E. Spitznagel
Math. Dept.

LECTURE NOTES ON GROUP THEORY

BY

PHILIP HALL

I. Elements of Group Theory.

§1. The laws of group theory. The symmetric groups.

(A). The theory of groups originated in the study of the permutations of a finite set of objects: for example, the roots of an algebraic equation; or the faces, edges and vertices of a regular solid. From this beginning the concept of a group was derived by abstraction, that is to say by the elimination of inessentials, in the following way.

A <u>permutation</u> α of a set X (which need not be finite) is by definition any mapping

$$x \longrightarrow x\alpha \qquad (x \in X)$$

of X into itself with these two properties: (i) $x\alpha = y\alpha$ implies $x = y$; and (ii) every y in X has the form $x\alpha$ for some $x \in X$. (i) states that the mapping α is <u>one-to-one</u> and implies that the solution x of the equation $y = x\alpha$ in (ii) is for given y unique. Therefore with every permutation α of X there is associated another permutation α^{-1}, the <u>inverse</u> of α, defined by the rule that $y\alpha^{-1} = x$ whenever $x\alpha = y$.

The number of elements in a set X is denoted by $|X|$. If this number is finite, the two properties (i) and (ii) are equivalent: each implies the other.

The set of all ~~possible~~ permutations of X is denoted by $\Sigma(X)$ and is called the <u>symmetric group</u> on X. If $|X| = n$ is finite, then $|\Sigma(X)| = n!$

Let α and β be in $\Sigma(X)$. Their <u>product</u> $\alpha\beta$ is the mapping of X defined by

$$x(\alpha\beta) = (x\alpha)\beta \qquad (x \in X).$$

It is the result of applying first α, then β; and it is also a permutation of X. Thus the set $\Sigma(X)$ is closed with respect to two operations: (i) inversion, which is a singulary operation; and

(ii) multiplication, a binary operation.

These two operations satisfy the following laws:

I. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$, the associative law of multiplication;

II. $(\alpha^{-1})^{-1} = \alpha$;

III. $(\alpha\alpha^{-1})\beta = \beta = \beta(\alpha\alpha^{-1})$, the law of cancellation.

Note that the product $\alpha\alpha^{-1}$ is the <u>identity</u> mapping of X which maps each element of X into itself. In these laws, α, β and γ are arbitrary permutations of X.

(B). Now let G be any non-empty set in which "inverses" and "products" have been defined. Provided the laws I, II and III hold for all α, β and γ in G, then G is called a <u>group</u>.

The notations α^{-1}, $\alpha\beta$ are the conventional ones used in the general theory of groups. They are not necessarily the most appropriate in every particular instance. For example, in the set Q of all rational integers, "negatives" and "sums" are defined, and the laws

I^{+}. $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$;

II^{+}. $-(-\alpha) = \alpha$;

III^{+}. $(\alpha+(-\alpha))+\beta = \beta = \beta+(\alpha+(-\alpha))$

hold for all α, β and γ in Q. We express this by calling Q an <u>additive group</u>. The distinction between additive groups like Q and multiplicative groups like $\Sigma(X)$ is not one of principle, but merely of notation.

(C). Some easy consequences of the group-laws I, II and III are to be noted.

<u>Lemma 1.1</u> In any group G, the element $\xi\xi^{-1}$ is independent of the choice of ξ in G. It is called the <u>unit element</u> of G and usually denoted by 1.

The unit element of $\Sigma(X)$ is the identity mapping of X. In an additive group like Q, one speaks of the <u>zero element</u> rather than the unit element, and the notation is 0, not 1. Thus

$\xi + (-\xi) = 0$ for all $\xi \in Q$.

Lemma 1·2. Given elements $\xi_1, \xi_2, \ldots, \xi_n$ in a group G, not necessarily distinct, their product in the given order is a uniquely determined element $\xi_1 \xi_2 \ldots \xi_n$ of G and does not depend on the precise way in which the multiplication is carried out.

