \underline{\underline{C}}.$$

□

Let

$$w(X_1, \dots, X_n) = 1,$$

be a law in G^* and $G \in \underline{\underline{C}}$. For any $g_1, \dots, g_n \in G$, let

$$H = gp(g_1, \dots, g_n)\ (\leq G).$$

Now, $G \in \underline{\underline{G}}$ and $\underline{\underline{C}}$ is closed under the operations of taking subgroups.

Therefore

$$H \in \underset{=}{C}; \text{ infact}$$
$$H \in \underset{=}{F}.$$

Hence

$$H \simeq H_\alpha \text{ for some } \alpha.$$

Denote this isomorphism by θ. Let φ_α be the projection of G^* onto H_α. Then $\varphi_\alpha \theta^{-1}$ is an epimorphism of G^* onto H.

118 Therefore,

as
$$w(X_1, \ldots, X_n) = 1$$

is a law in G^*, it is also a law in H, and thus in particular

$$w(g_1, \ldots, g_n) = 1$$

is a relation in H and in G. But $g_1, \ldots, g_n$ were arbitrarily chosen in G. Hence

$$w(X_1, \ldots, X_n) = 1$$

is a law in G. Thus every law valid in G^* is also valid in $\underset{=}{G}$ and hence in $\underset{=}{V}$.

We have to verify from an axiomatic set-theoretic point of view that the construction of the cartesian product of the H_α is legitimate, that is to say we have to verify that the H_α form a family (or that they can be indexed by a set). Note that we have made a distinction between "class" and "set", though no emphasis has been placed on this distinction, as being outside group theory proper.

Now, every H_α is isomorphic to a quotient group of a free group of finite rank, say

$$H \simeq F_n/R,$$

where F_n is the free group of rank n and R a suitable normal subgroup
119 of F_n. Clearly F_n is countable for every n and therefore the cardinality of the set of all such Rs cannot exceed $2^{\mathcal{N}0}$. Hence there cannot be more H_α s than $\mathcal{N}_0 2^{\mathcal{N}0} = 2^{\mathcal{N}0}$; and thus they form a family. Hence we have

Corollary. *The group G^* of the lemma can be chosen to have order*

$$|G^*| \leq 2^{2^{\aleph_0}}.$$

Lemma 2. Let G^* be a group with the property that every law valid in G^* is also valid in $\underset{=}{G}$ (and hence in $\underset{=}{V}$), and let I be a set. Then there is a subgroup $F^* \leq G^{*^{G^{*^I}}}$ such that F^* is generated by a set of cardinal $|I|$, say

$$F^* = gp(\{f_i\}_{i \in I})$$

and if $G \in \underset{=}{V}$ is also generated by a set of cardinal $|I|$, say

$$G = gp(\{e_i\}_{i \in I}),$$

then there is an epimorphism φ of F^* onto G with

$$f_i^{\varphi} = e_i, \; i \in I.$$

Proof. Every element of $G^{*^{G^{*^I}}}$ is a function on G^{*^I} with values in G^*. To every $i \in I$, we define $f_i \in G^{*^{g^{*^{P_I}}}}$, by

$$f_i(g) = g(i), \text{ for all } g \in G^{*^I}.$$

Let 120

$$F^* = gp(\{f_i\}_{i \in I}).$$

We define the mapping φ of $\{f_i\}_{i \varphi I}$ onto $\{e_i\}_{i \in I}$ by

$$f_i = e_i, \text{ for all } i \in I.$$

We claim that φ can be extended to an epimorphism of F^* onto G. To prove this we have only to show that all the relations of F^* go over to the relations of G upon applying φ. □

Let

$$u(f_{i_1}, \ldots, f_{i_n}) = 1,$$

be a relation in F^*, with $f_{i_1}, \ldots, f_{i_n} \in F^*$. Then

$$u(f_{i_n}, \ldots, f_{i_n})(g) = 1, \text{ for all } g \in G^{*^I}$$

i.e.,
$$u(f_{i_n}, \ldots, f_{i_n}(g)) = 1, \text{ for all } g \in G^{*^I}$$

i.e.,
$$u(g(i_1), \ldots, g(i_n)) = 1, \text{ for all } g \in G^{*^I}.$$

Let $g_1^*, \ldots, g_n^*$ be arbitrary elements of G^*. There is an element of G^{*^I}, that is a function on I to G^*, which takes the values $g_1^*, \ldots, g_n^*$, at $i_1, \ldots, i_n$ respectively. We only have to define $h \in G^{*^I}$ by

$$h(i_1) = g_1^*, \ldots, h(i_n) = g_n^*$$

121 and $h(i)$ arbitrary otherwise, say

$$h(i) = 1 \text{ when } i \neq i_1, \ldots, i_n.$$

Then
$$u(g_1^*, \ldots, g_n^*) = u(h(i_1), \ldots, h(i_n)) = 1,$$

thus, as $g_1^*, \ldots, g_n^*$ where arbitrary elements of G^*,

$$u(X_1, \ldots, X_n) = 1$$

is a law in G^* and therefore a law in $\underset{=}{V}$; that is,

$$u(X_1, \ldots, X_n) = 1$$

is a law in G in particular

$$u(e_{i_1}, \ldots, e_{i_n}) = 1.$$

This proves φ can be extended to an epimorphism of F^* onto G. Hence the lemma.

Proof of Theorem 2. We shall now prove that

$$\underset{=}{C} = \underset{=}{V}.$$

Let G be any group of $\underline{\underline{V}}$ and E be a set of generators of E,

$$G = gp(E).$$

By Lemma 1, there is a group $G^* \in \underline{\underline{C}}$ such that every law in G^* is
122 a law in $\underline{\underline{V}}$. We choose an index set I with $|I| = |E|$. Then by Lemma 2, there is a subgroup $F^* \leq G^{*^{G^{*I}}}$ such that G is an epimorphic images of F^*. Now, since $\underline{\underline{C}}$ is closed under the operations Q, R, S, we have

$$G^* \in \underline{\underline{C}};$$

and therefore G, being an epimorphic image of F^*, is in $\underline{\underline{C}}$ that is

$$\underline{\underline{V}} \subseteq \underline{\underline{C}}.$$

combining this with the reversed inclusion which we have already proved, we get

$$\underline{\underline{C}} = \underline{\underline{V}}.$$

Corollary 1. *The group F^* is a reduced free group, of rank $|I|$, of the variety $\underline{\underline{V}}$.*

Corollary 2. *Let the class $\underline{\underline{G}}$ consist of a single group G_0 only, and let G_0 be finite. Then every reduced free group F^* of finite rank d of the least variety $\underline{\underline{V}}$ containing G_0 is finite, and its order is bounded by*

$$|F^*| \leq |G_0|^{|G_0|^d}$$

Proof. Take G_0 as the G^* of Lemma 2 and $|I| = d$. By Corollary 1, the 123
group F^* is a reduced free group of rank d.

Further

$$|F^*| \leq |F_0|^{|G_0^d}$$

Now, since F^* is a finite group it has finite number of defining relations, say

$$u_i(\underline{\mathrm{f}}) = 1,\ i = 1, \ldots, n.$$

We have already proved that

$$u_i(\underline{X}) = 1, \ i = 1, \ldots, n$$

are laws in $\underset{=}{V}$. Therefore every law of $\underset{=}{V}$ not involving more than d variables is a consequence of these n laws. In other words, the set of laws, not involving more than d variables, where d is an arbitrary positive integer, is "finitely based". Notice that this does not prove that $\underset{=}{V}$ is finitely based. (See section 2, ch.5, p.67). □

Theorem 3 (P. Hall (unpublished))**.** *Let $F = gp(\{f_i\}_{i\in I})$ be a group with the property that every mapping η of $\{f_i\}_{i\in I}$ into F can be extended to an endomorphism of F. Then F is a reduced free group of rank $|I|$ of the least variety containing F.*

Proof. Let

$$u(f_{i_1}, \ldots, f_{i_n}) = 1,$$

124 be a relation in F. We assert that

$$u(X_1, \ldots, X_n) = 1$$

is a law in F. Let $b_1, \ldots, b_n$ be arbitrary elements of F. Consider the mapping η of $\{f_i\}_{i\in I}$ into F defined by

$$f_{i_k}^{\eta} = b_k, \ k = 1, \ldots, n$$

and arbitrarily otherwise, say

$$f_i = f_i, \ i \neq i_1, \ldots, i_n.$$

□

By the hypothesis of the theorem, η can be extended to an endomorphism of F. which we also denote by η. Now

$$u(b_1, \ldots, b_n) = u(f_{i_1}^{\eta}, \ldots, f_{i_n}^{\eta}) = (u(f_{i_1}, \ldots, f_{i_n}))^{\eta} = 1^{\eta} = 1.$$

As $b_1, \ldots, b_n$ were chosen arbitrarily in F,

$$u(X_1, \ldots, X_n) = 1$$

is a law in F.

It follows that F is written as the factor group of a free group with respect to a normal ("relation") subgroup R, then R is verbal in the free group ($cf.$ Chapter 5). By Theorem 5, p.79 F then is a reduced free group of rank $|I|$ as claimed.

2

In this section we shall construct new varieties out of given varieties. **125**

Let $\underline{\underline{C}}, \underline{\underline{D}}$ be any two classes of groups. We say that a group G is a $\underline{\underline{C}}-$ by $-\underline{\underline{D}}$ group if G is an extension of a group $A \in \underline{\underline{C}}$ by a group $B \in \underline{\underline{D}}$. We define the class $\underline{\underline{C}}-$ by $-\underline{\underline{D}}$ as the class of all such groups G. [Thus e.g. a finite-by-abelian group is one with a finite normal subgroup whose factor group is abelian.]

Let $\underline{\underline{U}}, \underline{\underline{V}}$ be two varieties defined by the set of laws M and N respectively, where

$$M = \{u_i(\underline{X}) = 1\}_{i \in I} \text{ and}$$
$$N = \{v_j(\underline{X}) = 1\}_{j \in J}.$$

Without loss of generality we can assume that the set X of variables is countable, say

$$X = \{X_1, X_2, \ldots\}.$$

We denote by F the free group on these variables,

$$F = gp(X, \phi).$$

Our objective is to prove that the class $\underline{\underline{U}}-$ by $-\underline{\underline{V}}$ is a variety. Let

$$U = \{u(\underline{X}) | u(\underline{X}) = 1 \text{ a law in } \underline{\underline{U}}\}$$

and

$$V = \{v(\underline{X}) | v(\underline{X}) = 1 \text{ a law in } \underline{\underline{V}}\}.$$

We know that the groups U, V are verbal subgroups of F; in fact **126**
U, V are the verbal subgroups generated by the left-hand sides of M and

N respectively. We shall also denote these left-hand sides by M and N respectively.

Let

$$u(X_1, \ldots, X_m) = 1,$$

be a law in $\underset{=}{U}$ and

$$v_i(X_1, \ldots, X_{n_i}) = 1, i = 1, \ldots, m,$$

be laws in $\underset{=}{V}$. Write

$$w(\underline{\mathrm{X}}) = u(\underline{\mathrm{v}}(\underline{\mathrm{X}})) = u(v_1(X_1, \ldots, X_{n_1}), v_2(X_{n_1+1}, \cdots, X_{n_1+n_2}), \\ \ldots, v_m(X_{n_1+,\cdots+n_{m-1}+1}, \ldots, X_{n_1+\ldots+n_m})).$$

Let L denote the set of all laws of the form $w(\underline{\mathrm{X}}) = u(\underline{\mathrm{v}}(\underline{\mathrm{X}}) = 1$, with $u(\overline{X}) \in U$, $v(\underline{\mathrm{X}}) \in V$. We also denote the set of all left-hand sides of L by L. Let W be the verbal subgroup generated by L in F and $\underline{\mathrm{W}}$ be the variety defined by L. We shall use the notation

$$W = U_\circ V$$

and $$\underset{=}{W} = \underset{=}{U}\underset{=}{V}.$$

127 We shall now prove that

$$\underset{=}{U} - \text{ by } - \underset{=}{V} = \underset{=}{U}\underset{=}{V}.$$

If H is any set of words in the variables $X_1, X_2, \ldots$ and G any group, then we denote the verbal subgroup defined by H in G by G_H. In particular

$$W = F_L = F_W,\ U = F_U = F_{\{u_i\}\ i\in I}, V = F_V = F_{\{v_j\}\ j\in J}.$$

Let G be any group in the class $\underset{=}{U}-$ by $-\underset{=}{V}$. Then there exist groups A, B, such that

$$A\Delta G,\ G/A \simeq B, \text{ with } A \in \underset{=}{U},\ B \in \underset{=}{V};$$

that is, there is an epimorphism β of G onto B with A as its kernel. We assert that the verbal subgroup defined by V in G, namely G_V, is a subgroup of A. For consider

$$v(g_1, \ldots, g_n) \text{ with } v(\underline{X}) \in V, g_1, \ldots, g_n \in G;$$

we have $(v(g_1, \ldots, g_n))^\beta = v(g_1^\beta, \ldots, g_n^\beta) = 1$, since $B \in \underline{\underline{V}}$.

Hence 128

$$G_V \le A.$$

Now if

$$\begin{aligned} w(\underline{X}) = u(\underline{v}(\underline{X})) &\in W, \text{ where} \\ \underline{v}(\underline{X}) = (v_1(\underline{X}), \ldots v_m(\underline{X})), &\text{ then} \end{aligned}$$

$v_i(g) \in G_V \le A$, with gs belonging to G and for $i = 1, \ldots, m$. Since

$$u(X_1, \ldots, X_m) = 1$$

is a law in $\underline{\underline{U}}$ and hence in A, we have

$$\begin{aligned} u(\underline{v}(g)) = 1; &\text{ that is} \\ u(\underline{v}(\underline{X})) = 1 & \end{aligned}$$

is a law in G in other words,

$$G \in \underline{\underline{W}} = \underline{\underline{U}}\,\underline{\underline{V}}.$$

Hence

$$\underline{\underline{U}} - \text{ by } - \underline{\underline{V}} \subseteq \underline{\underline{U}}\underline{\underline{V}}.$$

Conversely let G be any group of the variety $\underline{\underline{U}}\,\underline{\underline{V}}$. The verbal subgroup G_V is fully invariant and hence trivially normal in G. It is easy to 129
verify that $G/G_V \in \underline{\underline{V}}$. (This is in fact true for any group G.) We claim that

$$G_V \in \underline{\underline{U}};$$

for let

$$u(X_1, \ldots, X_m) = 1$$

be any law in $\underline{\underline{U}}$ and $v_1(\underline{\mathrm{g}}), \ldots, v_m(\underline{\mathrm{g}}) \in G_V$; then

$$u(\underline{\mathrm{v}}(\underline{\mathrm{g}})) = u(v_1(\underline{\mathrm{g}}), \ldots, v_m(\underline{\mathrm{g}})) = 1;$$

that is, $$u(X_1, \ldots, X_m) = 1$$

is a law in G_V.Hence

$$G_V \in \underline{\underline{U}},$$

i.e., $$G \in \underline{\underline{U}} - \text{ by } -\underline{\underline{V}}.$$

Therefore,

$$\underline{\underline{U}}\,\underline{\underline{V}} \subseteq \underline{\underline{U}} - \text{ by } -\underline{\underline{V}}.$$

Combining this with the above reversed inclusion we get

$$\underline{\underline{U}}\,\underline{\underline{V}} = \underline{\underline{U}} - \text{ by } -\underline{\underline{V}}.$$

130 This proves that $\underline{\underline{U}} - by - \underline{\underline{V}}$ is a variety. In the case of varieties we shall use the simpler notation and write $\underline{\underline{U}}\,\underline{\underline{V}}$ instead of $\underline{\underline{U}}$ -by $-\underline{\underline{V}}$.

Theorem 4 (Hanna Neumann, 1956)**.** *The multiplication of varieties is associative.*

Proof. Let $\underline{\underline{T}}, \underline{\underline{U}}, \underline{\underline{V}}$ be three varieties defined by the set of laws L, M and N respectively. The variety $\underline{\underline{T}}\,\underline{\underline{U}}$ is defined by all laws of the form

$$w(\underline{\mathrm{X}}) = t(\underline{\mathrm{u}}(\underline{\mathrm{X}})) = 1, \text{ where}$$
$$t(\underline{\mathrm{X}}) = 1 \text{ and } u(\underline{\mathrm{X}}) = 1$$

are laws in $\underline{\underline{T}}$ and $\underline{\underline{U}}$ respectively. Therefore the variety $(\underline{\underline{T}}\,\underline{\underline{U}})\underline{\underline{V}}$ is defined by all laws of the form

$$w(\underline{\mathrm{v}}(\underline{\mathrm{X}})) = t(\underline{\mathrm{u}}(\underline{\mathrm{v}}(\underline{\mathrm{X}}))) = 1, \text{ where}$$

$\underline{\mathrm{v}}(\underline{\mathrm{X}}) = 1$ are laws in $\underline{\underline{v}}$. Similarly one can see that the variety $\underline{\underline{T}}(\underline{\underline{U}}\,\underline{\underline{V}})$ is also defined by all laws of the form

$$t(\underline{\mathrm{u}}(\underline{\mathrm{v}}(\underline{\mathrm{X}}))) = 1.$$

This proves that

$$(\underline{\underline{T}}\,\underline{\underline{U}})\underline{\underline{v}} = \underline{\underline{T}}(\underline{\underline{U}}\,\underline{\underline{V}}).$$

□

The above theorem can also be proved in the following way. We first observe that if $\underline{\underline{U}}$ is any variety defined by a set of laws M, then 131

$$G \in \underline{\underline{U}}$$

if and only if

$$G_M = \{1\}.$$

Further if $\underline{\underline{V}}$ is any other variety defined by a set laws N, then

$$G \in \underline{\underline{U}}\,\underline{\underline{V}},$$

if and only if

$$(G_N)_M = 1.$$

For if, $G \in \underline{\underline{U}}\,\underline{\underline{V}}$, then $G_N \in \underline{\underline{U}}$. Hence

$$G \in (\underline{\underline{T}}\,\underline{\underline{U}})\underline{\underline{V}}$$

if and only if

$$((G_N)_M)_L = 1.$$

Let the variety $\underline{\underline{U}}\,\underline{\underline{V}}$ be defined by P. Then $G \in T(\underline{\underline{U}}\,\underline{\underline{V}})$ if and only if

$$(G_P)_L = 1.$$

To prove the theorem we have only to prove that

$$G_P = (G_N)_M.$$

It is easy to verify that G_P is the least normal subgroup of G such 132
that $G/G_P \in \underline{\underline{U}}\,\underline{\underline{V}}$. Now,

$$((G/(G_N)_M)_N)_M = (G_N)_M/(G_N)_M = \{1\};$$

that is to say

$$G/(G_N)_M \in \underline{\underline{U}}\,\underline{\underline{V}}.$$

Further if S is any normal subgroup of G such that

$$G/S \in \underline{\underline{U}}\,\underline{\underline{V}}, \text{ then}$$

$$((G/S)_N)_M = \{1\}; \text{that is}$$

$$(G_N)_M \leq S.$$

Thus $(G_N)_M$ is the unique minimal normal subgroup of G such that

$$(G_N)_M \in \underline{\underline{U}}\,\underline{\underline{V}}.$$

Therefore

$$G_P = (G_N)_M.$$

This proves the theorem.

The associative law does not hold for arbitrary classes of groups; in
133 other words if $\underline{\underline{C}}, \underline{\underline{D}}, \underline{\underline{E}}$ are three classes of groups, then in general

$$(\underline{\underline{C}} - \text{ by } - \underline{\underline{D}}) - \text{ by } \underline{\underline{E}} \neq \underline{\underline{C}} - \text{ by } (\underline{\underline{D}} - \text{ by } - \underline{\underline{E}}).$$

Consider the following example. Let $\underline{\underline{C}}$ be the class of all cyclic groups. Consider the normal series of A_4,

$$\begin{aligned}
&\{1\} \triangle C \triangle B \triangle A_4, \text{ where}\\
&B = \{1, (12)(34), (13)(24), (14)(23)\},\\
&C = \{1, (12)(34)\}.
\end{aligned}$$

The groups $A_4/B, B/C$ and C are cyclic groups; that is $A_4/B \in \underline{\underline{C}}$ and

$$B \in \underline{\underline{C}} - by - \underline{\underline{C}}; \text{ thus}$$

$$A_4 \in (\underline{\underline{C}} - by - \underline{\underline{C}}) - by - \underline{\underline{C}}.$$

But, $A_4 \notin \underline{\underline{C}} -$ by $-(\underline{\underline{C}} - by - \underline{\underline{C}})$, as A_4 does not contain any cyclic normal subgroup.

Let $\underline{\underline{U}}$ be variety. We define $\underline{\underline{U}}^1 = \underline{\underline{U}}, \underline{\underline{U}}^{n+1} = \underline{\underline{U}}^n\underline{\underline{U}} = \underline{\underline{U}}U^n$. As the multiplication of varieties is associative, $\underline{\underline{U}}^n$ is uniquely determined.

Let $\underline{\underline{A}}$ be the variety of all abelian groups. We call the variety $\underline{\underline{A}}^n$ the variety of *soluble groups* of length n. A group G is *soluble* if it is in $\underline{\underline{A}}^n$ for some n. It is immediate that

$$\underline{\underline{A}}^1 \subseteq \underline{\underline{A}}^2 \subseteq \underline{\underline{A}}^3 \subseteq \ldots,$$

It is easy to verify that this definition is equivalent to the following **134**
more usual definition which can be found in most text books on group theory.

A group G is soluble if there exits a "normal series".

$$\{1\} = H_0 \triangle H_1 \triangle H_2 \triangle \cdots \triangle H_n = G$$

with H_{i+1}/H_i abelian, for $n = 0, 1, \ldots, n-1$. When G is finite and soluble, then G has a series with the corresponding factor groups cyclic. A (not necessarily finite) group G is said to be *polycyclic* if it has a normal series with the corresponding factor groups cyclic. Thus every finite soluble group is a polycyclic group. Polycyclic groups were first studied by Hirsch who called them S-groups. The term "polycyclic " is due to P. Hall who introduced it as a part of a systematic terminology.

The class of all soluble groups do not form a variety. One can prove that for every integer n, there is a $G_n \in \underline{\underline{A}}^n, G_n \notin \underline{\underline{A}}^{n-1}$. Consider the cartesian product P of $G_n, n = 1, 2 \ldots$. If P were soluble, then $P \in \underline{\underline{A}}^m$, for some m. Therefore every G_n, being an epimorphic image of a subgroup of P is in $\underline{\underline{A}}^m$. This is absurd. Thus, the class of all soluble groups is not closed under the operation of taking cartesian products and therefore does not from a variety.

We have already remarked in Chapter 1 that the class of all fields
does not form a variety. To see this, it suffices to observe that the class of **135**

fields is not closed under the operation of forming cartesian products: in fact one easily sees that the direct product of two fields contains proper zero-divisions and thus cannot be a field.

Chapter 8

An Embedding Theorem

1

The group theoretical constructions which we have discussed in Chapter **136**
6 will be used to prove the following embedding theorem.

Theorem 1 (Higman,Neumann and Neumann)**.** *Every countable group G can be embedding in a 2-generator group H.*

Proof. Let

$$G = gp(a_1, a_2, \dots)$$

be a group generated by $\{a_i\}_{i\varepsilon I}$ where I is countable; and let C be an infinite cyclic group generated by an element c,thus

$$C = gp(c).$$

[Later we shall modify this by choosing C is a finite cyclic group provided that certain conditions are satisfied; cf p.146.] □

We form the wreath product of the groups G and C,

$$P = GWrC.$$

Every element of P is of the form $c^s f$ where f is a function on C
with values in G and the product of any two elements $c^s f$ and $c^t g$ of P **137**
is given by

$$(c^s f)(c^s g) = c^{s+t} f^{c^t} g, \quad \text{where} \quad f, g \in G^C, \quad \text{and}$$
$$f^{c^t}(c^n) = f(c^{n-t}), \quad \text{for} \quad n = 0, \pm 1, \pm 2, \ldots$$

In the group P (and in fact in G^C) we single out certain elements $g_i, i \in I$, defined by

$$g_i(c^j) = g_i^{-j}, i \in I, j = 0, \pm 1, \pm 2, \ldots$$

We now compute the elements $k_i, i \in I$, where

$$k_i = [g_i, c].$$

As
$$k_i = g_i^{-1} c^{-1} g_i c = g_i^{-1} g_i^c,$$
we see that $k_i \in G^C$; and

$$\begin{aligned} k_i(c^j) &= g_i^{-1} g_i^c(c^j) = g_i^{-1}(c^j) g_i^c(c^j) \\ &= g_i^{-1}(c^j) g_i(c^{j-1}) = a_i^j a_i^{-(j-1)} = a_i. \end{aligned}$$

Thus k_i are constant functions taking the value a_i for all c_s^j. The constant functions clearly form a group $G^\triangle$ and this is isomorphic to G. We call $G^\triangle$ the diagonal subgroup of G^C. [The diagonal can be defined
138 in arbitrary cartesian powers, not only of groups.] It is not difficult to see that all constant functions are generated by those among them whose values are the generators a_i of G, thus

$$gp(\{k_i\}_{i \in I}) = G.$$

Note also that we have embedded G in the commutator subgroup of P.

Now let B be a cyclic group generated by an element b and let B be "big enough" to contain $b_i \in B, i \in I$, satisfying the following conditions

$$b_i \neq 1, b_i \neq b_j \text{ for } i \neq j$$

and $1 \neq b_i b_j, b_i b_j \neq b_k$, for all $i, j, k \in I$. This we can achieve by taking B to be infinite cyclic group

$$B = gp(b), \text{ if } |I| = \mathscr{N}_0 :$$

and if $|I| = g < \mathscr{N}_o$, we can either take B to be the infinite cyclic group or

$$B = gp(b; b^m = 1), m = 3d \text{ or } m \geq 4d - 1.$$

When B is the infinite cyclic group or $m = 3d$, we choose for instance

$$b_i = b^{3i-1}, i \in I.$$

If $m \geq 4d - 1$, we choose

$$b_i = b^{2i-1}, i \in I.$$

It is easy to verify that $b_i, i \in I$ satisfy the above conditions. We now **139**
form the wreath product of P and B. Let

$$Q = PWrB.$$

Define $q \in Q$ (in fact $q \in P^B$) by

$$q(1) = c$$
$$g(b_i^{-1}) = g_i, i \in I,$$

and $q(y) = 1$, for $y \neq 1, b_i^{-1}, i \in I$. Define further

$$h_i[q^{b_i}, q] \in P^B \leq Q, \text{ for } i \in I.$$

We now compute h_i

$$\begin{aligned} h_i(1) &= [q^{b_i}, q](1) = [q^{b_i}(1), q(1)] \\ &= [q(b_i^{-1}), q(1)] = [g_i, c] = k_i; \\ \text{next} \qquad h_i(b_j^{-1}) &= [q^{b_i}, q](b_j^{-1}) = [q^{b_i}(b_j^{-1}), q(b_j^{-1})] \\ &= [g(b_j^{-1} b_i^{-1}), q(b_j^{-1})]. \end{aligned}$$

Now, we have chosen b_i, such that

$$1 \neq b_i b_j, b_i b_j \neq b_k, \text{ for } i, j, k \in I.$$

Therefore we have **140**

$$h_i(b_j^{-1}) = [q(b_j^{-1}b_i^{-1}), q(b_j^{-1})] = [1, g_j^{-1}] = 1,\ j \in I.$$

Finally

$$h_i(y) = [q^{b_i}(g), q(y)] = [q^{b_i}(y), 1] = 1,\ \text{for } y \neq 1, b_j^{-1},\ j \in I.$$

Thus

$$h_i(1) = k_i,$$
$$h_i(y) = 1, y \neq 1.$$

We denote the group generated by the h_i by G^*; it is then obvious that

$$G^* = gp(\{h_i\}_{i\in I}) \cong gp\{k_i\}_{i\in I} \cong G.$$

Further

$$G^* \leq gp(q, b) = H$$

This proves the theorem.

This theorem was first proved (Higman, Neumann, Neumann, 1949) using quite different methods. The proof (Neumann and Neumann, 1959) which we have given here provides answer to a number of interesting questions of the form: if G has the property P, can H be chosen
141 to have the property P or some property closely related to P?

2 Corollaries

2.1 If $G \in \underline{\underline{V}}$, a variety, then $H \in \underline{\underline{V}}\,\underline{\underline{A}}^2$. For $G^C \in \underline{\underline{V}}$ and $P = G\,Wr\,C \in \underline{\underline{V}}\,\underline{\underline{A}}$, and therefore,

$$Q = P\,Wr B \in \underline{\underline{V}}\,\underline{\underline{A}}^2$$

Since $H \leq Q$, we have

$$H \in \underline{\underline{V}}\,\underline{\underline{A}}^2.$$

In particular if $G \in \underline{\underline{A}}^{\ell}$, we get

$$H \in \underline{\underline{A}}^{\ell+2};\ \text{thus we have}$$

2.2 A countable group which is soluble of length $\leq \ell$ can be embedded in a 2-generator group, soluble of length $\ell + 2$.

This is the best possible result in the sense that we can make examples of groups that are countable and soluble of length $\leq \ell$ and which cannot be embedded in any finitely generated soluble group of length $\ell + 1$.

We shall have give an example with $\ell = 1$; that is, we shall give an example of a countable abelian group which cannot be embedded in any finitely generated metablian group. In this context, we need a theorem which we state here without proof Theorem (P. Hall, 1954[b]). A finitely generated metabelian group satisfies the maximal condition for normal subgroups.

Consider the group G with a countable set of generators $a_1, a_2, \ldots$ **142**
presented by

$$G = gp(a_1, a_2, \ldots; a_1^p = 1, a_2^p = a_1, \ldots, a_{i+1}^0 = a_i, \ldots),$$

where p is a prime. It is easy to verify that G is isomorphic to the group of all p^n th roots of unity for $n = 1, 2, \ldots$. The group G is known as "Prufer p^∞ - group" or quasi-cyclic group. This group has many interesting properties. For instance all proper subgroups of G are finite cyclic groups. For if $H \neq 1$ is a proper subgroup of G, then

$$H = gp(a_n),$$

where n is the least positive integer such that $a_{n+1} \notin H$. It is easy to verify that

$$G/H \cong G.$$

Thus all the factor groups of G are either isomorphic to G or the trivial group.

We shall now show that G cannot be embedded in a finitely generated metabelian group.

Assume G to be embedded in a metabelian group K. We shall identify the isomorphic of G in K with G and take $G \leq K$. Consider the **143**
canonical mapping φ of K onto K/K' where K' is the derived subgroup of K. Since all the factor groups of G are either isomorphic to G or the

trivial group, the image G_1 of G under φ is either group or is isomorphic to G.

Now if $G_1 \cong G$, then G_1 is not finitely generated. But we know that every subgroup of a finitely generated abelian group is finitely generated. (See Kurosh, 1955§20, p.149) Therefore, K/K' and hence K is not finitely generated.

On the other hand, if G is the trivial group, then

$$G \leq K'.$$

Let G^K be the normal closure of G in K. Then

$$G^K \leq K'.$$

Define $A_n \leq G^K$ by

$$A_n \left\{ g \middle| g \in G^K, g^{p^n} = 1 \right\}.$$

Since K is merabelian, K' is abelian. Therefore A_n is a group, for every n. We claim that A_n are invariant in G^K. For, let η be an endomorphism of G^K, then $(g^\eta)^{p^n} = (g^{p^n})^\eta = 1^\eta = 1$, for all $g \in A_n$; that

$$A_n^\eta \leq A_n.$$

144 Therefore A_n are fully invariant and thus, a fortiori, characteristic in G^K. But

$$G^K \triangle K(\text{ trivially }).$$

Hence,

$$A_n \triangle K, \text{ for all } n.$$

Now we assert that

$$A_1 \leq A_2 \leq A_3 \cdots$$

is an infinite strictly ascending chain. For,

$$a_{n+1} \in A_{n+1} \text{ and } a_{n+1} \notin A_n.$$

Therefore by P. Hall's theorem K cannot be finitely generated. Thus G cannot embedded in any finitely generated metabelian group.

2.3 If G is abelian, in the proof of Theorem 1 we can take the group C to be of order 2. But in this case we define $g_i \in G^C$, $i \in I$, by

$$\begin{aligned} &g_i(1) = a_i \\ &g_i(c) = 1, \text{ where } C = gp(c; c^2 = 1). \end{aligned}$$

Then, 145

$$\begin{aligned} k_i = [g_i, c] &= g_i^{-1} g_i^c \in G^c, i \in I \text{ and} \\ k_i(1) &= g_i^{-1}(1) g_i^c(1) = a_i^{-1}, \\ k_i(c) &= g_i^{-1}(c) g_i^c(c) = a_i. \end{aligned}$$

It is easy to verify that when G is abelian the mapping φ of $\{a_i\}_{i\in I}$ into $P = G\,Wr\,C$ defined by

$$a_i^{\varphi} = k_i, i \in I$$

can be extended a monomorphism of G into P. Now one can proceed as in the proof of the Theorem 1.

If further, G is finitely generated, we have seen that B could be taken to be a finite group. We have

2.4 If $G \in \underline{\underline{A}}$ and finitely generated, then $H \in \underline{\underline{A}}^3$ can be chosen as an abelian-by-finite group.

Now,

$$G^C \Delta P; \quad \text{and}$$

hence
$$(G^C)^B \Delta P^B.$$

It is easy to verify that

$$P^B/(G^C)^B \cong (P/G^C)^B.$$

Now, since $|B| < \infty$ and $|P/G^C| < \infty$, we have 146

$$|P^B/(G^C)^B| < \infty.$$

Now for any $f \in (G^C)^B$, we have

$$b^{-1} f b = f^b (G^C)^B.$$

Therefore

$$(G^C)^B \Delta gp(P^B, b) = Q.$$

Further,

$$Q/P^B = \frac{Q/(G^C)^B}{P^B/(G^C)^B}$$

Since, $|Q/P^B| < \infty, |P^B/(G^C)^B| < \infty$, follows that

$$|Q/(G^C)^B| < \infty.$$

As G is abelian, the group Q is abelian- by - finite. It is not difficult to prove that the property of being abelian-by-finite is inherited by subgroups (and also by factor groups).

2.5 If $a_i^n = 1$, for all $i \in I$, in the embedding procedure of Theorem 1
147 we can take C be to be a cyclic group of order n. It is easy to verify that in this case the functions g_i are un ambiguously defined.

2.6 It G has finite exponent n and is finitely generated, say by d elements, then H can be chosen of finite exponent n^{2+r}, where r is an integer such that $m = n^r$ is a possible choice for the order of the group B occurring in the proof of the theorem; that is $m = 3d$ or $m \geq 4d - 1$.

Now,

$$P = G \, Wr \, C,$$

where C is a cyclic group of order n. Since G is a group of exponent n, so is G^C. Further

$$P/G^C \cong C.$$

If $x \in P$, then $x^n \in G^C$, and

$$(x^n)^n = x^{n^2} = 1;$$

that is P and therefore P^E is of exponent n^2. Again

$$Q/P^B \cong B,$$

where B has been chosen to be a finite cyclic group of order n^r.

Now if $y \in Q$, then $y^{n^r} \in P^B$, and therefore

$$(y^{nr})^{n^2} = y^{n^{2+r}} = 1,$$

that is Q, and hence $H \leq Q$ is of exponent n^{2+r}. **148**

From Corollary 6, we immediately get the following reduction theorems for the Burnside conjectures.

2.7 Reduction Theorem for the Full Burnside Conjecture All finitely generated groups of exponent n, are finite if all 2-generator groups of exponent n^s, for all s, are finite.

This "reduction theorem" was first proved by Sanov (1945). It has lost interest in view of Novikov's recent results.

2.8 Reduction Theorem for the Restricted Burnside Conjecture It there is a number $\beta(n^k, 2)$ such that every finite 2−generator group of exponent n^k has order $\leq \beta(n^k, 2)$, then there is a number $\beta(n, d)$ such that every finite d-generator group with $d \leq \dfrac{1}{4}(n^{k-2} + 1)$ and of exponent n has order $\leq \beta(n, d)$. In fact,

$$\beta(n, d) \leq \beta(n^k, 2).$$

Chapter 9

Generalised Free Products of Groups with Amalgamations

1

In this chapter we shall consider the question under what conditions a **149**
given family of groups with prescribed intersections can be embedded in a group. More precisely the problem is the following.

Let $\{G_i\}_{i\in I}$ be a family of groups and $\{H_{ij}\}_{i\in I}$ be a given family of subgroups of G_i, for every $i \in I$. We then ask: does there exist a group P and monomorphism θ_i of G_i into P for every $i \in I$ with the property

$$G_i^{\theta_i} \cap G_j^{\theta_j} = H_{ij}^{\theta_i} = H_{ji}^{\theta_j}, \text{ for all } i, j \in I?$$

Certain conditions are necessary for the existence of such a group.

First we note that

$$H_{ii} = G_i.$$

Since H_{ij} and H_{ji} are to be mapped onto the same subgroup of P, they must be isomorphic. In fact φ_{ij}, the restriction of $\theta_i\theta_j^{-1}$ to H_{ij}, must be an isomorphism of H_{ij} onto H_{ji}. It is immediate that

$$\varphi_{ij}\varphi_{ji} = \ell,$$

the identity map of H_{ij} onto itself. Further, **150**

$$G_i^{\theta_i} \cap G_j^{\theta_j} \cap G_k^{\theta_k} = H_{ij}^{\theta_i} \cap H_{ik}^{\theta_i} = H_{ji}^{\theta_i} \cap H_{jk}^{\theta_j} = H_{ki}^{\theta_k} \cap H_{kj}^{\theta_k}.$$

Thus the three intersections,

$$H_{ij} \cap H_{ik}, H_{ji} \cap H_{jk}, H_{ki} \cap H_{kj}$$

must be mapped onto one and the same subgroup

$$G_i^{\theta_i} \cap G_j^{\theta_j} \cap G_k^{\theta_k}.$$

Now

$$\begin{aligned}(H_{ij} \cap H_{ik})^{\varphi_{ij}} = (H_{ij} \cap H_{ik})^{\theta_i\theta_j^{-1}} &= (H_{ij}^{\theta_i} \cap H_{ik}^{\theta_i})^{\theta_j^{-1}} \\ &= \left(H^{\theta^{\theta_j}_{ji}} \cap H^{\theta^{-1}_{jk}}\right)^{\theta_j^{-1}} = H_{ji} \cap H_{jk}.\end{aligned}$$

The mapping $\varphi_{ij}\varphi_{jk}$ is an isomorphism of $H_{ij} \cap H_{ik}$ onto $H_{ij} \cap H_{ik}$; in fact

$$\varphi_{ij}\varphi_{jk} = \varphi_{ik} \text{ on } H_{ij} \cap H_{ik}.$$

We can similarly write down further necessary conditions which
arise from the fact that the the intersection of more than three groups
151 H_{ij}, H_{ik}, ... are to be mapped onto one and the same intersection of
groups $G_i^{\theta_i}, G_j^{\theta_j}, \ldots$. But once the necessary conditions in terms of the intersection of three groups are satisfied other such conditions involving more than three groups are automatically satisfied. For instance, say four groups G_i, G_j, G_k, G_ℓ. Then

$$\begin{aligned}(H_{ij} \cap H_{ik} \cap H_{i\ell})^{\theta_i} &= H_{ij}^{\theta_i} \cap H_{ik}^{\theta_i} \cap H_{i\ell}^{\theta_i} \\ &= (H_{ij}^{\theta_i} \cap H_{ik}^{\theta_i}) \cap (H_{ij}^{\theta_i} \cap H_{i\ell}^{\theta_i}) \\ &= (H_{ji}^{\theta_i} \cap H_{jk}^{\theta_j})(H_{ji}^{\theta_j} \cap H_{i\ell}^{\theta_j}) \\ &= H_{ji}^{\theta_i} \cap H_{jk}^{\theta_j} \cap H_{j\ell}^{\theta_j}, \text{ and so on .}\end{aligned}$$

It is easy to verify that

$$\varphi_{ij}\varphi_{ik}\varphi_{k\ell} = \varphi_{i\ell} \text{ on } H_{ij} \cap H_{ik} \cap H_{i\ell}.$$

Thus we have proved

Theorem 1. *In order that $\{G_i\}_{i\in I}$ be embeddable in a group with prescribed intersections $\{H_{ij}\}_{(i,j)\in I\times I}$ it is necessary that there be isomorphisms φ_{ij} of H_{ij} onto H_{ji} satisfying the following conditions.*

(1) $\varphi_{ij}\varphi_{ji} = \ell$, the identity map of H_{ij} onto itself **152**

(2) φ_{ij} maps $H_{ij} \cap H_{ik}$ onto $H_{ji} \cap H_{jk}$

(3) $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ on $H_{ij} \cap H_{ik}$, for all $i, j, k \in I$.