For example, when $n = 4$, there are five ways of calculating $\xi_1 \xi_2 \xi_3 \xi_4$ viz. $((\xi_1 \xi_2)\xi_3)\xi_4$, $(\xi_1 \xi_2)(\xi_3 \xi_4)$, $(\xi_1 (\xi_2 \xi_3))\xi_4$, $\xi_1((\xi_2 \xi_3)\xi_4)$ and $\xi_1(\xi_2(\xi_3 \xi_4))$. The associative law I ensures that all five give the same answer. Thus, in writing products of three or more elements of a group, brackets may be dispensed with.

However, the ordering of the factors is usually important. In general $\xi\eta \neq \eta\xi$. If it should happen that $\xi\eta = \eta\xi$, then the elements ξ and η are said to commute. Groups in which every pair of elements commute form a very special class called Abelian groups after N.H. Abel 1802-29. Groups, like Q above, which are written in additive notation are nearly always Abelian.

The powers of an element α of a group are defined inductively by the equations

$$\alpha^0 = 1, \quad \alpha^1 = \alpha, \quad \alpha^{n+1} = \alpha^n . \alpha, \quad \alpha^{-n-1} = \alpha^{-n} . \alpha^{-1}$$

for $n = 1, 2, 3, \ldots$

Lemma 1·3. For all m, n in Q, we have

$$\alpha^m \alpha^n = \alpha^{m+n} = \alpha^n \alpha^m \; ; \; (\alpha^m)^n = \alpha^{mn}.$$

If α and β commute, we also have $(\alpha\beta)^m = \alpha^m \beta^m$.

(D). The most significant deduction from the group laws is

Theorem 1.4. Let α be an element of the group G. Then the mapping $r(\alpha)$ of G defined by

$$r(\alpha) : \xi \to \xi\alpha \qquad (\xi \in G)$$

is a permutation of G, i.e. $r(\alpha) \in \Sigma(G)$. Also, $r(\alpha\beta) = r(\alpha)r(\beta)$ and $r(\alpha^{-1}) = r(\alpha)^{-1}$. Finally, $r(\alpha) = r(\beta)$ only if $\alpha = \beta$.

This theorem brings us back to permutations from which we started. The statement that $r(\alpha) \in \Sigma(G)$ means that, for given α and β in G, the equation $\xi\alpha = \beta$ has always a unique solution ξ in G. This unique ξ is $\beta\alpha^{-1}$. For $\xi\alpha = \beta$ implies that $\beta\alpha^{-1} = (\xi\alpha)\alpha^{-1} = \xi(\alpha\alpha^{-1})$ by I, $= \xi$ by III; while $(\beta\alpha^{-1})\alpha = \beta(\alpha^{-1}\alpha)$ by I, $= \beta$ by III, since $\alpha = (\alpha^{-1})^{-1}$ by II.

$r(\alpha)$ is the operation of multiplying the elements of G on the right by α. The operation $l(\alpha)$ of multiplying the elements of G on the left by α is also a permutation of G, because for given α and β in G, the equation $\alpha\eta = \beta$ always has the unique solution $\eta = \alpha^{-1}\beta \in G$ However $l(\alpha\beta) = l(\beta)\,l(\alpha)$ which is different from $l(\alpha)\,l(\beta)$ unless α and β commute. If G is Abelian, $l(\alpha) = r(\alpha)$ for all $\alpha \in G$.

The permutations $r(\alpha)$ and $l(\alpha)$ with $\alpha \in G$ are called the right and left translations of G. Obviously $r(1) = l(1)$ is the identity mapping of G. The word "translation" is a reminder that, if $\alpha \neq 1$, $r(\alpha)$ and $l(\alpha)$ leave no element of G invariant. For example, $\xi\alpha = \xi$ implies $\alpha = \xi^{-1}\xi = 1$.

The law of inversion for products of group elements

Lemma 1.5 $(\xi_1\xi_2\cdots\xi_n)^{-1} = \xi_n^{-1}\cdots\xi_2^{-1}\xi_1^{-1}$.

(E) Inverses and products can be defined in a natural way for arbitrary subsets $A, B, X_1, X_2, \dots$ of a group G.

A^{-1} is the set of all inverses α^{-1} of the elements $\alpha \in A$; while AB is the set of all elements ξ of G which are expressible (in at least one way) in the form $\xi = \alpha\beta$ with $\alpha \in A$, $\beta \in B$.

The laws I, II and 1.5 extend at once to these operations on subsets:

$$(AB)C = A(BC) \; ; \; (A^{-1})^{-1} = A \; ; \; (X_1 X_2 \dots X_n)^{-1} = X_n^{-1} \dots X_2^{-1} X_1^{-1}.$$

But law III applies to subsets only in exceptional cases.

The inversion $\alpha \to \alpha^{-1}$ $(\alpha \in G)$ is a permutation of G whose square is the identity. Since it is a permutation, we have $|A^{-1}| = |A|$. By 1.4 we also have

Lemma 1.6 For all subsets A, B and all elements ξ, η of a group we have $|A\xi| = |A|$, $|\eta B| = |B|$.

Obviously $|AB| \leq |A| \cdot |B|$.

§2. Subgroups, Cosets and Indices, Quotient Groups.

(A). If a non-empty subset H of a group G is closed with respect to the inversion and multiplication in G, it forms a group in its own right. For the group laws I, II and III hold in G and therefore certainly hold also in H. Such a subset is called a subgroup of G. The study of particular groups is largely bound up with the discovery and study of the subgroups they contain.

Let H be a subgroup of G and let $\alpha \in H$. Then $\alpha^{-1} \in H$ and so $\alpha\alpha^{-1} = 1 \in H$. Every subgroup H of G contains the unit element of G and this is at the same time the unit element of H. Since $1^{-1} = 1.1 = 1$, the unit element taken by itself is a subgroup, the unit subgroup of G. We do not need to make a pedantic distinction between the unit element 1 of G and the unit subgroup which has 1 as its sole element.

Lemma 2.1 Let $(H_\lambda)_{\lambda \in \Lambda}$ be any family of subgroups of a group G. Then their intersection

$$H = \bigcap_{\lambda \in \Lambda} H_\lambda$$

is also a subgroup of G.

For H contains 1 and so it is not empty. And it inherits the requisite closure properties from the subgroups H_λ.

Note that the intersection of two sets X and Y is usually written $X \cap Y$.

(B). Let X be any subset of G. The intersection of all the subgroups of G which contain X is called the subgroup <u>generated</u> by X and written $\{X\}$. It is the smallest subgroup of G which contains X.

<u>Lemma 2.2</u> If X is not empty, $\{X\}$ consists of all elements of G which are expressible in at least one way as a product of elements of the set $X \cup X^{-1}$.

Here $X \cup Y$ is the <u>union</u> of the sets X and Y and consists of all elements which belong to at least one of these two sets. Obviously $\{X\}$ must contain all products of elements of $X \cup X^{-1}$. But the set of all such products is closed with respect to multiplication, and also by 1.5 with respect to inversion. Hence it is a subgroup containing X, and contained in $\{X\}$. Therefore it coincides with $\{X\}$ by definition.

If $H, K, L, \ldots$ are subgroups of G, then $\{H \cup K \cup L \cup \ldots\}$ is usually written $\{H, K, L, \ldots\}$. It is the <u>join</u> of $H, K, L, \ldots$; the smallest subgroup which contains them all.

If $P(\xi, \eta, \ldots)$ is a proposition involving certain elements $\xi, \eta, \ldots$ of a group, then $\{\xi, \eta, \ldots ; P(\xi, \eta, \ldots)\}$ denotes the subgroup generated by all $\xi, \eta, \ldots$ for which $P(\xi, \eta, \ldots)$ is true.

A subset X of a group G such that $\{X\} = G$ is called a <u>set of generators</u> of G. Such a set can usually be chosen in many different ways. $X = G$ is always a possible choice.

A group which can be generated by a single element is called <u>cyclic</u>. Every element ξ of a group G generates a cyclic subgroup $\{\xi\}$ and 1.3 shows that this consists of all the powers ξ^n of ξ. $n = 0, \pm 1, \pm 2, \ldots$; it shows also that all cyclic groups are Abelian.