Here after we shall refer to the family of subgroups $\{H_{ij}\}_{(i,j)\in I\times I}$ satisfying the necessary conditions of Theorem 1 as the family of *amalgamated subgroups*.

Let $\{G_i\}_{i\in I}$ be a family of groups with amalgamated subgroups $\{H_{ij}\}_{(i,j)I\times I}$ and et

$$G_i = gp(E_i; R_i)$$

be a presentation of G_i with generators E_i and a set of defining relations R_i. Let

$$\begin{aligned} H_{ij} &= gp(D_{ij}), \text{ where} \\ H_{ij} &= \{d_{ij\nu}\}, \end{aligned}$$

ν running over some index set. Since H_{ij} and H_{ji} are isomorphic, we can choose generators D_{ij} in such a way that

$$\begin{aligned} D_{ij}^{\varphi_{ij}} &= D_{ji} \text{ and} \\ d_{ij\nu}^{\varphi_{ij}} &= d_{i\nu}. \end{aligned}$$

Thus ν runs over one and the same index set for D_{ij} and D_{ij}. Without **153**
loss of generality we can take

$$\bigcup_j D_{ij} \subseteq E_i.$$

Now for every $i \in I$, we take a set E_i^* with $|E_i| = |E_i^*|$; that is there is a $1-1$ and onto map θ_i^* of E_i onto E_i^*. Let R_i^* be the set of all relations defined by

$$R_i^* = \left\{ r\left(e_1^{\theta_i^*}, \ldots, e_n^{\theta_i^*}\right) = 1 \middle| (r(e_1, \ldots, e_n) = 1) \in R_i, e_1, \ldots, e_n \in E_1 \right\}$$

Let

$$P^* = gp\left(\bigcup_{i\in I} E_i^{\theta_i^*}; \bigcup_{i\in I} R_i^*, d_{ij\nu}^{\theta_i^*} = d_{ij\nu}^{\theta_i^*}, \text{ for all } i, j, \nu\right)$$

We shall refer to the collection $\{G_i\}_{i\in I}$ with amalgamated subgroups $\{H_{ij} \in \}_{(i,j)I\times I}$ as an *amalgam* . If there exists a group P embedding the family $\{G_i\}_{i\in I}$ with amalgamated $\{H_{ij} \in \}_{(i,j)I\times I}$, we say that "$P$ embeds the amalgam".

Theorem 2. *If there exists a group P embedding the amalgam, then the group P^* also embeds the amalgam and if θ_i is the corresponding canonical monomorphism of G_i into P, then there is a homomorphism φ of P^* into P, mapping*

$$G_i^* = gp(E_i^{\theta_i^*}) \leq P^*$$

154 *isomorphically onto $G_i^{\theta_i^*}$ such that*

$$(G_i^* \cap G_j^*)^{\varphi} = G_i^{\theta_i} \cap G_j^{\theta_j} = H_{ij}^{\theta_i} = H_{ji}^{\theta_j}.$$

Proof. Define the mapping φ of $\bigcup_{i\in I} E_i^{\theta_i^*}$ into P by

$$(e_i^{\theta_i^*})^{\varphi} = e_i^{\theta_i}, \text{ for } e_i \in R_i \text{ and}$$

where θ_i is the embedding monomorphism of G_i into P. We claim that φ can be extended to a homomorphism of P^* into P. □

For let

$$r_1(e_{i_1}^{\theta_i^*}, \ldots, e_{i_n}^{\theta_i^*}) = 1 \text{ we a relation in } R_i^*.$$

Then

$$\left(r_i\left(e_{i_1}^{\theta_i^*}, \ldots, e_{i_n}^{\theta_i^*}\right)\right) = r_i\left(e_{i_1}^{\theta_i^*\varphi}, \ldots, e_{i_n}^{\theta^*i\varphi}\right) = r_i\left(e_{i_1}^{\theta_i}, \ldots, e_{i_n}^{\theta_i}\right) = 1,$$

since
$$r_1(e_{i_1}, \ldots, e_{in}) = 1$$

is a relation in R_i and θ_i is a monomorphism of G_i into P.

155 Further,

$$d_{ij\nu}^{\theta_i^*} = d_{ij\nu}^{\theta_j^*} \text{ implies}$$
$$d_{ij\nu}^{\theta_i} = d_{ij\nu}^{\theta_j}.$$

For, $$d_{ij\nu}^{\varphi_{ij}} = d_{ij\nu}^{\theta_i\theta_j^{-1}} = d_{ji\nu}.$$

Thus the defining relations of P^* go over to relations of P upon applying φ and therefore φ can be extended to a homomorphism of P^* into P, by von Dyck's Theorem. We shall denote this homomorphism also by φ. Again an application of von Dyck's theorem shows that θ_i^*, the mapping of E_i into P^*, can be extended to a homomorphism of G_i into P^*, which we also denote by θ_i^*. It is obvious that

$$G_i^{\theta_i^*} = G_i^*.$$

We claim that (since P embeds the amalgam) θ_i^* is a monomorphism of G_i into P^*. By the definition of

$$\theta_i^*\varphi = \theta_i \text{ on } G_i.$$

Therefore the kernel of θ_i^* is contained in that of θ_i. But θ_i, being a monomorphism has trivial kernel. Therefore θ_i^* has a trivial kernel; **156**
that is θ_i^* is a monomorphism of G_i into P^*. To show P^* embeds the amalgam we have only to prove that

$$G_i^{\theta_i^*} \cap G_j^{\theta_j^*} = H_{ij}^{\theta_i^*} = H_{ji}^{\theta_j^*}, i, j \in I.$$

Now,

$$\begin{aligned} H_{ij}^{\theta_i^*} &= \left(gp(\{d_{ij\nu}\})\right)^{\theta_i^*} = gp\left(\{d_{ij\nu}^{\theta_i^*}\}\right) \\ &= gp\left(\{d_{ji\nu}^{\theta_j^*}\}\right) = \left(gp(\{d_{ij\nu}\})\right)^{\theta_j^*} = H_{ji}^{\theta_j^*}; \text{ and} \\ H_{ij}^{\theta_i^*} &= H_{ji}^{\theta_j^*} \subseteq G_i^{\theta_j^*} \cap G_j^{\theta_j^*}. \end{aligned}$$

Let $h^* \in G_i^{\theta_i^*} \cap G_j^{\theta_j^*}$. Then,

$$h^{*\varphi} \in (G_i^{\theta_i^*} \cap G_i^{\theta_j^*})^{\varphi} \subseteq G_i^{\theta_i^*\varphi} \cap G_j^{\theta_j^*\varphi} = G_i^{\theta^i} \cap G_j^{\theta_j}.$$

Now P embeds the amalgam. Hence

$$h^{*\varphi} \in G_i^{\theta_i} \cap G_j^{\theta_j} = H_{ij}^{\theta_i} = H_{ji}^{\theta_j}$$

Therefore there is a unique $h \in H_{ij}$ such that

$$h^{*\varphi} = h^{\theta_i} \in H_{ij}^{\theta_i}.$$

157 Now θ_i^* is an isomorphism of G_i onto G_i^*. Therefore

$$h^{*\theta_i{}^{*-1}} = h; \text{ that is}$$
$$h^{\theta_i^*} \in H_{ij}^{\theta_i^*}; \text{ that is to say}$$
$$G_i^{\theta_i^*} \cap G_j^{\theta_j^*} \subseteq H_{ij}^{\theta_i^*}$$

Combining this with the reversed inclusion which we have already proved we have

$$G_i^{\theta_i^*} \cap G_j^{\theta_j^*} = H_{ij}^{\theta_i^*} = H_{ji}^{\theta_j^*}.$$

This proves that P^* embeds the amalgam. Further φ restricted to $G_i^{\theta_i^*}$ is precisely the mapping $\theta_i^{*-1}\theta_i$ and hence is $1-1$; that is the mapping φ restricted to $G_i^{\theta_i^*}$ is a monomorphism.

We shall refer to P^* as the "canonic group" of the amalgam and θ_i^* as the "canonic homomorphism" of G_i into $P*$.

If P^* embeds the amalgam, we call P^* the *generalised free product* of the amalgam. The name " generalised free product" is justifiable as
158 there is a homomorphism of P^* into any group that embeds the amalgam.

2

If all the amalgamated subgroups H_{ij} are trivial, then the cartesian product of $\{G_i\}$ is one that embeds the amalgam. Therefore the corresponding P^* also embeds the amalgam; this is known as the *free product* of the family of groups $\{G_i\}$. Free products occur naturally in applications of group theory. For instance the free group

$$G = gp(E; \phi)$$

is the free product of infinite cyclic groups $\{gp(e_i)\}_{e_i \in E}$. Another example of a free product is the following. Consider the set M of all linear transformations of the form

$$z^{\varphi} = \frac{az+b}{cz+d} \text{ with } ad - bc = \pm 1, \text{ where}$$

a, b, c, d are rational integers. It is not difficult to verify that M is a group with composite of maps as the multiplication. The group M is known as the *modular group* . This group M is the free product of two cyclic groups of order 2 and 3 generated by α and β respectively where

$$z^{\alpha} = -\frac{1}{z}; \alpha^2 = \ell \text{ and}$$
$$z^{\beta} = -\frac{1}{z-1}; \beta^3 = \ell \text{ thus}$$
$$M = gp(\alpha, \beta; \alpha^2 = \beta^3 = 1).$$

(See Coxeter and Moser 1957$pp.85 - 88$; the group is there called **159**
the *projective* modular group in 2- dimensions.)

The generalised free products, too, appear naturally in topology. For instance the clover knot group (i.e. the fundamental group of the residual space in S^3 of the clover knot) is the generalised free product of two infinite cyclic groups say gp(a) and gp(b) with gp(a^2) and $gp(b^3)$ as the amalgamated subgroups. More generally any torus knot group is the generalised free product of two infinite cyclic groups gp(a) and ga(b) with gp(a^m) and $gp(a^n)$ amalgamated.

3

We can make examples of amalgams which cannot be embedded in any group. Consider the following amalgam.

Let,

$$G_1 = gp(g_1, h_1, k_1; h_1^2 = k_1^2 = 1, h_1, k_1 = 1, g_1^2 = 1, h_1^g = k_1).$$

This is known the "dihedral group" of order 8 and it is precisely the group of automorphisms of a square. (One can describe G_1 also as the wreath product of two cyclic groups of order 2). We select the alternating group A_4 as G_2, presented as follows.

$$G_2 = gp(g_1, h_2, k_2; g_2^3 = 1, h_2^{g_2} = k_2, k_2^{g_2} = h_2 k_2.$$

160 We take C_6, the cyclic group of order 6, as G_3 and give it rather an "unorthodox" presentation; that is

$$G_3 = gp(c, d; c^2 = d^3 = 1; [c, d] = 1)$$

The following we take as the amalgamated subgroups.

$$\begin{aligned} H_{12} &= gp(h_1, k_1) \leq G_1, & H_{21} &= gp(h_2, k_2) \leq G_2 \\ H_{13} &= gp(g_1) \leq G_1, & H_{31} &= gp(c) \leq G_3 \\ H_{23} &= gp(g_2) \leq G_2, & H_{32} &= gp(d) \leq G_3. \end{aligned}$$

The amalgamating isomorphisms φ_{ij} are to map h_1 on h_2, k_1 on k_2, g_1 on c, g_2 on d.

It this amalgam can be embedded in a group, then the canonic group P^* also embeds the amalgam. Now P^* is the group generated by

$$g_1, h_1, k_1, g_2, h_2, k_2, c, d$$

with defining relations consisting of the defining relations of G_1, G_2, G_3 and the following amalgamating relations.

$$h_1 = h_2, k_1 = k_2, g_1 = c, g_2 = d.$$

Now in P^*, we have,

$$\begin{aligned} h_1 &= h_1^{[c,d]} = h_1^{[g_1,g_2]} = h_1^{g^{-1}} g_2^{-1} g_1 g_2 = k_1^{g_1^{-1} g_1 g_2} = k_2^{g_1^{-1} g_1 g_2} \\ &= h_2^{g_1 g_2} = h_1^{g_1 g_2} = k_1^{g_2} = k_2^{g_2} = h_2 k_2 = h_1 k_2; \end{aligned}$$

161 that is

$$k_2 = 1 \text{ and therefore}$$
$$h_2 = 1.$$

Hence,

$$h_1 = h_2 = k_1 = k_2 = 1.$$

Thus,

$$P^* \cong C_0$$

and therefore cannot embed the amalgam ; that is to say the amalgam we have considered cannot be embedded in any group. Note that the amalgam satisfies the necessary conditions. Thus an amalgam is not always embeddable in a group.

4

We can impose certain conditions on the amalgam to make it embeddable in a group. A special case when all the amalgamate subgroups coincide with a single group was first studied by Schreier (1927).

Theorem 3 (Schreier, 1927)**.** *If all the amalgamated subgroups coincide* 162
(with a single group) then the amalgam is embeddable.

Before proceeding to prove the theorem we make a definition. Let G be any group and $H \leq G$. Then G can be written as the union of disjoint left cosets of H. We choose one representative for each of these left cosets. The set of all such representatives is called a *left transversal* of H in G. Similarly a right transversal of H in G can be defined. If S is a left transversal of H in G, then

$$G = SH, \text{ with the property}$$
$$S' \subseteq S, G = S'H \text{ implies } S' = S.$$

(We call $|S|$ the index of H in G; notation $|S| = |G : H|$). Every element $g \in G$ can be written as

$$g = sh, \text{ with } s \in S, h \in H.$$

Moreover, this representation is unique. For if

$$g = sh = s'h', s \neq s', s, s' \in S, h, h' \in H,$$

then

$$s^{-1}s' = hh'^{-1} \in H; \text{ that is}$$
$$sH = s'H; \text{ and therefore by our}$$

163 choice of S,

$$s = s', h = h'.$$

It is often convenient to choose the transversal in such a way that H is represented by 1.

We shall give two proofs of Theorem 3. The second proof will be given in the next chapter, and applied there to give further embedding theorems.

First proof of Theorem 3. Let $\{G_i\}_{i \in I}$ be a family of groups and let G_i contain an isomorphic copy of a given group H, for every $i \in I$. Without loss of generality we can think of all these isomorphic copies as identified with each other, i.e.,

$$H \leq G_i, i \in I.$$

We call the G_i the *constituents* of the amalgam. We choose a left transversal S_i of H in G_i, for each $i \in I$, and we here represent H always by 1; thus $1 \in S_i$, for all $i \in I$. Now we pick out certain words in the elements of G_i. We call

$$w = s_1 s_2 \ldots s_n h$$

a *normal word* if it satisfies the following three conditions:

1) Each $s_\nu, \nu = 1, \ldots, n$, is a representative $\neq 1$ belonging to one of the left transversals we have chosen, say $S_{i(\nu)}$;

164 2) $i(\nu) \neq i(\nu + 1)$, for $\nu = 1, \ldots, n$, in other words, no two consecutive s_ν appearing in w belong to the same set of representatives.

3) $h \in H$.

We call n the *length* of the normal word w and denote it by $\ell(w)$. In particular n may be zero also. In fact

$$\ell(w) = 0$$

if and only if $w \in H$. We denote by w_o the normal word consisting of the identity element alone. Let W be the set of all normal words. Consider the mapping $\rho(g)$ of W into W, for all $g \in \bigcup_i G_i$, defined as follows.

For $g \in G_k, k \in I$ and

$$w = s_1 s_2 \cdots s_n h \in W$$

we put

$$w^{\rho(g)} = w',$$

where w' is defined as follows.

(i) If $n > 0, i(n) = k$; that is s_n lies in the same group G_k as g, then $s_n hg$ is a certain element of G_k and are be uniquely written as

$$s_n hg = s'h', s' \in S_k, h' \in H.$$

We then put

$$w' = s_1 s_2 \cdots s_{n-1} s'h', \text{ if } s' \neq 1$$

and $$w' = s_1 s_2 \cdots s_{n-1} h', \text{ if } s' = 1.$$

(ii) If $n = 0$ or $n > o$ and $i(n) \neq k$; that is if $s_n \notin G_k$, we represent 165
$hg \in G_k$ as

$$hg = s'h', s' \in S_k, h' \in H$$

and write $$w' = s_1 s_2 \cdots s_n s'h', \text{ if } s' \neq 1;$$

and $$w' = s_1 s_2 \cdots s_n h' \text{ if } s' \neq 1.$$

Thus $w' = w^{\rho(g)}$ is defined for every $w \in W$ and it is easy to verify that w' is again a normal word. If g is contained in more than one constituents G_i, say $g \in G_j \cap G_k$, then $g \in H$ and we can define w' according to (i) or (ii). Now, if

$$s_n hg = s'h', \text{ then}$$

since $g \in H$,

$$s_n = s'$$

and
$$gh = h'.$$

166 Therefore according to (i), we have

$$w' = s_1 s_2 \cdots s_{n-1} s' h' = s_1 s_2 \cdots s_n hg.$$

On the other hand, computing w' according to (ii) we have, as

$$hg = h',$$
$$w' = s_1 s_2 \cdots s_n h' = s_1 s_2 \cdots s_n hg.$$

Thus we get the same w' whichever way we compute it.
We shall now show that

$$\rho(gg') = \rho(g)\rho(g'), \text{ for } g, g' \in G_k.$$

Put
$$w^{\rho(g)} = w', w'^{\rho(g')} = w'', w^{\rho(gg')} = w^*.$$

(1) If $n > 0, i(n) = k$; then

$$s_n hg = \in G_k.$$

We write

$$s_n hg = s' h', s' \in S_k, h' \in H \text{ and}$$
$$s' h' g' = s'' h'', s'' \in S_k, h'' \in H.$$

167 Now,

$$w'' = s_1 s_2 \cdots s_{n-1} s'' h'' \text{ if } s'' \neq 1$$

and
$$w'' = s_1 s_2 \cdots s_{n-1} h'' \text{ if } s'' = 1.$$

On the other hand let

$$s_n h(gg') = s^* h^*, s^* \in S_k, h^* \in H.$$

Then

$$w^* = s_1 s_2 \cdots s_{n-1} s^* h^* \text{ if } s^* \neq 1$$

and
$$w^* = s_1 s_2 \cdots s_{n-1} h^* \text{ if } s^* = 1.$$

But,
$$s_n h(gg') = (s_n hg)g' = s'h'g' = s''h''.$$

Therefore,

$$s^* = s'', h^* = h''; \text{ that is}$$
$$w'' = w^*.$$

Notice that it does not matter whether $s' = 1$ or not as $i(n-1) \neq k$ **168**
and in either case we have to consider $s'h'g'$ to compute w''.

(2) If $n = 0$ or if $n > 0, i(n) \neq k$, write

$$hg = s'h', s' \in S_k, h' \in H$$

and
$$s'h'g' = s''h'', s'' \in S_k, h'' \in H.$$

Then,

$$w'' = s_1 s_2 \cdots s_n s'' h'' \text{ if } s'' \neq 1$$

and
$$w'' = s_1 s_2 \cdots s_n h'' \text{ if } s'' = 1.$$

On the other hand if we put

$$h(gg') = s^* h^*, s^* \in S_k, h^* \in H,$$

we have
$$w^* = s_1 s_2 \cdots s_n s^* h^* \text{ if } s^* \neq 1$$

and
$$w^* = s_1 s_2 \cdots s_n h^* \text{ if } s^* = 1.$$

But, **169**
$$s^* h^* = h(gg') = (hg)g' = s'h'g' = s''h''.$$

Therefore

$$s^* = s'', h^* = h''; \text{ that is}$$
$$w^* = w'.$$

In this case also not does not matter whether $s' = 1$ or $s' \neq 1$.