(C). If G is a group, $|G|$ is called the order of G. Unless the contrary is stated, all groups considered will be finite. If $\xi \in G$, the order of $\{\xi\}$ is also called the order of ξ.

Let H be a subgroup of G. The sets $H\xi$ with $\xi \in G$ are called the cosets of H in G. If X is any subset of G, the set HX is the union of a certain number of cosets of G and this number is denoted by $|HX : H|$. This notation is justified by

Lemma 2·3 Distinct cosets of H in G have no common element. $|HX| = |HX : H| \cdot |H|$ for any subset X of G.

Proof: Let $\zeta \in H\xi$. Then $\zeta = \eta\xi$ with $\eta \in H$. Hence $\xi = \eta^{-1}\zeta \in H\zeta$ since $\eta^{-1} \in H$. But H contains 1 and is closed with respect to multiplicati Hence $HH = H$ and so $H\xi = H\zeta$. Therefore if two cosets $H\xi$ and $H\xi'$ have an element ζ in common, they both coincide with $H\zeta$. By 1·6, $|H\xi| = |H|$ for all $\xi \in G$ and so $|HX| = |HX : H| \cdot |H|$ by definition of $|HX|$.

Obviously $G = HG$. The number $|G : H|$ is the total number of cosets of H in G. It is called the index of H in G. An immediate corollary of 2·3 is

Theorem 2·4 Let H be a subgroup of G. Then $|G| = |G : H| \cdot |H|$. The order of H and also its index in G divides the order of G. In particular, the order of every element of G divides $|G|$.

(D). This theorem is usually attributed to J. L. Lagrange 1736–1813. For cyclic groups, a much more precise result holds good. This is

Theorem 2·5 Let $G = \{\xi\}$ be a cyclic group of order n. Then the n elements of G are $1, \xi, \xi^2, \cdots, \xi^{n-1}$; and $\xi^n = 1$. For each divisor d of n, G has one and only one subgroup of order d viz. $\{\xi^{n/d}\}$ with elements $1, \xi^{n/d}, \xi^{2n/d}, \ldots, \xi^{(d-1)n/d}$. All subgroups of a cyclic group are cyclic.

Note that ξ^n is the first positive power of ξ which is equal to 1. $\xi^N = 1$ if and only if N is a multiple of n. $\xi^l = \xi^m$ if and only if

$l \equiv m \mod n$. For this reason, the order n of a cyclic group $\{\xi\}$ is often called the <u>period</u> of ξ.

Suppose $\xi \in \Sigma(X)$, and let $x \in X$. If r is the least positive integer such that $x\xi^r = x$, then the elements $x, x\xi, x\xi^2, \ldots, x\xi^{r-1}$ are all distinct. They form a <u>cycle</u> of ξ of order r. If $y = x\xi^k$, the cycle $y, y\xi, \ldots, y\xi^{r-1}$ differs from this only superficially; they contain the same r elements of X in the same cyclic order. As cycles, they are to be considered the same. On this understanding, distinct cycles of ξ contain no common term. The n elements of X fall into a certain number of cycles of ξ which are mutually disjoint. If the orders of these cycles are $r_1, r_2, \ldots, r_k$ then $n = \sum r_i$. The numbers $r_1, \ldots, r_k$ are the parts of a <u>partition</u> of n and this partition is called the <u>cycle-type</u> of the permutation ξ. Obviously the order or period of ξ is the least common multiple of the orders of its cycles. Note that this l.c.m. divides $n!$ the order of $\Sigma(X)$.