Thus we proved that in both the cases

$$w^{\rho(gg')} = \left(w^{\rho(g)}\right)^{\rho(g')}$$

As this is true for all $w \in W$, we have

$$\rho(gg') = \rho(g)\rho(g').$$

Again, as this true for all $g, g' \in G_k$ we conclude that mapping ρ_k of G_k into the semigroup of the mappings of W into itself, defined by

$$g^{\rho_k} = \rho(g), \text{ for all } g \in G_k$$

is a homomorphism; and therefore the image $G_k^{\rho_k}$ is a group. Hence every $\rho(g), g \in G_k$ has a two sided inverse, that is $\rho(g)$ is a permutation
170 of W, for all $g \in G_k$. We claim that ρ is an isomorphism of G_k onto $G_k^{\rho_k}$. For, if

$$\rho(g) = L, g \in G_k, \text{ then}$$
$$w_o^{\rho(g)} = w_o$$

But,

$$w_o^{\rho(g)} = sh, \text{ where}$$
$$g = sh, s \in S_k, h \in H.$$

Therefore,

$$sh = 1; \qquad \text{that is}$$
$$s = 1, h = 1$$

i,e., $$g = 1.$$

Hence the kernel of ρ_k is trivial; that is to say, ρ_k is an isomorphism of G_k onto $G_k^{\rho_k}$. Let $\sum$ denote the group of permutations of W generated by the $G_i^{\rho i}, i \in I$; that is

$$\sum = gp(\left\{G_i^{\rho i}\right\}).$$

By what we have just proved all groups G_i are embedded in by the isomorphism ρ_i. Now let

$$g^{\rho_i} = g'^{\rho_k}, g \in G_i, g' \in G_i, g' \in G_k . i \neq k;$$

that is
$$\rho(g) = \rho(g').$$

Let 171

$$g = sh \text{ with } s \in S_i, h \in H, \text{ and}$$
$$g' = s'h' \text{ with } s' \in S_k, h' \in H.$$

Then,

$$w_o^{\rho(g)} = sh \text{ or } h, \text{ according as } s \neq 1 \text{ or } s = 1.$$

Similarly,

$$w_o^{\rho(g')} = s'h' \text{ or } h' \text{ according as } s' \neq 1 \text{ or } s' = 1.$$

But
$$w_o^{\rho(g)} = w_o^{\rho(g')}.$$

Therefore

$$s = s' = 1, h = h'; \text{ that is}$$
$$g = g' = h.$$

Hence
$$g^{\rho_i} = g'^{\rho_k} \in H^{\rho_i} = H^{\rho_k},$$

Thus, 172
$$G_k^{\rho_k} \cap G_i^{\rho_i} = H^{\rho_i} = H^{\rho_k}, \text{ for all } i, k \in I.$$

This proves that the group $\sum$ embeds the amalgam under consideration.

5

We shall now turn W into a group isomorphic to $\sum$ by defining a suitable multiplication in W, in fact $\sum$ will turn out to be the right-regular permutation representation of the group W, we are to define. Consider the mapping η of $\sum$ into W defined by

$$\sigma^{\eta} = w_o^{\sigma}, \text{ for every } \sigma \in \sum.$$

Let

$$w = s_1 s_2 \cdots s_n h$$

be any normal word in W. Put

$$\sigma = \rho_{(s_1)} \rho_{(s_2)} \cdots \rho_{(s_n)} \rho_{(h)}.$$

It is easy to verify that

$$w_o^{\sigma} = s_1 s_2 \cdots s_n \cap = w$$

Thus the mapping is 'onto' W. Now we shall show that η is $1-1$.

173 We shall first prove the following lemma.

Lemma 1. *Let*

$$\sigma = \rho_{(g_1)} \cdots \rho_{(g_m)} \in \sum, \text{ with } g_{\mu} G_{i(\mu)} (1 \leq \mu \leq m).$$

and $i(\mu) \neq i(\mu + 1)$. Then the length of the normal word w_o^{σ} is m if $m > 1$ and further

$$w_o^{\sigma} = s_1 s_2 \cdots s_m h \text{ with } s_{\mu} \in S_{i(\mu)}, 1 \leq \mu \leq m, h \in H.$$

If $m = 1$, then the length of w_o^{σ} is 0 or 1 according g_1 is in H or not.

Proof. The proof of the lemma will be by induction. For $m = 2$, we have

$$\sigma = \rho(g_1) \rho(g_2), g_1 \in G_{i(1)}, g_2 \in G_{i(2)}, i(1) \neq i(2).$$

Now,

$$w_o^{\rho(g_1)} = s_1 h_1 \text{ with } 1 \neq s_1 \in S_{i(1)}, h \in H$$

and $$g_1 = s_1 h_1;$$
and $$w_o^\sigma = (w_o^{\rho(g_1)})^{\rho(g_2)} = s_1 s_2 h_2, 1 \neq s_2 \in S_{i(2)}, h \in H$$
and $$h_1 g_2 = s_2 h_2.$$

□

Thus 174

$$\ell(w_o^\sigma) = 2.$$

Assume the lemma to be true for all or with $2 \leq r < m$. Let $m > 2$. Put

$$\hat{\sigma} = \rho(g_1)\rho(g_2)\cdots\rho(g_{m-1}).$$

Then by induction hypothesis

$$w_o^{\hat{\sigma}} = s_1 s_2 \cdots s_{m-1} h', s_\mu \in G_{i(\mu)}, 1 \leq \mu \leq m-1, h' \in H.$$

Now,

$$\begin{aligned} w_o^\sigma &= \left(w_o^{\hat{\sigma}}\right)^{\rho(g_m)} = (s_1 s_2 \cdots s_{m-1} h)^{\rho(g_m)} \\ &= s_1 s_2 \cdots s_{m-1} s_m h, \text{ where} \\ h' g_m &= s_m h, 1 \neq s_m \in S_{i(m)}, h \in H. \end{aligned}$$

This completes the induction and proves that

$$\ell(w_o^\sigma) = m \text{ if } m > 1.$$

If $m = 1$, then

$$\sigma = \rho(g_1).$$

It is obvious that $\ell(w_o) = 0$ or 1 according as g_1 is in H or not. 175

Now if,

$$w_o^\sigma = w_o^\sigma, \sigma, \sigma' \in \sum,$$

then

$$w_o^{\sigma\sigma'^{-1}} = w_o.$$

Choose m to be the least positive integer such that

$$\sigma\sigma'^{-1} = \rho(g_1)\cdots\rho(g_m), \text{ with } g_i i G_{i(\mu)}, 1 \leq \mu \leq m.$$

If $m > 1$, then $i(\mu) \neq i(\mu+1)$. For, otherwise $\sigma\sigma'^{-1}$ can be "shrunk" by amalgamating g_μ and $g_{\mu+1}$. Hence by the above lemma it follows that

$$\ell(w_o^{\sigma\sigma'^{-1}}) = m > 1.$$

Since

$$w_o^{\sigma\sigma'^{-1}} = w_o,$$

this is absurd.

Therefore, $m = 1$; thus let

$$\sigma\sigma'^{-1} = \rho(g_1), g_1 \in G_{i(1)}.$$

176 Then

$$w_o^{\sigma\sigma'^{-1}} = s_1 h_1, \text{ where}$$
$$g_1 = s_1 h_1 \text{ with } s_1 \in S_{i(1)}, h_1 \in H.$$

But

$$w_o^{\sigma\sigma'^{-1}} = w_o; \text{ and therefore}$$
$$s_1 = 1, h_1 = 1; \text{ that is}$$
$$g_1 = 1: \text{ that is to say}$$
$$\sigma\sigma'^{-1} = \rho(g_1) = L.$$

Hence

$$\sigma = \sigma'.$$

Thus the mapping η of $\sum$ onto W is $1-1$. We now put a group structure on W in the following way.

Define

$$wow' = w_o^{\sigma\sigma^{-1}}, \text{ where } w, w' \in W$$
$$\text{and} \qquad w_o^{\sigma} = w, w_o^{\sigma'} = w'.$$

One can easily verify that W is turned into a group with this multi-
177 plication and that the group $\sum$ is the right regular permutation representation of the group W. Further, W being isomorphic to $\sum$ also embeds

the amalgam. To return to our old notation, W will be renamed P. We shall identify the groups $G_k^{\rho_k \eta}$ with G_k. Under this identification,

$$G_k \leq P, \text{ for all } k \in I.$$

Further

$$G_i \cap G_j = H \text{ in } P.$$

Let

$$w = s_1 s_2 \cdots s_n h \in W, s_\mu \in S_{i(\mu)} 1 \leq \mu \leq n, h \in H.$$

It is easy to verify that

$$w = s_1 \circ s_2 \circ \cdots \circ s_n \circ h.$$

If

$$w' = s'_1 s'_2 \cdots s'_m h',$$

then in general the usual product of the words w and w' is not a normal word. If

$$\sigma = \rho(s_1)\rho(s_2)\cdots\rho(s_n)\rho(h) \text{ and}$$
$$\sigma' = \rho(s'_1)\rho(s'_2)\cdots\rho(s'_m)\rho(h'), \text{ then}$$
$$w_o w' = w_o^{\sigma\sigma'} = (s_1 s_2 \cdots s_n h)^{\sigma'} = w^{\sigma'}.$$

Now, 178

$$\sigma\sigma' = \rho(s_1)\cdots\rho(s_n)\rho(h)\rho(s'_1)\cdots\rho(s'_m)\rho(h').$$

If s_n and s'_1 do not be in the same constituent, then by our lemma

$$w_o^{\sigma\sigma'} = w_o^{\rho(s_1)\cdots\rho(s_n h)\rho(s'_1)\cdots\rho(s'_m h')}$$

is of length $n + m$ and

$$wow' = w_o^{\sigma\sigma'} = s_1 s_2 \cdots s_n s^{(1)} s^{(2)} \cdots s^{(m)} h^{(m)}$$

where

$$hs'_1 = s^{(1)} h^{(1)}$$

$$h^{(1)}s'_2 = s^{(2)}h^{(2)}$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$h^{(m-1)}s'_m = s^{(m)}h^{(m)}.$$

179 On the other hand if s'_1 and s_n are in the same constituent, we amalgamate $s_n h$ and s'_1 and write

$$s_n h s'_1 = s^{(1)}h^{(1)}$$

and proceed as in the above case.

We now proceed to show that $\sum$ is the generalised free product of the amalgam. Let

$$u(\underline{\rho(g)}) = L$$

be a relation in $\sum$; we show that it follows from the relations of the groups $\rho(G_i)$. We write the relation in the form

$$\rho(g_1)\rho(g_2)\cdots\rho(g_n) = L,$$

where $g_\nu G_{i(\nu)}, \nu = 1, \ldots, n$. [This can be done because $(\rho(g))^{-1} = \rho(g^{-1})$.] If $n = 1$, then we have $\rho(g_1) = L$, and we have seen already that this implies $g_1 = 1$, so the relation is trivial. Assume then that $n > 1$. We claim that there are two successive elements $g_\nu, g_{\nu+1}$ out of the same constituent, that is $i(\nu) = i(\nu + 1)$; for if not, then

$$\ell(w_o^{\rho(g_1)\rho(g_2)\cdots\rho(g_n)}) = n > 1,$$

by our lemma, and this contradicts the assumed relation. Now in $G_{i(\nu)}$, there is a product g^*, say of g_ν and $g_{\nu+1}$, so that

$$g_\nu g_{\nu+1} = g^*$$

180 is a relation in $G_{i(\nu)}$; thus also

$$\rho_{(g_\gamma)}\rho_{(g_{\gamma+1})} = \rho_{(g^*)}$$

is a relation in $\rho_{(G_{i(\nu)})}$, that is a consequence of the defining relations of $\rho_{(G_{i(\nu)})}$. By means of this relation we can now reduce the given relation to a shorter one,

$$\rho(g_1)\cdots\rho(g_{\gamma-1})\rho(g^*)\rho(g_{\nu+2})\cdots\rho(g_n) = \ell.$$

By an easy induction one deduces that the given relation follows from the defining relations of the constituent groups. This proves the theorem:

Theorem 4. *The group $\sum$ and hence P is the generalised free product of the family of groups $\{G_i\}_{i\in I}$ with all the amalgamating subgroups coinciding with H.*

We immediately have the following consequence:

Corollary. *The group $\sum$ (and hence P) does not depend upon the transversals S_i of H in G_i that have been chosen.*

Chapter 10

Permutational Products

1 Permutational products and Scbreier's Theorem

In this chapter we shall introduce another product called the "permutational product" of an amalgam. The permutational product of an amalgam will be used in giving an alternative proof of Schreier's Theorem. The embedding group we are going to construct will be in general different from the generalised product of the amalgam in question. Once we construct a group embedding the amalgam the existence of the generalised free product follows Theorem 2 of the preceding chapter. **181**

It the following we will be considering an amalgam of two groups. This is just for convenience. The same proof carries over the case of an amalgam of an arbitrary family of groups with a single amalgamated subgroup.

Let the amalgam consist of groups A, B with the amalgamated subgroup $H, H \leq A, H \leq B$. We choose arbitrary left transversals S, T of H in A and B respectively. Thus every $a \in A$ and $b \in B$ can be uniquely written as

$$a = sh,\ s \in S, h \in H$$
$$b = th_1,\ t \in T, h_1 \in H.$$

Consider the product set $K = S \times T \times H$. Our object is to realise the embedding group as a permutation group of the set K. For every $a \in A, b \in B$ we define mappings $\rho_{(a)}, \rho_{(b)}$ of K into K as follows. **182**

Let $k = (s, t, h) \in K$, $s \in S$, $t \in T$, $h \in H$. Then put

$$k^{\rho(a)} = k' = (s', t', h'),$$

where $$s'h' = s\,h\,a,$$
and $$t' = t.$$

Similarly we define

$$k^{\rho(b)} = k'' = (s'', t'', h''),$$

where $$s''h'' = t\,h\,b,$$
and $$s'' = s.$$

If $h^* \in H$, then $\rho_{(h^*)}$ can be defined in two ways, once considering it as an element of A and the other time considering it as an element of B. But,

$$s\,h\,h^* = s'\,h',$$

implies $$s = s', h' = hh^*.$$

183 Similarly

$$thh^* = t''\,h'',$$

implies $$t = t'', h'' = hh^*.$$

Therefore, whatever way we compute $k^{\rho(h^*)}$, we get

$$k^{\rho(h^*)} = (s, t, hh^*);$$

hence our definition of ρ is unambiguous. Also, $\rho(h^*)$ when applied to any $(s, t, h) \in K$ leaves s, t unaltered.

Conversely one can easily verify that if $\rho(x)$, $x \in A$ or B, does not alter s, t when applied to a triplet $(s, t, h) \in K$, then $x \in H$.

Now consider the mapping ρ_A of A into the semigroup of all mappings of K into itself defined by

$$a^{\rho_A} = \rho(a), \text{ for all } a \in A.$$

Let $a, a_1 \in A, (s,t,h) \in K$. We have,

$$(s,t,h)^{\rho(a)} = (s',t',h'),$$

with $$s'h' = s\,h\,a,$$

and $$t' = t;$$

and further $$(s',t',h')^{\rho(a_1)} = (s'',t'',h''),$$

where $$s''h'' = s'\,h'\,a_1,$$

and $$t'' = t'.$$

But 184

$$sh(aa_1) = (sha)a_i = s'h'a_i = s''h''.$$

Therefore,

$$(s,t,h)^{\rho(aa_1)} = (s'',t'',h'') = (s,t,h)^{\rho(a)\rho(a_1)}.$$

As this is true for all $(s,t,h) \in K$, we have

$$\rho(aa_1) = \rho(a)\rho(a_1).$$

Again as this is true for all $a, a_1, \in A$ it follows that the mapping ρ_A is a homomorphism. Therefore the homomorphic image $A^{\rho_A} = \rho(A)$ is a group. Hence every $\rho(a), a \in A$ has a two sided inverse; that is, $\rho(a)$ is a permutation group of K. Further if

$$\rho(a) = L, a \in A,$$

then for every $(s,t,h) \in K$, we have

$$(s,t,h)^{\rho(a)} = (s,t,h).$$

Therefore, 185

$$\text{sha} = \text{sh} \text{ ; that is}$$
$$a = 1$$

that is ρ_A is an isomorphism of A onto $A^{\rho_A} = \rho(A)$. Similarly the mapping ρ_B of B into the semigroup of all mapping of K into itself defined by

$$b^{\rho_B} = \rho_(b), \text{ for all } b \in B$$

is a monomorphism; that is B is isomorphic to $B^{\rho_B} = \rho(B)$. Denote by P the permutation group of K generated by $\rho(A)$ and $\rho_(B)$,

$$P = gp(\rho(A), \rho(B)).$$

It is evident that P contains isomorphic copies of A and B namely A^{ρ_A} and B^{ρ_B}. We claim that

$$A^{\rho_A} \cap B^{\rho_B} = H^{\rho_A} = H^{\rho_B}.$$

Let $$\rho_{(a)} = \rho_{(b)}, a \in A, b \in B.$$

186 Then $\rho_{(a)}$ fixes both s, t of any $(s, t, h) \in K$. Therefore,

$$a \in H.$$

Similarly,

$$b \in H.$$

Now, since ρ_A is an isomorphism and

$$\rho_{(a)} = \rho_{(b)},$$

it follows that

$$a = b \in H; \text{ thus}$$
$$A^{\rho_A} \cap B^{\rho_B} = H^{\rho_A} = H^{\rho_B}.$$

Hence P embeds the amalgam. This proves Schreier's Theorems. We call P a *permutational product* of the amalgam. This proof of Shchreier's theorem immediately leads us to the following corollary.

Corollary. *An amalgam of two finite groups is embeddable in a finite group.*

In this context we mention the following unsolved problem.

Unsolved problem. If an amalgam of $n(n > 2)$ finite groups embeddable in a group, is it embeddable in a finite group?

2

187 Now we shall consider amalgams of abelian groups. We ask the following question: If an amalgam of n abelian groups is embeddable in a group, is it embeddable in an abelian group ?

For $n = 2, 3, 4$, the answer to this question is 'yes'; for $n = 5$. 'no' (see Hanna Neumann, 1951 and B. H. Neumann and Hanna Neumann, 1953). For $n = 2$, we shall prove the assertion.

We shall start with a more general situation. Let A and B be any two groups and H, H_1 be isomorphic subgroups of A and B respectively, and let H, H_1 be contained in the centres of A and B,

$$H \leq \text{ centre } (A), H_1 \leq \text{ centre } (B).$$

Let θ be an isomorphism of H onto H_1. Consider the direct product $A \times B$ of A and B. We shall denote an arbitrary element of $A \times B$ by

$$a \times b, \text{ with } a \in A, b \in B.$$

Consider $N \subseteq A \times B$, defined by

$$N = \left\{ h^{-1} \times h_1 \middle| h_1 = h^{\theta} \right\}.$$

Now if $x = h^{-1} \times h_1, y = h'^{-1} \times h'_1 \in N$ with

$$\begin{aligned}
h_1 &= h^{\theta}, h'_1 = h'^{\theta}, \text{ then} \\
xy^{-1} &= (h^{-1} \times h_1)(h'^{-1} \times h_1)^{-1} = (h^{-1} \times h_1)(h' \times h_1'^{-1}) \\
&= h^{-1}h' \times h_1 h_1'^{-1} \\
&= (hh'^{-1})^{-1} (\text{ As } , h, h' \in \text{ centre } (A)) \\
&= (hh'^{-1})^{-1} \times h_1 h_1^{-1}.
\end{aligned}$$

But, 188

$$(hh'^{-1})^{\theta} = h^{\theta}(h^{\theta})^{-1} = h_1 h_1'^{-1}.$$

Therefore,

$$xy^{-1} \in N; \text{ that is}$$

$$N \leq A \times B.$$

It is easy to verify that

$$N \leq \text{ centre } (A \times B)$$

and therefore $$N \Delta A \times B.$$

Consider now the quotient group $A \times B/N$. We claim that the mapping π of A into $A \times B/N$ defined by

$$a^{\pi} = (a \times 1)N \in A \times B/N, a \in A.$$

189 is a monomorphism. That it is a homomorphism is easy to verify. Now if

$$a \times 1 \in N, \text{ then}$$
$$a \times 1 = h^{-1} \times h^{\theta}, \text{ for some } h \in H;$$

that is,

$$a = h^{-1}, 1 = h^{\theta}.$$

Since θ is an isomorphism,

$$1 = h^{\theta} \text{ implies } h = 1; \text{ that is}$$
$$a = h^{-1} = 1.$$

Hence π has a trivial kernel; that is π is a monomorphism. Similarly the mapping π_1 of B into $A \times B/N$ defined by

$$b^{\pi_1} = (1 \times b)N \in A \times B/N, b \in B$$

is a monomorphism. Thus the groups A and B are monomorphically embedded in $A \times B/N$. We assert that $A \times B/N$ embeds the amalgam in question. To see this we have only to prove

$$A^{\pi} \cap B^{\pi_1} = H^{\pi} = H_1^{\pi_1}.$$

Now for any $h \in H$, we have

$$(h \times 1)(1 \times h^{\theta})^{-1} = h \times (h^{\theta})^{-1} \in N: \text{ that is}$$

$$(h \times 1)N = (1 \times h^{\theta})N.$$

190 Making h run through all the elements of H, we get

$$H^{\pi} = H_1^{\pi}.$$

It is immediate that

$$H^{\pi} = H_1^{\pi_1} \subseteq A^{\pi} \cap B^{\pi_1}.$$

Conversely if $x \in A^{\pi} \cap B^{\pi_1}$, then

$$x = (a \times 1)N = (1 \times b)N \text{ for some } a \in A, b \in B.$$

This gives

$$a \times b^{-1} \in N;\ \text{that is}$$
$$a = h, b = h^{\theta} \text{ for some } h \in H;\ \text{that is}$$
$$x = (h \times 1)N \in H^{\pi} = H_1^{\pi_1}.$$

Hence

$$A^{\pi} \cap B^{\pi_1} \subseteq H^{\pi} = H_1^{\pi_1}.$$

Combining this with the above inclusion we have

$$A^{\pi} \cap B^{\pi_1} = H^{\pi} = H_1^{\pi_1}.$$

This proves that $A \times B/N$ embeds the amalgam. It is evident that 191

$$A \times B/N = A^{\pi} B^{\pi_1},$$

and every element of A^{π} commutes with every element of B^{π_1}. We call $A \times B/N$ a "generalised direct product" of the amalgam. [This is also called a "central product" by some authors.]

Let A and B any two groups each containing an isomorphic copy of a group H. Without loss of generality we can take $H \leq A, H \leq B$. Let A and B embedded monomorphically in a group G. We shall identify these monomorphic images with A and B respectively and take

$$A \leq G, B \leq G.$$

We call G a *generalised direct product* of the amalgam of A and B with the amalgamated subgroup H if

(i) $G = AB$

(ii) $A \cap B = H$

(iii) Every element of A commutes with every element of B

In particular when H is the trivial group we get the usual direct product. In order that a generalised direct product of the amalgam in question may exists necessary that

$$H \leq \text{ centre } (A), H \leq \text{ centre } (B).$$

192 This is immediate from (iii). We have also proved that the condition is sufficient.

Let G be a generalised direct product of the amalgam consisting of groups A and B with an amalgamated subgroup H. Consider the mapping φ of $A \times B/N$ onto G defined by

$$((a \times b)N)^{\varphi} = ab \quad G.$$

Once can easily verify that φ is an isomorphism. In other word, the generalised direct product of an amalgam in unique upto an isomorphism. Thus we can speak of *the* generalised direct product of an amalgam. In contract to this, the permutational product of an amalgam is in general not unique. We shall soon make an example. We summarise the results proved above in the following;

Theorem 1. *The generalised direct product of an amalgam consisting of groups A and B with an amalgamated subgroup H exists if and only if*

$$H \leq \textit{ centre } (A), H \leq \textit{ centre } (B);$$

and it is unique to an isomorphism.

Taking A and B to be abelian groups we have,

Corollary. *An amalgam of two abelian groups is embeddable in an abelian group;*

3

193 Consider again the amalgam of two groups A and B with an amalgamated subgroup H with, $H \leq$ centre $(A), H \leq$ centre (B). As before, we choose transversals S, T of H in A and B respectively and form permutational product P on the set $K = S \times T \times H$. We show now that in this case every $\rho(a)\rho(A)$ commutes with every element $\rho(b) \in \rho(B)$. Let $(s, t, h) \in K$, $\rho(a) \in \rho(A), \rho(b) \in (B)$. Then,

$$
\begin{aligned}
(s, t, h)^{\rho(a)} &= (s_1, t_1, h_1), \quad \text{with} \\
s_1 h_1 &= sha, t = t_1; \\
(s_1, t_1, h_1)^{\rho(b)} &= (s_2, t_2, h_2), \quad \text{with} \\
t_2 h_2 &= t_1 h_1 b, s_2 = s_1
\end{aligned}
$$

Now from the above equations it follows that

$$thb = th(h_1^{-1} t_1^{-1} t_2 h_2) = t_1 h(h_1^{-1} t_1^{-1} t_2 h_2).$$

But $H \leq$ centre (B). Therefore,

$$thb = t_2 t_1 t_1^{-1} h h_1^{-1} h_2 = h_2 h h_1^{-1} h_2.$$

Hence we have, 194

$$(s, t, h)^{\rho(b)} = (s, t_2, hh_1^{-1} h_2)$$

Again from the above equations and since $H \leq$ centre (A), we have

$$s(hh_1^{-1} h_2)a = (sha)h_1^{-1} h_2 = (s_1 h_1) = s_1 h_2 = s_2 h_2.$$

Therefore

$$
\begin{aligned}
(s, t, g)^{\rho(b)\rho(a)} &= (s, t_2, hh_1^{-1} h_2)^{\rho(a)} = (s_2, t_2, h_2); \\
&= (s, t, h)^{\rho(a)\rho(b)}.
\end{aligned}
$$

As this is true for all $(s, t, h) \in K$, we get

$$\rho(a)\rho(b) = \rho(b)\rho(a).$$

This is true for all $a \in A, b \in B$. Since

$$P = gp(\rho(A), \rho(B))$$

embeds the amalgam, we have proved that P is the generalised direct product of the amalgam. Thus we have:

195 **Theorem 2.** *If H is central in both A and B, then the permutational product of the amalgam is the generalised direct product.*

The uniqueness of the generalised product gives:

Corollary. *Under the assumptions of the above theorem the permutational product does not depend upon the transversals chosen.*

Incidentally, not that in this case the permutational product is not the generalised free product. For in the generalised free product $a \in A - H$ and $b \in B - H$ do not commute.

In general, the permutational product depends upon the transversals chosen. We give here an example. Take A, B to be groups isomorphic to S_3 and H to be a subgroup of order 2 of S_3. For A, B, H we give the following presentations.

$$\begin{aligned} A =& gp\ (p, r; p^3 = r^2 = (pr)^2 = 1), \\ B =& gp\ (p, r; q^3 = r^2 = (qr)^2 = 1), \\ H =& gp\ (p, r; p^2 = 1). \end{aligned}$$

For the transversals of H in A and B, first we choose

$$S_1 = \left\{1, p, p^2\right\}, T_1 = \left\{1, q, q^2\right\}$$

We rename the elements of $K_1 = S_1 \times T_1 \times H$, for convenience:

$$\begin{array}{ccc} (1,1,1) = 1; & (p,1,1) = 4; & (p^2,1,1) = 7; \\ (1,q,1) = 2; & (p,q,1) = 5; & (p^2,q,1) = 8; \\ (1,q^2,1) = 3; & (p,q^2,1) = 6; & (p^2,q^2,1) = 9; \\ (1,1,r) = 1'; & (p,1,r) = 4'; & (p^2,1,r) = 7'; \end{array}$$

$$(1, q, r) = 2'; \quad (p, q, r) = 5'; \quad (p^2, q, r) = 8';$$
$$(1, q^2, r) = 3'; \quad (p, q^2, r) = 6'; \quad (p^2, q^2, r) = 9'.$$

By a straightforward computation one obtains: **196**

$$\rho(p) = (147)(258)(369)(1'7'4')(2'8'5')(3'9'6'),$$
$$\rho(r) = (11')(22')(33')(44')(55')(66')(77')(88')(99'),$$
$$\rho(q) = (123)(456)(789)(1'3'2')(4'6'5')(7'9'8').$$

One can easily verify that

$$[\rho(p), \rho(q)] = L.$$

Thus $\rho(p)$ and $\rho(q)$ generate a group of order 9. Let p_1 denote the permutational product of the amalgam,

$$P_1 = gp(\rho(p), \rho(q), \rho(r)).$$

It is not difficult to verify that P_1 is an extension of $gp(\rho(p), \rho(q))$ by $gp(\rho(r))$. Thus **197**

$$|P_1| = 18.$$

Now we choose different transversals and form the permutation product. Choose

$$S_2 = \left\{r, p, p^2\right\}, T_2 = T = \left\{1, q, q^2\right\}$$

to form the permutational product. Let

$$K_2 = S_2 \times T_2 \times H.$$

As before we rename the elements of K_2

$$(r, 1, 1) = 1; \quad (r, q, 1) = 2; \quad (r, q^2, 1) = 3;$$
$$(p, 1, 1) = 4; \quad (p, q, 1) = 5; \quad (p, q^2, 1) = 6;$$
$$(p^2, 1, 1) = 7; \quad (p^2, q, 1) = 8; \quad (p^2, q^2, 1) = 9;$$
$$(r, 1, r) = 1'; \quad (r, q, r) = 2'; \quad (r, q^2, r) = 3';$$
$$(p, 1, r) = 4'; \quad (p, q, r) = 5'; \quad (p, q^2, r) = 6';$$

$$(p^2, 1, r) = 7'; \qquad (p^2, q, r) = 8'; \qquad (p^2, q^2, r) = 9'.$$

As we have not changed the transversal T_1, of H in $B, \rho(q)$ and $\rho(r)$ **198**
are not altered. The only generator that is altered is $\rho(p)$. One can again compute it without difficulty:

$$\rho(p) = (17'4')(28'5')(39'6')(1'47)(2'58)(3'69)$$

Now

$$[\rho(p), \rho(q)] = (132)(456)(1'2'3')(7'8'9').$$

Thus $gp(\rho(p), \rho(q))$ is not elementary abelian; in fact it turns out to be a group order 81. The group P_2, the permutational product with the above choice of transversals is given by

$$P_2 = gp(\rho(p), \rho(q), \rho(r)); \textit{ and}$$
$$P_1 \neq P_2.$$

Thus, in general, by selecting different transversals we get different permutational products. If we choose the transversals $\{r, p, p^2\}, \{r, q, q^2\}$ of H in A, B respectively, the corresponding permutational product P_3 we get, is a group of order 9; in fact it is the direct product of the alternating group, A_9 and a group of order 2 and therefore not soluble, whereas S_3 is metabelian. Thus the permutational product of two metabelian group with an amalgamated sub ground need not even be soluble.

4

199 Consider now the amalgam of any two groups with an amalgamated subgroup, say H. We have already seen that if H is central both in A and in B, then the permutational product does not depend upon the transversals of H chosen in A and B. We now prove that if H is central in A, then the permutational product is independent of the transversal of H in B we choose to form the product. More precisely we have

Theorem 3. *Let $H \leq$ center $(A), S$ a transversal of H in A.If T, T' are any two transversals of H in B, then the permutational product P on the set $K = S \times T \times H$ and the permutational product P' on $K' = S \times T' \times H$ are isomorphic.*

Proof. Let $\rho'(a)$, $\rho(b)$ $a \in A$, $b \in B$, denote the permutations on the set K' corresponding to permutations $\rho(a), \rho(b)$ on the set K. Consider the mapping φ of K into K',

$$(s,t,h)^{\varphi} = (s,t',h'), s \in S, h, h' \in H, t, \in T, t' \in T'$$

defined by

$$t'h' = th.$$

□

It is obvious that φ is $1-1$ and onto and

$$(s,t',h')^{\varphi-1} = (s,t,h), s \in S, t \in T, t' \in T', h, h' \in H,$$

where $$th = t'h'.$$

Now for $a \in A$, let us compute **200**

$$(s,t',h')^{\varphi^{-1}}(a\varphi), (s,t',h') \in K'.$$

We have

$$\begin{aligned}(s,t',h')^{\varphi^{-1}} &= (s,t,h), \text{ where}\\ th &= t'h', t \in T, h \in H; \text{ and}\\ (s,t,h)^{\varphi(a)} &= (s_1,t_1,h_1), \text{ where}\\ s_1h_1 &= sha, t = t_1, s_1 \in S, h_1 \in H; \text{ and}\end{aligned}$$

finally,

$$\begin{aligned}(s_1,t_1,h_1)^{\varphi} &= (s_1,t_1',h_1'), \text{ where}\\ t_1'h_1' &= t_1h_1, t_1' \in T', h_1' \in H.\end{aligned}$$

Now,

$$t_1'h_1' = t_1h_1 = th_1 = th.h^{-1}h_1 = t'h'h^{-1}h_1.$$

Therefore, **201**

$$t_1' = t', h_1' = h'h^{-1}h_1.$$

Using the hypothesis that $H \leq$centre (A), we get

$$\begin{aligned} (sa)h &= sha = s_1h_1; \text{ that is} \\ sa &= s_1h_1h^{-1} \text{ and} \\ sh'a = (sa)h' &= (s_1h_1h^{-1})h' = s_1(h_1h^{-1}h') = s_1h'_1. \end{aligned}$$

Thus

$$(s, t', h')^{\varphi^{-1}\rho(a)\varphi} = (s_1, t'_1, h_1) = (s_1, t', h'_1) = (s, t', h')^{\rho'(a)}.$$

As this is true for all $(s, t', h') \in K'$, we have

$$\varphi^{-1}\rho(a)\varphi = \rho'(a).$$

Now consider $\varphi^{-1}\rho(b)\varphi$, for $b \in B$. We have

$$(s, t'h')^{\varphi-1} = (s, t, h), th = t'h';$$

and $$(s, t, h)^{\rho(b)} = (s, t_1, h_1),$$

where $$t_1h_1 = thb, t_1 \in T, h_1 \in H:$$

and $$(s, t, h_1)^{\varphi} = (s, t'_1, h'_1),$$

where $$t'_1h'_1 = t_1h_1, t_1 \in T', h'_1 \in H.$$

202 But,

$$t'h'b = thb = t_1h_1 = t'_1h'_1.$$

Therefore,

$$(s, t', h')^{\varphi-1\rho(b)\varphi} = (s, t'_1, h'_1) = (s, t', h')^{\rho(b)}.$$

Again as this is true for all $(s, t', h') \in K'$, we get

$$\varphi^{-1}\rho(b)\varphi = \rho'(b).$$

It is obvious that the mapping η of $\rho(A) \cup \rho(B)$ into $\rho'(A) \cup \rho'(B)$ defined by

$$\rho(x)^{\eta} = \varphi^{-1}\rho(x)\varphi, x \in \rho(A) \cup \rho(B),$$

is 1 – 1 and 'onto '. Further if

$$u(\rho(x_1), \ldots, \rho(x_n) = L),$$

is a relation in P_1, with

$$x_i \in \rho(A) \cup \rho(B), i = 1, \ldots, n,$$

then

$$u(\rho(x_1)^\eta, \ldots, \rho(x_n^\eta) = (u(\rho(x_1), \ldots, \rho(x_n))^\eta) = \varphi^{-1}$$
$$u(\rho(x_i), \ldots, \rho(x_n))\varphi = \varphi^{-1}\ell\varphi = L.$$

Therefore by von Dyck's Theorem, η can be extended to an isomor- **203**
phism of P onto P', as $\rho(A) \cup \rho(B)$ and $\rho'(A) \cup \rho'(B)$ generate P and P' respectively. This proves the theorem.

5

We shall now consider questions of the form:

If the groups A and B have the property $\mathcal{P}$, can the amalgam be embedded in a group P with the property $\mathcal{P}$?

Let $\mathcal{P}$ be a property of groups. We say that a group G has the property $\mathcal{P}$ *locally* if every finite set of elements of G is contained in a subgroup of G having $\mathcal{P}$. In particular, a group G is *locally finite* if every finitely generated subgroup of G is finite. Similarly we can speck if *locally soluble* and *locally nilpotent* groups.

A locally finite group is obviously periodic. For a long time nothing was known about the converse of this statement; but the recent results of Novikov provide example of periodic groups that are not locally finite.

Consider an amalgam of groups A, B with an amalgamated subgroup H. We ask if A and B are locally finite, can the amalgam be embedded in a locally finite group? The answer to this question, in general, is 'no'. **204**
But if we impose certain 'good' conditions on H such an embedding can be achieved. The answer to the above question is 'yes' if H is finite or H is central both in A and B. (See Theorems 4 and 5.) If H is central

only in A or B, the answer is not completely known; for a partial result, see the end of this Chapter.

We can repeat the same question replacing "locally finite" by "periodic"; that is, we ask: if A and B are periodic, can the amalgam be embedded in a periodic group? Again, in general, the answer is 'no'. If H is central in both A and B, the answer is 'yes'. Nothing is known in the case when H is finite or when H is central only in A or B.

We now give an example to show that if A and B are locally finite, the amalgam need not even be embeddable in a periodic group.

Let C be a periodic abelian group in which the orders of the elements is unbounded. For instance we can take C to be the Prufer p^∞ -group. Let

$$H = C \times C.$$

Take

$$A = gp(H, a; a^4 = 1, (c, d)^a = (d^{-1}, c), \text{ for all } (c, d) \in H)$$

and $$B = gp(H, b; b^3 = 1, (c, d)^b = (c^{-1}d, c^{-1}), \text{ for all} (c, d) \in H).$$

205 A is the splitting extension of H by the cyclic group (of order 4) generated by a; similarly, B is the splitting extension of H by the cyclic group (of order 3) generated by b. It is not difficult to show (cf. the lemma in the next section) that an extension of a locally finite group by a locally finite group (or as we also say a locally finite-by-locally finite group) is itself locally finite. Thus A and B are locally finite. Their intersection is, of course,

$$A \cap B = H.$$

Let P be any group embedding the amalgam, consider the element

$$p = ab \in P.$$

We have for any $(c, d) \in H$,

$$(c, d)^p = (c, d)^{ab} = (d^{-1}, c)^b = (dc, d).$$

It is easy to verify that

$$(c, d)^{p^n} = (d^n c, d), \text{ for } n = 1, 2, 3, \ldots.$$

206 If p were of finite order, say m, then

$$(c,d)^{p^m} = (d^m c, d) = (c,d);$$

that is,

$$d^m c =: \text{that is}$$
$$d^m =, \text{ for all } d \in H.$$

This contradicts our choice of H. Therefore P is not periodic.

6

In this section we shall give two sufficient conditions for the amalgam of two locally finite groups A and B with an amalgamated subgroup H to be embeddable in a locally finite group.

Theorem 4. *The amalgam of two locally finite groups A and B with an amalgamated subgroup H is embeddable in a locally finite group if H is central both in A and B.*

Proof. Since

$$H \leq \text{ centre } (A), H \leq \text{ centre } (B),$$

the generalised direct product P of the amalgam exists. We claim that P is locally finite. One can prove this directly. But, we shall deduce it from a more general lemma. □

Lemma. *An extension of a locally finite group by a locally finite group is a locally finite group.*

Proof. Let P be an extension of a locally finite group A by a locally finite group B, so that 207

$$A \triangle P, P/A \cong B.$$

Let $p_1, \ldots, p_n$ be arbitrary elements of P, where n is any positive integer and

$$G = gp(p_1, \ldots, p_n).$$

□

Consider the canonical mapping φ of P onto P/A. We have

$$|G^{\varphi}| = |gp(p_1^{\varphi}, \ldots, p_n^{\varphi})| < \infty, \text{ since}$$

P/A is isomorphic to B and thus locally finite. If φ_0 is the restriction of φ to G, we have

$$\varphi_0^{-1}\left\{1\right\} = G \cap A, G^{\varphi_0} = G^{\varphi}.$$

Therefore,

$$G/G \cap A \cong G^{\varphi}.$$

Now since G is finitely generated and $G \cap A$ has finite index in G, by a theorem of Schreier (1927, cf, e.g Kurosh 1956, p. 36) also $G \cap A$ is finite generated. Therefore the local finiteness of A implies that the group $G \cap A$ is finite. Now, since $G \cap A$ and $G/G \cap A$ are finite, G itself is
208 finite. This prove that P is locally finite. Now to complete that proof of Theorem 4, we have only to remark that the generalised direct product P of the amalgam is an extension of A by a factor group of B (namely by B/H).