If a partition contain m_1 parts equal to 1, m_2 parts equal to 2 and so on, it is usually denoted by the symbol $(1^{m_1}2^{m_2}\ldots)$. It is a partition of the number $m_1 + 2m_2 + 3m_3 + \cdots$

(E). Transversals. Let K be a subgroup of the group G. A subset T of G which contains exactly one element from each coset of K in G is called a transversal to K in G. Now ξ and η lie in the same coset of K if and only if $\xi\eta^{-1} \in K$. For T to be transversal to K in G it is therefore necessary and sufficient that

$$G = KT \quad \text{and} \quad K \cap TT^{-1} = 1.$$

Now let

$$H = H_0 \leqq H_1 \leqq \cdots \leqq H_r = G$$

be a chain of subgroups of G each contained in the next. (Here $X < Y$ means that the set X is a proper part of the set Y; $X \leqq Y$ that X is contained in Y.) Then we have the product law of indices:

Lemma 2.6 $$|G : H| = \prod_{i=1}^{r} |H_i : H_{i-1}|.$$

Proof: By induction we may assume $r = 2$. Suppose then that K is a subgroup of G containing H. Let T be a transversal to K in G and let S be a transversal to H in K. Then $G = KT$ and $K = HS$ so that $G = HST$. Hence $|G : H| \leqq |ST| \leqq |S| \cdot |T|$.

Suppose that $\sigma_1\tau_1$ and $\sigma_2\tau_2$ lie in the same coset of H, where $\sigma_i \in S$, $\tau_i \in T$, $i = 1, 2$. Then $\sigma_1\tau_1\tau_2^{-1}\sigma_2^{-1} \in H$ and so $\tau_1\tau_2^{-1} \in \sigma_1^{-1}H\sigma_2$ which is contained in K since $S \leqq K$, $H \leqq K$. Hence $\tau_1\tau_2^{-1} \in K$ and so $\tau_1 = \tau_2$ since T is transversal to K. It follows that $\sigma_1\sigma_2^{-1} \in H$ and so $\sigma_1 = \sigma_2$ since S is transversal to H. Thus we obtain $|G : H| = |ST| = |S| \cdot |T|$. Since $|S| = |K : H|$ and $|T| = |G : K|$, the result follows. Note that ST is a transversal to H in G.

The word transversal will sometimes be used in a more general sense. If η is an equivalence relation defined on a set X, then X splits up into the union of a number of disjoint non-empty subsets, the η-classes, each of which consists of all $x \in X$ equivalent under η to some fixed element of X. A transversal to the η-classes is any subset of X which contains just one number from each η-class.

(F) The product HK of two subgroups H and K is contained in but usually distinct from their join $\{H, K\}$. This is one of the more awkward facts of group theory. Since H and K both contain 1, HK contains both H and K. Hence $HK = \{H, K\}$ if and only if HK is a subgroup. For this there is a simple criterion:

Lemma 2.7 HK is a subgroup if and only if $HK = KH$.

Proof: Suppose HK is a subgroup. Then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Conversely, let $HK = KH$. Then $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$ and $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$. So HK is closed with respect to inversion and multiplication: it is a subgroup.

Two subgroups H and K for which $HK = KH$ are called *permutable*. This does not imply that their elements commute. We also call two subsets X and Y of a group permutable if $XY = YX$.

The most important subgroups of a group are usually those which are permutable with every subset. These are called *normal subgroups*. In order that a subgroup H of the group G shall be a normal subgroup of G it is necessary and sufficient that

$$H\xi = \xi H$$

for all $\xi \in G$. Now $(H\eta)^{-1} = \eta^{-1}H^{-1} = \eta^{-1}H$. Sets of the form ξH with $\xi \in G$ may therefore be called *inverse cosets* of H in G. Two distinct inverse cosets of H have no common element. The condition for H to be normal in G is the cosets of H in G shall be the same as the inverse cosets. The normality relation is denoted by

$$H \triangleleft G.$$

~~A fundamental consequence of normality is~~

Theorem 2.8. If $H \triangleleft G$, then the cosets of H in G form a group G/H called the *quotient group* of G by H

Since $H \triangleleft G$, we have $(H\xi)^{-1} = \xi^{-1}H = H\xi^{-1}$ and $(H\xi)(H\eta) = H(\xi H)\eta = H(H\xi)\eta = (HH)\xi\eta = H\xi\eta\lambda$ for all ξ, η in G. The set G/H whose elements are the $|G:H|$ distinct cosets of H in G is therefore closed with respect

It should be read "H is a normal subgroup of G" or "H is normal in G." A fundamental fact is stated in

Theorem 2·8. Let $H \lhd G$. Then

$$(H\xi)^{-1} = H\xi^{-1} \quad \text{and} \quad (H\xi)(H\eta) = H\xi\eta$$

for all ξ and η in G. The set G/H whose elements are the cosets of H in G is a group. It is called the quotient group of G by H.