Theorem 5. *The amalgam of locally finite groups A and B with an amalgamated subgroup H is embeddable in a locally finite group if H is finite.*

Proof. Choose transversals S, T of H in A and B respectively and form the permutational product P of the amalgam on the set $K = S \times T \times H$. Let,

$$G = gp(p_1, \ldots, p_r), p_i \in P, i = 1, \ldots .r$$

be any finitely generated subgroup of P. Each p_i is a word in the elements of $\rho(A)$ and $\rho(B)$. Let $\rho(a_i), i = 1, \ldots, m$ and

$$\rho(b_i), i = 1, \ldots, \ell, a_i \in A, b_i \in B$$

occur when p_i are expressed as words in the elements of $\rho(A)$ and $\rho(B)$. Let,

$$A_1 = gp(a_1, \ldots, a_m, H)\text{and}$$
$$B_1 = gp(b_1, \ldots, b_m, H); \text{so that}$$

$$G = gp(p_1, \ldots, p_r) \leq gp(\rho(A_1), \rho(B_1), \rho(H)) = P_1(say).$$

$\square$

Now since H is finite and A and B are locally finite, the groups A_1 and B_1 are finite. Further **209**

$$A_1 \cap B_1 = H.$$

We now define $K_{ab} \subseteq K, a \in A, b \in B$ by

$$K_{ab} = \left\{(s,t,h) \middle| s \in aA_1, t \in bB_1\right\}$$

Since A_1, B_1 and H are finite, each K_{ab} is finite; in fact,

$$\left|K_{ab}\right| = \left|S \cap aA_1\right|\left|T \cap bB_1\right|\left|H\right| = \left|A_1 : H\right|\left|B_1 : H\right|\left|H\right| = \frac{\left|A_1\right| \left|B_1\right|}{\left|H\right|}.$$

Further for $a, c \in A, b, d \in B$ either

$$K_{ab} \cap K_{cd} = \phi \text{or}$$
$$K_{ab} = K_{cd}.$$

For, if $(s,t,h) \in K_{ab} \cap K_{cd}$, then

$$s \in aA_1 \cap cA_1, t \in bB_1 \cap dB;$$

hence $$aA_1 = cA_1, bB_1 = dB_1,$$

and $$K_{ab} = K_{cd}.$$

Now since every $(s,t,h) \in K_{st}$, it follows that $K = \bigcup_{a\in A, b\in B} K_{ab}$. We **210**
claim that every K_{ab} admits P_1. For let $(s,t,h) \in K_{ab}$; then, for $i = 1,\ldots,m$,

$$(s,t,h)^{\rho(a_i)} = (s_1,t_1,h_1) \text{ where}$$
$$s_1 h_1 = sha_i, t_1 = t;$$

Thus

$$s^{-1}s_1 = ha_i h_1^{-1} \in A_1,$$

and $$sA_1 = s_1 A_1.$$

But $(s, t, h) \in K_{ab}$. Therefore

$$s_1A_1 = sA_1 = aA_1; \text{ that is, } s_1 \in aA_1.$$

Moreover, $t_1 = t \in bB_1$. Hence $(s, t, h)^{\rho(a_i)} \in K_{ab}$. Similarly it can be proved that

$$(s, t, h)^{\rho(a_i)} \in K_{ab}, \text{ for every } (s, t, h) \in K_{ab}.$$

211 It is also obvious that, for every $h' \in H$,

$$(s, t, h)^{\rho(h')} \in K_{ab}, (s, t, h) \in K_{ab}.$$

Thus for every $a \in A, b \in B$, the elements of P_1 restricted to K_{ab} are permutations of the set K_{ab}. Hence P_1 is a subgroup of the Cartesian product of symmetric groups of permutations on the sets K_{ab}. Now since all of the sets K_{ab} have the same cardinal, the group P_1 can be regarded as a subgroup of a Cartesian power of the group $S(F)$ where $S(F)$ is the symmetric group of permutations on a set F of cardinal $|K_{ab}|$. Now the group P_1 is finitely generated. The following lemma proves that the group P_1 is finite.

Lemma. *Let E be a finite group, Y any set and Q a finitely generated subgroup of E^γ. Then Q is finite.*

Proof. Let $Q = gp(q_1, \ldots, q_n) \in E^Y$, with $q_i \in E^Y$. Consider the n-tuples

$$(q_1(y), \ldots, q_n(y)), y \in Y.$$

Since F is finite, there can only be a finite number of distinct such n-tuples. In fact the number N of distinct n-tuples cannot exceed $|E^n|$. Let $y_1, \ldots, y_N \in Y$. be such that

$$(q_1(y), \ldots, q_n(y)), i = 1, \ldots, N$$

212 are N distinct n-tuples. Let

$$Y_0 = \left\{y_1, \ldots, y_N\right\}$$

Consider the mapping θ of Q into E^{Y_0} defined by

$$q^\theta = q_0,$$

where q_0 is the restriction of q to Y_0. It is easy to verify that is a homomorphism. In fact θ is a homomorphism. For let $q \in Q$ belongs to the kernel of θ, that is $q^\theta = e_0$, where e_0 is the neutral element of E^{γ_0}; that is

$$e_0(y_i) = 1, i = 1, \ldots, N.$$

□

If $q = u(q_1, \ldots, q_n)$, then

$$q(y) = u(q_1(y), \ldots, q_n(y)).$$

Now there exists a $y_j, 1 \leq j \leq n$ such that

$$q_i(y) = q_i(y_j), i = 1, \ldots, n.$$

Now

$$u(q_1(y_j), \ldots, q_n(y_j)) = 1, \text{ since } q^\theta = e_0.$$

Therefore **213**

$$q(y) = u(q_1(y_j), \ldots, q_n(y_j)) = 1;$$

as y was an arbitrary element of Y, we see that q is the unit elements of E^Y. Thus the kernel of θ is trivial, in other words, θ is a homomorphism. Now θ, being isomorphic to a subgroup of the finite group E^{Y_0}, is finite. This completes the proof of the lemma.

Thus we have proved that every finitely generated subgroup P_1 of P is finite; that is P is locally finite.

Observing that in the proof of the above theorem the transversal S, T were arbitrary we have:

Corollary. *Every permutational product of the amalgam of two locally finite groups with an amalgamated subgroup is locally finite if the amalgamated subgroup is finite.*

If A and B are locally finite and if H is central in A and of countable index in A, it can be proved that there is an embedding (in a permutation product with a suitable transversal S of H in A) in a locally finite group. We shall, however, not prove this.

Chapter 11

Embedding of Nilpotent and Soluble Groups

1

Let G be a group and $A \subset G, B \subset G$ be any two subsets of G. We define the *commutator subgroup* $[A, B]$ of these subsets as 214

$$[A, B] = gp\left(\left\{[a, b]\middle|a \in A, b \in B\right\}\right).$$

In particular $[G, G]$ is the *derived group* of G. A normal series of the form

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots$$

is called a *descending central series* if

$$G_i \Delta G, i = 1, 2, \ldots, \text{ and}$$
$$G_i/G_{i+1} \leq \text{ centre } (G_i/G_{i+1}), i = 0, 1, 2, \ldots.$$

It is immediate that

$$G_i/G_{i+1} \leq \text{ centre } (G/G_{i+1})$$

if and only if

$$[G, G_i] \leq G_{i+1}.$$

In general a descending central series may not become stationary in **215**
a finite number of steps. We call a group G *nilpotent of classes n* if G has a descending central series with

$$G_n = \left\{1\right\}.$$

The normal series

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots$$

where $$G_{i+1} = [G_i, G], i = 0, 1, 2, \ldots$$

is called the *lower central series.* One can show that the terms of the lower central series are verbal subgroups of G and hence fully invariant in G. A group G is nilpotent of class n if and only if the n^{th} term in the lower central series is the trivial group. Further if n is the least integer such that the n^{th} term of the lower central series is the trivial group, then G is nilpotent of class n but not of class $n-1$.

A series of the form

$$\{1\} = H_\circ \leq H_1 \leq H_2 \cdots$$

is called an *ascending central series series* if

$$H_i \Delta G, i = 1, 2, \ldots, \text{ and}$$
$$H_{i+1}/H_i \leq \text{ centre } (G/H_i)$$

216 or equivalently if

$$\left[G, H_{i+1}\right] \leq H_i.$$

Obviously, in a nilpotent group there is an ascending central series terminating in G in a finite number of steps. The ascending central series

$$\{1\} = H_0 \leq H_1 \leq H_2 \leq \cdots$$

with $$H_{i+1}/H_i = \text{ centre } (G/H_i)$$

is called the *upper central series* of G. In general, the upper central series does not become stationary in a finite number of steps and even if it does it may not end in G. But the upper central series of a nilpotent group reaches G in a finite number of steps. Further the upper and the lower central series of a nilpotent group (broken off as soon as the former has reached G and the latter 1) have the same length.

Obviously every nilpotent groups is soluble and the length of solubility does not exceed the class of nilpotency. It is not difficult to prove 217
that

Theorem 1. *A group of order p^n where p is a prime and $n > 1$ is nilpotent of class $n-1$.*

The proofs of the above statements including Theorem 1 are straight forward (see eg. Krosh (1956), Chapter XV,p.211.)

2

We have seen in the last chapter that an amalgam of two abelian groups (i.e. nilpotent groups of class 1) is embeddable in and abelian group. We now ask:

Can every amalgam of two nilpotent (soluble) groups be embedded in a nilpotent (soluble) group?

In general, the answer to this question is 'no'. In fact, there is an amalgam of an abelian group A and a nilpotent group B of class $c = 2$ which cannot be embedded in any nilpotent group. (J.Wiegold, 1959)

The following example shows that an amalgam of two nilpotent groups need not even be embeddable in a soluble group.

Let

$$\begin{aligned} K &= gp(g,h; \quad g^5 = h^5 = 1, \qquad [g,h] = 1),\\ A &= gp(H,a; \quad g^a = gh, h^a = h, \qquad a^5 = 1),\\ B &= gp(H,b; \quad g^b = g, h^b = g^{-1}h, \quad b^5 = 1). \end{aligned}$$

Clearly, 218

$$|H| = 5^2, |A| = |B| = 5^3.$$

By Theorem 1, A and B are nilpotent groups of class 2. Consider the amalgam of the groups A and B with the amalgamated subgroup H. From the definition of A and B we readily confirm that

$$H\Delta A, H\Delta B.$$

We now prove that the amalgam of A and B with the amalgamated subgroup H is not embeddable in any soluble group. Let G be a group embedding the amalgam and

$$p = gp(A, B) \leq G.$$

We first note that

$$H\Delta P.$$

Let Γ be the group of all automorphisms of H induced by the inner automorphisms of P. It is well known that

$$\Gamma \cong P/N,$$

where N is the centralizer of H in P. (The set N of all elements in P which commute with every element of H is group; the group N is called the *centralizer* of H in P. Since H is normal in P, one easily verifies that $N\Delta P$.)

219 Now,

$$\Gamma = gp(\alpha, \beta),$$

where α, β are the automorphisms of H induced by the inner automorphisms φ_a, φ_b of P given by

$$x^{\varphi_a}a = a^{-1}xa, \text{ for every } x \in P$$

and

$$x^{\varphi_b} = b^{-1}xb, \text{ for every } x \in P.$$

The group H being abelian and of exponent 5 can be considered as a vector space over the prime field $GF(5)$ of characteristic 5. In fact H becomes a two dimensional vector space over $GF(5)$ with (g, h) as a basis. Thus the endomorphisms ring of H is the ring of all 2×2 matrices over $GF(5)$. Let us now take the matrix representations of the automorphisms α, β of H. Now writing the operations of H additively, we have

$$g^{\alpha} = g^2 = g + h$$
$$h^{\alpha} = h^a = h.$$

Thus α corresponds to the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Similarly it is easy to see that β corresponds to the matrix 220

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

The multiplicative group M generated by the matrices α, β is precisely the group of all 2×2 matrices with determinant 1 over $GF(5)$. The group Γ is isomorphic to this group M. We identify Γ with M. The group M is well known and is called the binary icosahedral group (see Coxeter and Moser, 1957, p.69). The binary icosahedral group has order 120. Its centre is cyclic of order 2, and the factor group of the centre is the icosahedral group (or alternating group A_5 of degree 5). Thus M is not soluble. This prove that P and therefore G is not soluble. Thus the amalgam of two nilpotent group of class 2 need not even be embeddable in a soluble group.

3

In this section we shall impose some conditions on the amalgamated subgroup H to achieve a 'good' embedding of the amalgam of nilpotent or soluble groups.

Theorem 2. *Let A, B be two nilpotent groups of class c (soluble groups of length ℓ). The amalgam of A and B with an amalgam subgroup H can be embedded in a nilpotent group of class c (soluble group of length ℓ) if H is central both in A and in B.* 221

Proof. Let P be the generalised direct product of the amalgam. Then

$$P = A \times B/N, N \Delta A \times B.$$

Now the direct product of two groups (and indeed the Cartesian product of an arbitrary family of groups) that are nilpotent of class c (soluble of length ℓ) is itself a nilpotent of class c (soluble of length ℓ)¿ In fact the nilpotent groups of class c, and also the soluble groups of length ℓ, form a variety. [For soluble groups, of cf. Chapter 7, for nilpotent groups we omit the proof]. It follows that $A \times B$, and then also P, is nilpotent of class c (soluble length ℓ). □

If H is central in A but not necessarily central in B then Wiegold's example (see Section 2) shows that we cannot in general hope for an embedding in a nilpotent group. But in the case of solubility the situation is different as is shows by the following theorem.

Theorem 3. *If A is soluble of length ℓ, B soluble of length m and if H is central in A then the permutational product P of the amalgam (irrespective of the transversal chosen) is soluble of length $n \leq \ell + m - 1$.*

Proof. Let S, T be transversals of H in A and B respectively and $K = S \times$
222 $T \times H$. Let P be the permutational product of the amalgam corresponding of the transversals S, T. For every $f \in B^S$, we define a mapping $\gamma(f)$ of K, called a *quasi-multiplication*, as follows:

$$(s, t, h)^{\gamma(f)} = (s, t, h)^{\rho(f(s))}, (s, t, h) \in K.$$

In other words, $\gamma(f)$ coincides with $\rho(f(s))$ on all those elements of K whose first coordinate is s. Thus

$$(s, t, h)^{\gamma(f)}(s^*, t^*, h^*), \text{ where}$$
$$s^* = s, t^* h^* = thf(s).$$

Consider the mapping η of the Cartesian power B^S into, and in fact onto, the set Γ of all quasi-multiplications, η being defined by

$$f^\eta = \gamma(f), f \in B^S.$$

First we prove that

$$\gamma(fg) = \gamma(f)\gamma(g), \text{ for } f, g \in B^S.$$

Let (s,t,h) be an arbitrary element of K. Then

$$(s,t,h)^{\gamma(fg)} = (s,t,h)^{\rho(fg(s))} = (s,t,h)^{\rho(f(s)).g(s))} \quad = (s,t,h)^{\rho(f(s))\rho(g(s))}.$$
$$= \left((s,t,h)^{\gamma(f)}\right)^{\rho(g(s))}.$$

□

Now since s is not altered after applying $\gamma(f)$, we have 223

$$\left((s,t,h)^{\gamma(f)}\right)^{\rho(g(s))} = \left((s,t,h)^{\gamma(f)}\right)^{\gamma(g)} = (s,t,h)^{\gamma(f)\rho(g(s))\circ\gamma(g)}.$$

Therefore

$$\gamma(fg) = \gamma(f)\gamma(g).$$

This proves that η is a homomorphism, and the homomorphic image is a group. In particular, this proves that the quasi-multiplications are permutations on the set K. Now if

$$\gamma(f) = L, \text{ then}$$
$$(s,t,h)^{\gamma(f)} = (s,t,h) \text{ for every } (s,t,h) \in K;$$

that is

$$thf(s) = th, \text{ for every } s \in S; \text{ i.e.},$$
$$f(s) = 1, \text{ for every } s \in S.$$

Thus the kernel of η is trivial; that is, η is an isomorphism. Thus 224

$$B^S \cong \Gamma.$$

Further,

$$\rho(B) \leq \Gamma$$

For,

$$\begin{aligned} \rho(b) = \gamma(f_b), b \in B, &\text{ where} \\ f_b \in B^S &\text{ is such that} \\ f_b(s) = b \text{ for every } s \in S; \end{aligned}$$

in other words f_b is in the diagonal of B^S.

Consider the group

$$\Delta = \Gamma \cap P.$$

We claim that

$$\Delta \Delta P.$$

Let $a \in A, \gamma(f) \in \Gamma$, $f \in B^S$ and

$$\rho(a^{-1})\gamma(f)\rho(a) = \rho(a)^{-1}\gamma(f)\rho(a) = \gamma'.$$

225 Let $(s, t, h) \in K$ and

$$sa^{-1} = \bar{s}\bar{h}, \bar{s} \in S, \bar{h} \in H.$$

Thus $\bar{s}, \bar{h}$ are completely determined by a and s. Then

$$(s, t, h)^{\rho(a^{-1})} = (\bar{s}, t, h\bar{h});$$

for, H being central in A, we have

$$sha^{-1} = sa^{-1} = \bar{s}\bar{h}h.$$

Now

$$\begin{aligned} (\bar{s}, t, h\bar{h})^{\gamma(f)} = (\bar{s}, t, h\bar{h})^{\rho(f(\beta\bar{s}))} = (\bar{s}, t_1, h_1), &\text{ where} \\ t_1 h_1 = th\bar{h} f(s). \end{aligned}$$

Finally we have,

$$\begin{aligned} (\bar{s}, t_1, h_1)^{\rho(a)} = (s_1, t_1, \bar{h}_1), &\text{ where} \\ s_1 \bar{h}_1 = \bar{s} h_1 a. \end{aligned}$$

Now, again since $H \leq$ centre (A), we have

$$s_1\overline{h}_1 = \overline{s}h_1 a = (\overline{s}a)h_1 = s(\overline{h}^{-1}h_1)$$

226 Therefore,

$$s = \overline{s}; \text{ and}$$
$$\overline{h}_1 = \overline{h}^{-1}h_1.$$

Further

$$t_1\overline{h}_1 = t_1\overline{h}^{-1}h_1 \qquad = (t_1h_1)\overline{h}^{-1} = (th\overline{h}f(\overline{s}))\overline{h}^{-1}$$
$$= th(\overline{h}f(\overline{s})\overline{h}^{-1})$$

Now, since $\overline{s}, \overline{h}$ are completely determined by s and a, the function f' defined by

$$f'(s) = \overline{h}f(\overline{s})\overline{h}^{-1}$$

is well defined and is in B^S. We have

$$(s,t,h)^{\rho(a^{-1})\gamma(f)\rho(a)} = (s_1,t_1,\overline{h}_1); \text{ and}$$
$$s_1 = s, t_1\overline{h}_1 = thf'(s).$$

Therefore 227

$$\rho(a^{-1})\gamma(f)\rho(a) = \gamma(f') \in \Gamma.$$

It is now immediate that

$$\rho(a^{-1})\Delta\rho(a) = \Delta.$$

Since $\rho(B) \leq \Delta$, we have

$$\rho(b^{-1})\Delta(b) = \Delta, b \in B.$$

Hence,

$$\Delta\Delta P.$$

Further,

$$P/_Delta \cong \rho(A)/\rho(A) \cap \Delta$$

Now $\rho(A)/\rho(A) \cap \Delta$ is soluble of length ℓ and $\Delta \leq B^s$ is soluble of length m. Therefore P is soluble of length $\ell + m$. This almost proves Theorem 3; but we still want to improve the bound for the soluble length of P. Consider now,

$$\rho(a^{-1})\rho(b)\rho(a) \in \Gamma.$$

By what we have proved, it follows that

$$\rho(a^{-1})\rho(b)\rho(a) = \gamma(f')$$

228 where $f' \in B^S$ is defined by

$$f'(s) = \overline{h}b\overline{h}^{-1} \text{ where}$$
$$s\overline{a}^{-1} = \overline{sh}$$

Define $g \in B^S$ by

$$g(s) = \overline{h}, s \in S \text{ and}$$
$$f_b \in B^s \text{ by}$$
$$f_b(s) = b \text{ for every} s \in S.$$

Then,

$$\rho(a^{-1})\rho(b)\rho(a) = \gamma(g f_b g^{-1}).$$

Therefore,

$$[\rho(b), \rho(a)] = \rho(b^{-1})\rho(a^{-1})\rho(b)\rho(a) = \gamma(f_b^{-1} g f_b g^{-1})$$
$$= \gamma[f_b, g^{-1}] \in \Gamma', \text{ for all } a \in A, b \in B.$$

Therefore,

$$[\rho(A), \rho(B)] \leq \Gamma'.$$

It is not difficult to show that if a group G is generated by its sub-
229 groups G_1, G_2 then its derived group is

$$G' = G_1' G_2' [G_1, G_2];$$

hence

$$P' = [\rho(A), \rho(A)]\ [\rho(B), \rho(B)]\ [\rho(A), \rho(B)]$$

$$\leq \rho(A')\Gamma'.$$

Again,

$$P'' = \rho(A'')\Gamma''[\rho(A'), \Gamma'] \leq \rho(A'')\Gamma'.$$

Continuing in this fashion we arrive at $P^{(\ell)} \leq \rho(A^{(\ell)}\Gamma'$, where $P^{(\ell)}$, $A(\ell)$ denote the ℓth derived groups of P and A respectively. Now since A is soluble of length ℓ, we have

$$A^{(\ell)} = \{1\}.$$

Hence,

$$P^{(\ell)} \leq \Gamma'.$$

Therefore,

$$P^{(\ell+m-1)} \leq (\Gamma')^{(m-1)} = \Gamma^{(m)} = \{1\},$$

as $\Gamma \cong B^s$ is soluble of length m. Therefore te group P is soluble of **230**
length $\ell + m - 1$.