For $(H\xi)^{-1} = \xi^{-1}H = H\xi^{-1}$ and $H\xi\, H\eta = HH\xi\eta = H\xi\eta$. These equations show that G/H is closed with respect to inversion and multiplication Laws I and II hold for arbitrary subsets of G. As for law III, we need only note that $(H\xi)(H\xi)^{-1} = H\xi\, H\xi^{-1} = H\xi\xi^{-1} = H$ for all $\xi \in G$ and $H(H\eta) = H\eta = (H\eta)H$ for all $\eta \in G$. Thus III also holds in G/H. So G/H is a group whose unit element is the subgroup H itself. The unit subgroup of G/H is more appropriately denoted by H/H.

The unit subgroup 1 of G is normal in G and $G/1$ need not be distinguished from G itself. We also have $G \lhd G$ and G/G is a unit group with only one element.

If $G \neq 1$ and has no normal subgroups other than 1 and G it is called simple. For example, if $|G| = p$ is a prime, then $G = \{\xi\}$ for every $\xi \neq 1$ in G by 2·4. So G is cyclic and has no subgroups at all other than 1 and G. The discovery and study of simple groups of composite order is one of the most interesting but also one of the most difficult parts of group theory.

By way of contrast, in an Abelian group every subgroup is normal.

Quotient groups H/K, where H is a subgroup of G and $K \lhd H$, are called sections of G, following Wielandt. Their study is an essential adjunct to the investigation of the subgroups of G.

§3. Isomorphic Groups and Homomorphic Mappings.

(A). Let G and Γ be groups and let f be a mapping of G into Γ, or (what it the same thing) a function whose argument ranges through G and whose values lie in Γ. If

$$f(\xi\eta) = f(\xi)f(\eta) \qquad (1)$$

for all ξ, η in G, then f is called homomorphic; it is also called a homomorphism of G into Γ.

Taking $\eta = 1$, we find that, if f is homomorphic, then $f(1)$ is the unit element of Γ. Taking $\eta = \xi^{-1}$, we deduce that

$$f(\xi^{-1}) = f(\xi)^{-1}. \qquad (2)$$

The image of G under f is the set $f(G)$ of all $f(\xi)$ with $\xi \in G$. $f(G)$ is a subgroup of Γ. If $f(G) = \Gamma$, then f is said to map G onto Γ: it is an epimorphism. On the other hand, if $f(\xi) = f(\eta)$ implies $\xi = \eta$, then f is a one-to-one mapping: it is a monomorphism. If f is both an epimorphism and a monomorphism, then it is called as isomorphism of G onto Γ. In this case, the inverse mapping f^{-1} exists and this will be an isomorphism of Γ onto G.

Two groups G and Γ are called isomorphic if there exists an isomorphism f mapping one onto the other. This relation is written

$$G \cong \Gamma.$$

The isomorphism f allows us to translate any group-theoretical statement about G into a corresponding statement about Γ. Conversely, using f^{-1}. Hence isomorphic groups are simply copies of each other. They have the same order and their subgroups can be put in one-to-one correspondence, with normal subgroups corresponding to normal subgroups, joins and intersections being preserved and so on. We may describe them as instances of the same type of group. For example, cyclic groups of the same order are isomorphic. If $|X| = |Y|$, then $\Sigma(X) \cong \Sigma(Y)$.

Evidently, a monomorphism f of G into Γ is at the same time an isomorphism of G onto $f(G)$, which is a subgroup of Γ.

From 1.4 we have

Theorem 3.1. For any group G, the mapping

$$\xi \to r(\xi) \qquad (\xi \in G)$$

is a monomorphism of G into $\Sigma(G)$, called the regular representation of G. Thus $G \cong r(G)$; every group is isomorphic with a permutation group.