This proves our assertion.

Chapter 12

The Problems of Heinz Hopf

1

More than twenty five years ago, Heinz Hopf formulated the following two problems which are closely related. These problems arose out of a topological problem, which we do not formulate here (cf. B.H. Neumann, 1953). 231

First Hopf Problem. Can a finitely generated group be isomorphic to one of its proper factor groups?

Second Hopf Problem. If G is a finitely generated group and H an epimorphic image of G, and G an epimorphic image of H, are G and H necessarily isomorphic?

We now take following definition

Definition. *A* group G is a *Hopf group* if G is not isomorphic to ant of its proper factor groups.

In virtue of this definition, the First Hopf Problem can be reformulated as follows:

Is every finitely generated group Hopf group?

There are examples of non-finitely generated groups which are not Hopf group. For instance, one can easily verify that the direct power or the cartesian power of any group $G \neq 1$ over any infinite index set $I(e, g.I = \{1, 2, 3, \cdots\})$ is not a Hopf group. The Prufer group $Z(p^{\infty})$ (see Ch.8, Section 2 Corollary 3) is also a non-Hopf group. 232

A negative answer to the second problem implies an affirmative answer to the first. In other words the existence of two non-isomorphic finitely generated groups which are epimorphic images of each other implies the existence of a finitely generated non-Hopf group. For let G be a finitely generated group and H any group and let θ and ψ be endomorphisms of G onto H and H onto G respectively. Then the composite map $\theta\psi$ is an epimorphism of G onto G. Now if ψ has a non-trivial kernel then $\theta\psi$ also has a not-trivial kernel. Let N be the kernal of $\theta\psi$. Then it follows that

$$G \cong G/N,$$

that is, G is not a Hopf group. On the other hand, the existence of a finitely generated non-Hopf group does not by itself solve the second Hopf Problem.

It is known that all finitely generated free groups are Hopf groups (Magnus (1935); see also Kurosh, (1956)39, *p*.59). Magnus (1935) also proved that the finitely generated reduced free groups of the variety of nilpotent groups of class c are Hopf groups. Reinhold Baer made an example of finitely generated non Hopf group. Though he later withdrew this as containing a mistake, it suggested the possibility of finding such a group. B.H. Neumann (1950) thereupon constructed a 2 gener-
233 ator non-Hopf group; this has an infinite number of defining relations. Graham Higman (1951) constructed a finitely related 3-generator non-Hopf group. Using the group of Graham Higman (1951), B.H. Neumann (1953) gave an example of 3-generator finitely related groups G and H which are epimorphic images of each other, but are not isomorphic. Thus the first and the second Hopf Problems have been solved now.

Let G be a non-Hopf group, Then there exists a non-trivial normal subgroup N of G such that

$$G \cong G/N.$$

Let φ denote the isomorphism of G/N onto G, and θ the canonical epimorphism of G onto G/N. The mapping

$$\psi = \theta\varphi$$

is an epimorphism of G onto G. Let N_1 be the kernal of the mapping ψ. Then

$$N_1 = \{1\}^{\psi-1} = \left(\{1\}^{\varphi^{-1}}\right)^{\theta-1} = \{1\}^{\theta^{-1}} = N.$$

Consider now the epimorphism ψ^2 of G onto G. By an easy application of well-known isomorphism theorems one finds that the kernal N_2 of ψ^2 is such that

$$N_1 < N_2, N_2/N_1 \cong N.$$

More generally, if N_r is the kernel of the epimorphism ψ, we have 234

$$N_{r-1} < N_r, N_r/N_{r-1} \cong N.$$

Thus,

$$N_1 < N_2 < N_3 < \cdots$$

is a strictly ascending of normal subgroups. As this is not possible is a group satisfying the maximal condition for normal subgroups, we have

Theorem 1. *A group satisfying the maximal condition for normal subgroups is a Hopf group.*

We know that a finitely generated nilpotent group satisfies the maximal condition for subgroups. (See Kurosh, 1956, Ch. XV, p. 232) Hence we have:

Corollary 1. *A finitely generated nilpotent group is a Hopf group.*

Again, by a theorem of P. Hall (1954[b]) already quoted (in Chapter 8, p. 141) a finitely generated metabelian group satisfies the maximal condition for normal subgroups. Thus we have:

Corollary 2. *A finitely generated metabelian group is a Hopf group.*

This is the best possible result so far as soluble length of soluble Hopf groups is concerned; we shall later make an example of a finitely generated non-Hopf group which is soluble of length 3 (see section 4 of this Chapter).

2

Definition 1. A subgroup G of a group H is an *E-subgroup of H if for every normal subgroup R of G, there exist a normal subgroup S of H such that* 235

$$S \cap G = R.$$

The above definition is equivalent to the following:

Definition 2. *A* subgroup G of a group H is an E-subgroup of H if for every normal subgroup R of G, we have

$$R^H \cap G = R,$$

where R^H is the normal closure of R in H. It is clear that if $R^H \cap G = R$, then we can take R^H as the S of Definition (1); conversely, if there is a normal subgroup S of H such that $S \cap G = R$, then $R \leq S$, hence $R^H \leq S^H = S$, and

$$R \leq R^H \cap G \leq S \cap G = R;$$

thus also $R^H \cap G = R$. We give yet another equivalent definition of an E-subgroup:

Definition. *A* subgroup G is an E-subgroup of H if every epimorphism θ of G onto a group $G_1 = G^\theta$ can be extended to an epimorphism θ^* of H onto a group H_1 containing G_1.

Let $G \leq H$ satisfy the conditions of Definition (2).

236 Let θ be any epimorphism of G onto a group G_1 and R be its kernel. Then

$$R = \{1\}^{\theta^{-1}} \Delta G.$$

Therefore

$$R^H \cap G = R.$$

Now

$$GR^H/R^H \cong G/R^H \cap G = G/R \cong G_1.$$

Let θ^* be the natural map of H onto H/R^H. By identifying G_1 with GR^H/H canonically θ^* becomes an extension θ.

Conversely, assume the conditions of Definition (10). Let $R\Delta G$, and let θ be the canonic epimorphism of G onto $G_1 = G/R$. Extend θ to an epimorphism θ^* of H onto a group H_1 containing G_1, and let the kernel of θ^* be S. As $R^{\theta^*} = R^\theta$ is trivial, $R \leq S \cap G$. Now if $s \in S \cap G$ then

$$1 = s^{\theta^*} = s^\theta,$$

and thus $s \in R$. It follows that $S \cap G \leq R$, and hence

$$S \cap G = R.$$

This is the condition of Definition (1), which we already know to be equivalent to Definition (2). Thus all the three definitions are equivalent.

If H is the direct product of two groups F and G then F and G are E-subgroups of H. More generally, if H is the direct product or the Cartesian product of a family of groups, say $\{G_i\}_{i\in I}$, then each factor G_i is an E-subgroup of H. If H is any group and $Z(H)$ its center, then any subgroups of $Z(H)$ is an E-subgroup of H. This follows from the fact that every subgroup of $Z(H)$ is a normal subgroup of H. Further, if H is a simple group then a proper non-trivial subgroup of H is not an E-subgroup of H. We now prove the following: 237

Theorem 2. *The relation "E- subgroup of" is transitive; in other words, if G is an E-subgroup of H, and H an E-subgroup of K, then G is an E-subgroup of K.*

Proof. Let,

$$R\Delta G.$$

□

Then since G is an E-subgroup H, there is an $S \leq H$ such that

$$S\Delta H, S \cap G = R.$$

Now since H is an E-subgroup of K, there is a $T \leq K$ such that

$$T\Delta K, T \cap H = S.$$

We have

$$G \cap T = G \cap H \cap T = G \cap S = R.$$

238 This proves that G is an E-subgroup of K.

3

Let A, B be any two groups. Let

$$P = AWrB.$$

We shall now prove that the coordinate subgroups $A_b \leq A^B, b \in B$ (that is,

$$A_b = \left\{ f \middle| f \in A^B, f(y) = 1, \text{ for all } y \neq b \right\})$$

and the diagonal $A^\Delta \leq A^B$ are E-subgroups of P.

Let φ be any epimorphism of A onto a group A_o. Let

$$P_o = A_o WrB.$$

Consider the mapping φ^* of P onto P_o defined as follows. For every $p = bf \in P$, with $b \in B, f \in A^B$,

$$p^{\varphi^*} = (bf)^{\varphi^*} = bf_o, \text{ where } f_o \in A_o^B \text{ and}$$
$$f_o(y) = (f(y))^\varphi, y \in B.$$

We claim that φ^* is an epimorphism of P onto P_o. Let $p = bf, p' = b'f' \in P, b, b' \in B, f, f' \in A^B$.

239 Then

$$p^{\varphi^*} = bf_o, p'^{\varphi^*} = b'f'_o, \text{ where}$$
$$f_o(y) = (f(y))^\varphi, y \in B, , \text{ and}$$
$$f'_o(y) = (f'(y))^\varphi, y \in B.$$

Now

$$pp' = (bf)(b'f') = bb'.f^{b'}f'; \qquad \text{and}$$

therefore, $(pp')^{\varphi^*} = bb'.h,$ where $h \in A_o^B$
and $h(y) = (f^{b'} f'(y))^{\varphi}$

$$= (f^{b'}(y).f'(y))^{\varphi} = (f^{b'}(y))^{\varphi}(f'(y))^{\varphi},$$
$$= (f(yb^{-1}))^{\varphi}(f'(y))^{\varphi}, \text{ for all } y \in B.$$

On the other hand,

$$p^{\varphi^*} p'^{\varphi^*} = (bf_o)(b'f'_o) = bb' f_o^{b'} f'_o.$$

Now 240

$$f_\circ^{b'} f'_\circ(y) = f_\circ^{b'}(y).f'_\circ(y)$$
$$= f_\circ(yb'^{-1})f'_\circ(y) = (f(yb^{-1}))^{\varphi}(f'(y))^{\varphi}.$$

Thus,

$$(pp')^{\varphi*} = p^{\varphi*}p'^{\varphi*}.$$

This proves that φ^* is a homomorphism. It is easy to see that it maps P onto P_0 ; hence it is an epimorphism, as claimed.

Let θ be an epimorphism of A_b(or A^Δ) onto a group A_0 and ψ be isomorphism of A onto A_b (or A^Δ). Then the epimorphism

$$\varphi = \psi\theta$$

of A onto A_0 gives rise to a mapping φ^* of P onto P_0. If the group A_0 is identified with A_{ob}(or A_0^Δ), it follows without difficulty that φ^* is an extension of θ. This proves:

Lemma 1. In a wreath product the coordinate subgroups and the diagonal subgroup are E-subgroups.

In Chapter 8 we proved that a countable group G can be embedded in a 2-generator group H. We shall now prove that the embedding pro- 241
cedure given there embeds G as an E-subgroup of H. In the rest of this Chapter we shall use the notation of Chapter 8.

Let us briefly recall the embedding procedure of Chapter 8.

We started with a countable group G where

$$G = gp(\{a_i\}_{i\in I}) \text{ and}$$

$$I = \{1, 2, 3, \ldots\}.$$

We then formed the wreath product

$$P = GWrC, \text{ where}$$
$$C = gp(c);$$

and we embedded G as the diagonal subgroup G^Δ,

$$G^\Delta \leq G \leq P.$$

We then formed the wreath product

$$Q = PWrB,$$

where B was any group containing elements $b_i, i \in I$, with the property,

$$b_i \neq 1, b_i \neq b_j, b_ib_j \neq 1, b_ib_j \neq b_k.$$

242 Then we realised G as a subgroup G^* of

$$H = gp(q, B), q \in P^B.$$

In fact

$$G^* = gp(\{h_i\}_{i \in I}), \text{ where}$$
$$h_i[q^{b_i}, q] \in P^B.$$

(For the definitions of q andh_i, see Chapter 8.)

Now be Lemma 1, G^Δ is E-subgroup of P. Further, G^* is a subgroup of the coordinate subgroup $P_1 \leq Q$, where

$$P_1 = \left\{ f \middle| f \in P^B, f(y) = 1 \text{ for all } y \neq 1, y \in B \right\}$$

and G is mapped onto G^* under the natural isomorphism of P onto P_1. Therefore

$$G^* \text{ is an E-subgroup of } P_1.$$

Again by Lemma 1, P_1 is an E-subgroup of Q. Hence by the transitivity property of E-subgroups, G^* is an E-subgroup of Q. Now, since

$$G^* \leq H \leq Q,$$

it suffices for our purpose to show the following simple lemma.

243 **Lemma 2.** If $G \leq H \leq K$, and if G is an E-subgroup of K, then G is an E-subgroup of H.

For if $R\Delta G$, there is a subgroup $T\Delta K$ with

$$T \cap G = R;$$

put $S = T \cap H$: then $S\Delta H$and

$$S \cap G = T \cap H \cap G = T \cap G = R.$$

Applying this lemma to $G* \leq H \leq Q$, we obtain the stated result:

Corollary 3. *G^* is an E-subgroup of H.*

Let us now take G to be the free group of countably infinite rank presented by

$$G = gp(\{a_i\}_{i\in I}; \phi), \text{ where}$$
$$I = \{\ldots 2, -1, 0, 1, \ldots\}.$$

Take B to be the infinite cyclic group

$$B = gp(b), \text{ and}$$
$$b_i = b^{3i-1}$$

Then

$$h_i\left[q^{b^{3i-1}}, q\right] = \left[b^{1-3i}, qb^{3i-1}, q\right].$$

Identifying the group G with 244

$$G* = gp(\left\{h_i\right\}_{i\in I})$$

we have
$$G \leq H = gp(q, b).$$

Let now F be the free group

$$F = gp(s, t; \phi).$$

Define $E \le F$ as

$$E = gp(\left\{e_i\right\}_{i\in I}), \text{ where}$$
$$e_i = \left[s^{1-3i}, ts^{3i-1}, t\right], i \in I.$$

We prove:

Theorem 3. *The subgroup E is an E-subgroup of F.*

Proof. Let θ be the epimorphism of F onto H defined by

$$s^\theta = b, t^\theta = q.$$

Then we have

$$e_i^\theta = h_i, i \in I, \text{ and}$$
$$E^\theta = G.$$

□

245 Since G is freely generated by $\left\{h_i\right\}_{i\in I}$, it follows that E is also freely generated by $\left\{e_i\right\}_{i\in I}$. Hence the restriction of θ to E is an isomorphism. Let

$$R \Delta E.$$

Then

$$R^\theta = R_0 \Delta G.$$

Now since G is an E-subgroup of H, there is a $S_0 \Delta H$ such that

$$G \cap S_0 = R_0.$$

Let $S = S_0^{\theta^{-1}}$. Then

$$S \Delta F.$$

We have

$$(S \cap E)^\theta \le S^\theta \cap E^\theta = S_0 \cap G = R_0 = R^\theta.$$

This gives

$$S \cap E \leq R,$$

as the restriction of θ to E is one- one. But evidently also $R \leq S \cap E$; hence,

$$S \cap E = R.$$

This proves that E is an E-subgroup of F. 246

It may be of interest to remark that Theorem 3 is equivalent to the embedding theorem proved in Chapter 8. For a countable group G is an epimorphic image of E by an epimorphism, say θ. Now since E is an E-subgroup of F, θ can be extended to an epimorphism θ^* of F. Then

$$G \leq F^{\theta^*}, \text{ and}$$

F^{θ^*} is generated by 2 elements. The following is an unsolved problem in this context.

Unsolved problem. Is there a free infinite rank in the group

$$F = gp(s, t; s^p = t^q = 1)?$$

For $p \geq 2, q \geq 6$, the answer (unpublished) to this question is 'yes'.

For $p = 2, q = 3$, we have the following interesting problem:

Problem. Has the modular group an E-subgroup that is free of infinite rank?

4 Finitely generated soluble non-Hopf group

The object of this section is to construct a finitely generated soluble non-Hopf group. In this section also we shall use the notation of Chapter 8. 247
Using the embedding procedure of Chapter 8, we embed the free abelian group of countably infinite rank into a 3-generator group H by suitably choosing the group B; and then we prove that a certain factor group of H is a non-Hopf group.

Let G be the free abelian group of countably infinite rank presented by

$$G = gp(\{a_i\}_{i \in I}; \left[a_i, a_j\right] = 1, i, j, \in I),$$

where $$I = \Big\{ \dots -1, 0, 1, 2, \dots \Big\}.$$

As in Chapter 8, we embed G as the diagonal subgroup G^{Δ} of G^C in

$$P = G\,Wr\,C, \text{ where}$$
$$C = gp(c).$$

We now take the group B to be the free abelian group of rank 2 presented by

$$B = gp(b, b'; [b, b'] = 1)$$

and form the wreath product

$$Q = PWrB.$$

248 Choose the elements b_i (see Chapter 8) as

$$b_i = b^i b', i \in I.$$

One easily verifies that these b_i satisfy the inequalities:

$$b_i \neq 1, b_i \neq b_j, b_i b_j \neq 1, b_i b_j \neq b_k.$$

Therefore, as in Chapter 8, the group G is embedded as the subgroup $G*$ of H, where

$$H = gp(q, B) = gp(q, b, b') \leq Q$$

and $G^* = gp(\{a_i\}_{i \in I}) \leq H$.

We recall that $q \in P^B$ is defined by

$$q(1) = c,$$
$$q(b_i^{-1}) = g_i, i \in I,$$
$$q(y) = 1 \text{ otherwise },$$

where

$$g_i \in G^C \text{ is defined by}$$

$$g_i(c^n) = a_i^{-n}, n \in I; \text{ and further },$$
$$h_i = [q^{b_i}, q], i \in I.$$

249 Consider the mapping of B onto B defined by

$$b^\beta = b \text{ and}$$
$$b'^\beta = bb'.$$

It is easy to verify that β is an automorphism of B. We want to extend β to an automorphism β^* of Q. (Our procedure is applicable to an arbitrary automorphism of B, but we require it only for the particular β we have specified.) To do this we first extend β to an automorphism of P^B as follows:

For every $f \in P^B$, define $f^{\beta^*} \in P^B$ by

$$f^{\beta^*}(y) = f(y^{\beta^{-1}}), \text{ for all } y \in B.$$

It is easy to verify that β^* is one-one.