This remark is due to A. Cayley 1821-95. Note that the mapping

$$\xi \to l(\xi^{-1}) \qquad (\xi \in G)$$

is also a monomorphism of G into $\Sigma(G)$.

Another example follows from 2.8. This is

Theorem 3.2 Let $H \lhd G$. Then the mapping

$$\xi \to H\xi \qquad (\xi \in G)$$

is an epimorphism of G onto G/H. This is called the natural epimorphism

(B). Every homomorphism can be analysed into a natural epimorphism followed by a monomorphism. If G and Γ are groups, let

$$\mathrm{Hom}(G, \Gamma)$$

denote the set of all possible homomorphisms of G into Γ. Suppose that $f \in \mathrm{Hom}(G, \Gamma)$, and let $f(\xi) = f(\eta)$. Then $f(\xi\eta^{-1}) = 1$, the unit element of Γ, by (1) and (2). Conversely $f(\xi\eta^{-1}) = 1$ implies $f(\xi) = f(\eta)$. The set K of all $\xi \in G$ such that $f(\xi) = 1$ is called the kernel of f. For any $\eta \in G$ and $\xi \in K$, we have $f(\eta^{-1}\xi\eta) = f(\eta)^{-1} f(\xi) f(\eta) = 1$ since $f(\xi) = 1$. Hence $\eta^{-1} K \eta = K$ or $K\eta = \eta K$ for all $\eta \in G$. Since K is clearly a subgroup of G, it follows that $K \lhd G$. And $f(\xi) = f(\eta)$ if and only if ξ and η belong to the same coset of K. Hence we have a one-to-one mapping

$$K\xi \to f(\xi)$$

of the cosets of K onto the elements of $f(G)$. Since K is normal in G

$K\xi\, K\eta = K\xi\eta \to f(\xi)f(\eta) = f(\xi\eta)$. So this mapping is an isomorphism of G/K onto $f(G)$. This gives

Theorem 3.3. If f is any homomorphism of G with kernel K, then $K \lhd G$ and $G/K \cong f(G)$.

Thus the mapping $\xi \to f(\xi)$, $\xi \in G$, is the product of the natural epimorphism $\xi \to K\xi$ of G onto G/K, followed by the isomorphism $K\xi \to f(\xi)$ of G/K onto $f(G)$.

Theorem 3.4 Let H be any subgroup of G and let $K \lhd G$. Then KH is a subgroup of G and $K \cap H \lhd H$ and

$$H/K\cap H \cong KH/K.$$

Proof: since $K \lhd G$, it is permutable with H. So KH is a subgroup of G by 2.7. Obviously $K \lhd KH$. Let f be the restriction to H of the natural epimorphism of G onto G/K. Then $f(H) = KH/K$. Since f is a homomorphism of H with kernel $K\cap H$, the result follows from 3.3. It is usually called the first isomorphism theorem.

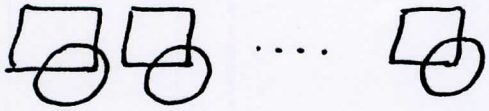
(C). If $K \lhd G$ and L is any subgroup of G containing K, then $K \lhd L$ and L/K is a subgroup of G/K. Every subgroup of G/K is of this form. Moreover $L \lhd G$ if and only if $L/K \lhd G/K$. Now if $L \lhd G$, the product f of the natural epimorphisms of G onto G/K and of G/K onto $\Gamma = (G/K)/(L/K)$ maps any element ξ of G onto that element $f(\xi)$ of Γ which contains $K\xi$ as as one of its members. Thus $f(\xi)$ is simply $L\xi$ considered not as a set of elements of G but as a union of certain cosets of K. Comparing f with the natural epimorphism of G onto G/L we obtain

Theorem 3.5 Let K and L be normal subgroups of G such that L contains K. Then

$$G/L \cong (G/K)/(L/K).$$

This rather obvious fact is sometimes known as the second isomorphism theorem.