Now if $f_1, f_2 \in P^B$, then for every $y \in B$, we have

$$(f_1 f_2)^{\beta_*}(y) = f_1 f_2(y^{\beta^{-1}}) = f_1(y^{\beta^{-1}}) f_2(y^{\beta^{-1}}) = f_1^{\beta^*}(y).f_2^{\beta^*}(y).$$

Hence,

$$(f_1 f_2)^{\beta*} = f_1^{\beta*} f_2^{\beta*};$$

it follows that β^* is an automorphism of P^B.

We now extend β^* to Q and denote the extension of β^* also by β^*. For every $q_o = b_o f \in Q$, with ba $\in B$, $f \in P^B$, define 250

$$q_0^{\beta*} \qquad Q \text{ as follows :}$$
$$q_0^{\beta*} = (b_0 f)^{\beta*} = b_\circ^\beta f^{\beta*}.$$

If

$$q_0 = b_0 f, b_0 \in B, f \in P^B \text{ and}$$
$$q_0' = b_0' f', b_0' \in B, f' \in P^B$$

are arbitrary elements of Q, then

$$(q_0q_0')^{\beta*} = (b_0fb_0'f')^{\beta*} = (b_0b_0'f^{b_0'}f')^{\beta*} = (b_0b_0')^{\beta*}.(f^{b_0'}f')^{\beta*}$$
$$= (b_0b_0')^{\beta*}(f^{b_\circ'})^{\beta*}f'^{\beta*}$$

and

$$q_0^{\beta*}q_0^{\beta*} = (b_0f)^{\beta*}(b_0'f')^{\beta*} = b_0^{\beta*}f^{\beta*}.b_0'^{\beta*}f'^{\beta*} = b_0^{\beta*}b_0'^{\beta*}(f^{\beta*})^{b_0'}f'^{\beta*}.$$

But

$$(f'^{b_\circ'})^{\beta*}(y) = f^{b_0'}(y^{\beta-1}) = f(y^{\beta-1}b_0'^{-1}) \text{ for all } y \in B,$$

and

$$(f^{\beta*})^{b_0'^{\beta*}}(y) = f^{\beta*}(y(b_0'^{\beta*})^{-1}) = f^{\beta*}(y(b_0'^{-1})^{\beta*})$$
$$= f((yb'^{-1\beta_0})^{\beta-1}) = f(y^{\beta-1}b_0'^{-1}),$$

251 for all $y \in B$.

Therefore

$$(f^{\beta*})^{b_0'} = f^{b_0'})^{\beta*}.$$

Hence

$$(q_0q')^{\beta*} = q_0^{\beta*}q'^{\beta*}.$$

Again one can easily verify that $\beta*$ is one-one and onto; that is, $\beta*$ is an automorphism of Q.

Next, let γ be the automorphism of G defined by

$$a_i^{\gamma} = a_{i+1}(i \in I).$$

We want to extend γ to an automorphism $\gamma*$ of Q. (Our procedure is applicable to an arbitrary automorphism of G, but we require it only for the particular γ we have specified.) Define the mapping γ^+ of G^C onto G^C as follows:

If $f \in G^C$, then $f^{\gamma+} \in G^C$, and

$$f^{\gamma+}(c^n) = (f(c^n)) \text{ for } n \in I.$$

252 A straight forward verification shows that γ^+ is an automorphism of G^C. We now extend γ^+ to P by putting

$$(c^t f)^{\gamma^+} = c^t f^{\gamma^+}, c \in C, f \in G^C, t \in I.$$

Let $p_1 = c^t f, P_2 = c^u f'$ belong to P. Then

$$(p_1 p_2)^{\gamma^+} = (c^{t+u} f^{c^u} f')^{\gamma^+} = c^{t+u}(f^{c^u} f')^{\gamma^+}$$
$$= c^{t+u}(f^{cu})^{\gamma^+} f'^{\gamma^+}; \text{ and}$$
$$p_1^{\gamma^+} p_2^{\gamma^+} = c^t f^{\gamma^+} c^u f'^{\gamma^+} = c^{t+u}(f^{\gamma^+})^{c^u} f'^{\gamma^+}.$$

But

$$(f^{c^u})^{\gamma^+}(c^n) = (f^{c^u}(c^n))^{\gamma} = (f(c^{n-u}))^{\gamma}$$
$$= f^{\gamma^+}(c^{n-u}) = (f^{\gamma^+})^{c^u}(c^n), \text{ for all } n \in I.$$

Therefore

$$(f^{c^u})^{\gamma^+} = (f^{\gamma^+})^{c^u}.$$

Hence 253

$$(p_1 p_2)^{\gamma^+} = p_1^{\gamma^+} p_2^{\gamma^+}$$

It is obvious that the extended mapping γ^+ is one-one and onto. Thus γ^+ is an automorphism of P.

We now extend γ^+ to an automorphism γ^+ of Q. We first define γ^+ on P^B as follows. For any $y \in P^B, g^{\gamma^*} \in P^B$ and

$$g^{\gamma *}(y) = (g(y))^{\gamma^+}$$

One easily verifies that $\gamma *$ is an automorphism of P^B. We now extend $\gamma *$ to Q by putting

$$(b_0 g)^{\gamma *} = b_0 g^{\gamma *}, \text{ for } b_0 \in B, g \in P^B.$$

Let

$$q_1 = b_0 g, q_2 = b_0' g', \text{ be in } Q \text{ with}$$
$$b_0, b_0' \in B, g, g' \in P^B. \text{ Then}$$

$$(q_1q_2)^{\gamma*} = (b_0b_0'g^{b_0'}g')^{\gamma*} = b_0b_0'(b^{b_0'}g')^{\gamma*}$$
$$= b_0b_0'(g^{b_0'})^{\gamma*}g'^{\gamma*};\ \text{and}$$
$$q_1^{\gamma*}q_2^{\gamma*} = b_\circ g'^{\gamma*}.b_0'b_0'(g^{\gamma*})^{b_0'}g'^{\gamma*}.$$

254 But,

$$(g^{b_0'})^{\gamma*}(y) = (g^{b_0'}(y))^{\gamma^+} = (g(yb_0'^{-1}))^{\gamma^+} = g^{\gamma*}(g^{b_0'}(g^{\gamma*})^{b_0}(y) \text{ for all } y \in B.$$

That is to say,

$$(g^{b_0'})^{\gamma*} = (g^{\gamma*})^{b_0'};\ \text{that is },$$
$$(q_1q_2)^{\gamma*} = q_1^{\gamma*}q_2^{\gamma*}.$$

One easily sees that $\gamma*$ is one-one and onto. Hence, $\gamma*$ is an automorphism of Q.

It will be noticed that the procedure of extending $\gamma^+$by $\gamma*$ is the same as that of extending γ to γ^+; in fact it applies to wreath products in gen-
255 eral. Now, however, we being to use the particular automorphisms β, γ we had chosen and the automorphisms $\beta*, \gamma*$ constructed from them.

Now consider automorphism $\beta * \gamma*$ of Q. For any $b_0 \in B$, we have $b_0^{\beta*\gamma*} = (b_0^{\beta})^{\gamma*} = b_0^{\beta}$; that is $\beta * \gamma*$ is an extension of β. Further.

$$q^{\beta*\gamma*}(y) = \left(q^{\beta*}\right)^{\gamma*}(y) = \left(q^{\beta*}(y)\right)^{\gamma^+} = \left(q(y^{\beta-1})\right)^{\gamma^+}.$$

Therefore

$$q^{\beta*\gamma*}(1) = (q(1^{\beta-1}))^{\gamma^+} = (c)^{\gamma^+} = c$$

and $$(q^{\beta*\gamma*}(b_i^{-1})) = (q((b_i^{-i})^{\beta-1}))^{\gamma^+} = (q((b_i^{\beta-1})^{-1})))^{\gamma^+}.$$

But

$$b_i^{\beta-1} = (b^ib')^{\beta-1} = (b^i)^{\beta-1}(b')^{\beta-1} = b^ib^{-1}b' = b^{i-1}b' = b_{i-1},$$

so that $$q^{\beta*\gamma*}(b_i^{-1}) = (q((b_{i-1}))^{\gamma^+} = (g_{i-1})^{\gamma^+}.$$

256 As

$$g_{i-1}^{\gamma^+}(c^n) = (g_{i-1}(c^n))^{\gamma} = (a_{i-1}^{-n})^{\gamma} = a_i^{-n},\ \text{for all } n \in I,$$

it follows that

$$q^{\beta*\gamma*}(b_i^{-1}) = g_{i-1}^{\gamma^+} = g_i, i \in I.$$

Now, since b_i permute among themselves upon applying β, we have

$$q^{\beta*\gamma*}(y) = 1, y \neq 1, b_i^{-1}, i \in I.$$

Therefore

$$q^{\beta*\gamma*} = q.$$

This shows that $\beta * \gamma*$ maps $H = gp(b, b', q)$ onto itself. Let α be the restriction of $\beta * \gamma*$ to H, so that α is an auto-morphism of H. We have

$$h_i^\alpha = [q^{b_i}, q]^\alpha = \left[q^{\alpha^{b_i^\alpha}}, q^\alpha\right] = \left[q^{b_i^\alpha}, q\right] = \left[q^{b_{i+1}}, q\right] = h_{i+1}$$
$$(\text{ for } b^{\alpha_i} = (b^i b')^\alpha = (b^i)^\beta b'^\beta = b^i bb = b^{i+1} b' = b_{i+1}).$$

Consider $R \leq G$, where

$$R = gp(\ldots, a_{-1}, a_0)$$

In the identification of G with G^*, R is identified with **257**

$$R^* = gp(\ldots, h_{-1}, h_0).$$

Trivially,

$$R^* \Delta G^*.$$

Now by the corollary of Lemma 2, G^* is an E-subgroup of H. There is therefore an

$$S^* \Delta H, \text{ such that}$$
$$R^* = S^* \cap G^*.$$

Let

$$K = H/S^*.$$

Then

$$K = H/S^* \cong H^\alpha/S^{*^\alpha} = H/S^{*^\alpha}.$$

Now

$$S^* \geq gp(\ldots, h_{-1}^{\alpha}, h_0^{\alpha}) = gp(\ldots, h_{-1}, h_0, h_1).$$

But, **258**

$$h_1 \notin R^* = S^* \cap G^*, \text{ so that}$$
$$h_1 \notin S^*$$

Thus S^* is strictly contained in $S^{*^{\alpha}}$. We have

$$H/S^{*^{\alpha}} \cong H/S^*/S^{*^{\alpha}}/S^*.$$

Thus

$$K = H/S^{*^{\alpha}} \cong H/S^*/S^{*^{\alpha}}/S^* = K/N,$$

where $N = S^{*^{\alpha}}/S^*$ is not trivial. Evidently K is a 3-generator group. Further by Corollary 2, p. 141 of Chapter 8, since G is abelian, H and therefore K is soluble of length 3. Thus we have proved:

Theorem 4. *The group*

$$K = H/S^*$$

is a 3-generator non-Hopf group, soluble of length 3.

Bibliography

[1] Baer, Reinhold (1953) - Das Hyperzentrum einer Gruppe III. Math. Zeitschr, 59, 299-338 259

[2] Birkhoff, Garret(1935)- On the structure of abstract algebras. Proc Cambridge Philos. Soc. 31, 433-454.

[3] Boone, W. W. (1954[a])- Certain simple uusolvable problems of group theory I.Proc. K. Nederl. Akad. Wetensch. Amsterdam (A) 57, 231-237.

(1954[b])- Certain simple unsolvable problems of group theory II. Proc. K. Nederl. Akad. Wetensch. Amsterdam (A)57, 492-497.

(1955[a])- Certain simple unsolvable problems of group theory III. Proc. K. Nederl. Akao. Wetensch. AMsterdam (A) 58, 252-256.

(1955[b])- Certain simple unsolvable problems of group theory IV. Proc. K. Nederl. Akad. Wetensch. Amsterdam (A)58, 571-577.

(1957)- Certain simple unsolvable problems of group theory VI. Proc. K. Nederl. Akad. Wetensch. Amsterdam (A)60, 22-27.

(1958)- The word problem. Proc. Nat. Acad. Sc. U.S.A.44, 1061-1065.

(1959)- The word problem. Annals of Math. (70) No.2, 207-265.

[4] Britton J.L.(1956)- Soution of the word problem for certain types of groups I. Proc. Glasgow Math. Assoc. 3, 45-54.

(1957)- Soution of the word problem for certain types of groups II. Proc. Glasgow Math. Assoc. 3., 68-90.

(1958) - The word problem for groups. Proc. Lond. Math. Soc. (3) 8, 493-506.

260 [5] Burnside, W.(1902) - On an unsettled question in the theory of discontinuous groups. Journal of Pure and Applied Maths. (Lond.) 33, 230-238.

[6] Coxeter, H.S.M.and W.O.J.Moser (1957) - Generators and relations for discrete groups. (Ergebnisse der Mathematik undihrer Grenzgebiete) Springer-Verlag, Berlin, Gottingen, Heidelberg.

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

(1954[a]) - The splitting properties of relatively free groups. Proc. London Math. Soc.(3) 4, 343-356.

(1954[b]) - Finiteness conditions on soluble groups. Proc. London Math. Soc. (3)4, 419-436.

[8] Hall, P. and Graham Higman (1956)- On the p-length of p-soluble groups and reduction theorems for Burnside's problem. Proc. London Math. Soc. (3) 6, 1-42.

[9] Hall, Marshall Jr.(1959)- Solution of the Burnside problem for exponent six. Illinois J. Math. Vol.2, No.4B(1958) 764-786.

[10] Higman, Graham (1951)- A finitely related group with an isomorphic proper factor group. J. London Math. Soc. 26, 59-61.

(1956)- On finite groups of exponent five. Proc. Cambridge Philos. Soc. 52, 381-390.

[11] Higman Graham and B.H. Neumann (1952)- Groups as groupoids with one law. Publ. Math. Debrecen 2, 215-221.

[12] Higaman Graham, B.H. Neumann and Hanna Neumann(1949)- Embedding theorems for groups. J. London Math. Soc. 24, 247-254.

[13] Hirsh, K. A.(1938[a])- On infinite soluble groups I. Proc. London Math. Soc. (2) 44, 53-60.

(1938[b])- On infinite soluble groups II. Proc. London Math. Soc. (2) 44, 336-344.

[14] Hirsch K.A. (1946) - On infinite soluble groups III. Proc. London **261**
Math. Soc. (2) 49, 184-194.

(1952)- On finfinite soluble groups IV. J. London math. Soc. 27, 81-85.

(1954)- On infinite soluble groups V. J. London Math. Soc. 29, 250-254.

[15] Kaloujnine, Leo(1948)- La struture des p-groupes des sylow des groupes symetriques finis. Ann. Sci. Ecole Norm. Sup. (3) 65, 239-276.

[16] Kaloujnine, Leo and Marc Krasner (1950)- Produit complet des groupes de permutations et probleme d'extension des roupes, Acta. Sci. Math. Szeged. Vol.13, 208-230.

(1951) - Produit complet des groupes de permutations et probleme d' extension des groupes, Acta Sci. Math. Szeged. Vol. 14, 39-66,69-82.

[17] Kostriken, A. I.(1955)- Solution of the restricted Burnside problem for exponent five, Izv. Akad. Nauk SSSR, Ser., at. 19, 233-244(Russian)

(1959)- On Burnside's problems. Izv. Akad. Nauk SSSR Ser Mat. (23), 3-34(Russian).

[18] Kurosh, A.G. (1955)- Theory of groups. Chelsea Publ, Co., New York, N.Y., Vol. I.

(1956)- Theory of groups. Chelsea Publ. Co., New York, N.Y., Vol. II.

[19] Levi, F. and B.L.van der Waerden (1933)- Über eine besondere Klasse von Gruppen Abh. Math. Sem. Hamburg, 154-158.

[20] Lyndon, R.C. (1952)- Two notes on nilpotent groups. Proc. Amer. Math. Soc. 3, 579-583.

[21] Magnus, Wilhelm (1932)- Oas Identitatsproblem fou Gruppen miteiner definierenden Relation, Math. Ann. 106, 295-307.

(1935)- Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. Math. Ann. 111, 259-280.

262 [22] Neumann, B.H.(1937^a) - Identical relations in groups I. Math. Ann. 114, 506-525.

(1937^b)- Some remarks on infinite groups. J. London Math. Soc. 12, 120-127.

(1950)- A two-generator group isomorphic to a proper factor group. J. London Math. Soc. 25, 247-248.

(1953)- On a problem of Hopf. J. London Math.Soc. 28, 351-353.

(1954)- An essay on free products of guoups with amalgamations. Phil. Trans. Roy. Soc. London. A, 246, 503-545.

(1956)- On some finite groups wiht trivial multiplicator. Publ. Math. Debrecan 4, 186-194.

[23] Neumann, Hanna (1957)- Generalised free products with amalgamated subgroups I. Amer. J. MATH. 70, 590-625.

(1949)- Generalised free products with amalgamated subgroups II. Amer. J. Math. 71, 491-540.

(1950)- Generalised free sums of cyclical groups. Amer. J. Math. 72. 671-685.

(1951)- On an amalgam of abelian groups. J. London Math. Soc. 26, 228-232.

(1956)- On varieties of groups and their associated near rings. Math. Math. Zeitschr. 65, 36-69.

[24] Neumann, B.H. and Hanna Neumann(1950)- A remark on generalised free products. J. London Math. Soc. 25, 202-204.

(1950-51)- Zwei Klassen charakteristischer unterguppen und ihre factor gruppen. Math. Nach. 4, 106-125.

(1953)- A contribution to the embedding theory of group amalgams. Proc. London Math. Soc. (3), 3, 245-256.

(1959)- Embedding theorems for groups. J. London Math. Soc. 34, 465-479.

[25] Newman, H.H.A. (1942) - On theories with a combinatorial defi- **263**
nition of "equivalence". Annals of Math, 43, 223-243.

[26] Novikov, P.S.(1952)- On the algorithmic unsolvability of the identity problem. Doklady Akad. Nauk SSSR 85, 709-712(Russian).

(1955)- On the algorithmic unsolvability of the word problem in group theory. Trudy Mat. Inst. im. Steklov No.44, Izdat, Akad. Nauk. SSSR 143 p.p. (Russian). = Amer. Math. Transl. seies 2, Vol.9 (1958)1-122.

(1959)- On periodic group. Doklady Akad. Nauk. SSSR 127, 749-752 (Russian).

[27] Polya, George(1937)- Kombinatorische Anzahlbestimmungen fur Group, Graphen und Chemische Verbindungen Acta Math. 68, 145-253.

[28] Sanov, I.N.(1940)- Solution of Burnside problem for exponent four. Ucenye Zapiski Leningrad Univ. 55, 16-170 (Russian).

(1947)- On the Burnside Problem. Dklady Akad. Nauk. SSSR 57, 759-761(Russian).

[29] Schiek, Helmut(1956)- Ahnlichkeitsanalyse von Gruppenrelationen. Acta Math. (96), 157-252.

[30] Schreier, Otto(1927)- Die Untergruppen der freien Gruppen. Abh. Math. Sem. Hamburg, 5, 161-183.

[31] Specht Wilhelm(1932)-Eine Verallgemeinerung der symmetrischen Gruppen. Schriften d. Math. sem. u.d. Inst. F. angew. Math. d. Univ. Berlin 1,4,1.

[32] Tartakovskiiu, V. A.(1949^{a})- The sieve method in the theory of group. Mat. Sb. N. S. 25(67), 3-50 (Russian). = Amer. Math. Soc. Transl. No. 60(1952),

264 (1949^{b}) - Application of the sieve method to the solution of the word problem in certain types of group. Math. Sb. W. S. 25(67), 251-274(Russian). = Amer. Math. Soc. Transl. No.60(1952), 63-92.

(1949^{c})- Solution of the word problem for groups with a k-reducible basis for $k > 6$, Izv. Akad. Nauk. SSSr Ser. Mat. 13, 43-494 (Russian). = Amer. Math. Soc. Transl. No. 60(1952), 93-110.

(1952)- On primitive composition. Mat. Sb. N.S. 30(72), 39-52 (Russian).

[33] Wiegold, James(1959)-Nilpotent products of groups with amalgemations. Publ. Math. Debrecen 6, 131-168.

[34] Wielandt, Helmut(1939)- Eine Verallgemeinerung der Untergruppen. Math. Zeitscher. 45, 209-244.

[35] Zassenhaus, Hans J.(1958)- The theory of group. Chelsea Publ. Co., New York.