(D). Let H/K and L/M be two sections of the group G. There is one simple case where we can be sure that $H/K \cong L/M$. This is when each element $K\eta$ $(\eta \in H)$ of H/K "meets" (has non-empty intersection with) exactly one element $M\lambda$ $(\lambda \in L)$ of L/M and when conversely each element of L/M meets exactly one element of H/K. The situation is like this:



where for example the squares represent elements of H/K and the circles elements of L/M. Two sections related in this way are called <u>incident</u>. If we make each $K\eta$ $(\eta \in H)$ correspond to the unique $M\lambda$ $(\lambda \in L)$ which it meets, we obtain an isomorphism of H/K onto L/M. Thus incident sections are isomorphic.

Now let H/K and L/M be any two sections of G. By 3·4, $L^* = K(L \cap H)$ is a subgroup of H because $K \lhd H$. Similarly $M^* = K(M \cap H)$ is a subgroup and $K \leqq M^* \leqq L^* \leqq H$. By 3·4 again, $M \cap H \lhd L \cap H$ because $M \lhd L$. Hence if $\eta \in L \cap H$ we have $\eta K = K\eta$ and $\eta(M \cap H) = (M \cap H)\eta$. Consequently $\eta M^* = M^* \eta$. But $K \leqq M^*$ and so every element of K is also permutable with M^*. It follows that every element of $L^* = K(L \cap H)$ is permutable with M^*. Consequently $M^* \lhd L^*$.

We call the quotient group L^*/M^* the <u>projection</u> of L/M in H/K. [illegible]

Similarly we can form the projection $H^\dagger/K^\dagger$ of H/K in L/M. Here $H^\dagger = M(H \cap L)$ and $K^\dagger = M(K \cap L)$. Then we have the Zassenhaus Lemma:

<u>Theorem 3·6</u> If H/K and L/M are any two sections of a group, then their projections L^*/M^* and $H^\dagger/K^\dagger$ in each other are incident. Hence we have

$$K(L \cap H)/K(M \cap H) \cong M(H \cap L)/M(K \cap L).$$

Proof : Since $K \leq M^* \leq L^*$, we have $L^* = M^*(L \cap H)$ and every element of L^*/M^* has the form $M^*\lambda$ with $\lambda \in L \cap H$. Similarly every element of $H^\dagger/K^\dagger$ has the form $K^\dagger\lambda$ with $\lambda \in L \cap H$. Hence each element of L^*/M^* "meets" some element of $H^\dagger/K^\dagger$ and vice versa.

Suppose $K^\dagger\lambda$ meets both $M^*\lambda_1$ and $M^*\lambda_2$ where λ, λ_1 and λ_2 are in $L \cap H$. Since $M \lhd L$, we have $K^\dagger = M(L \cap K) = (L \cap K)M$ and so $\kappa_1\mu_1\lambda \in M^*\lambda_1$ and $\kappa_2\mu_2\lambda \in M^*\lambda_2$ for some κ_1, κ_2 in $L \cap K$ and some μ_1, μ_2 in M. Hence $(\kappa_1\mu_1\lambda)(\kappa_2\mu_2\lambda)^{-1} = \kappa_1\mu_1\mu_2^{-1}\kappa_2^{-1} \in L^* \leq H$ and so $\mu_1\mu_2^{-1} \in M \cap H$. Since $K \lhd H$, it follows that $\kappa_1\mu_1\mu_2^{-1}\kappa_2^{-1} \in K(M \cap H) = M^*$. Hence $M^*\lambda_1 = M^*\lambda_2$ and $K^\dagger\lambda$ meets only one element of L^*/M^*. Similarly each element of L^*/M^* meets only one element of $H^\dagger/K^\dagger$. Thus the two projections are incident, as stated.

The first isomorphism theorem is a special case of the Zassenhaus Lemma, viz. the case $H = G$, $M = 1$.

(E). Let

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_r = G. \qquad (1)$$

Such a chain of subgroups is called a series of G; each term is normal in the next. Let

$$1 = L_0 \lhd L_1 \lhd \cdots \lhd L_s = G \qquad (2)$$

be any other series, also going from 1 to G. Let

$$L_{ij} = H_{j-1}(L_i \cap H_j) \quad \text{and} \quad H_{ji} = L_{i-1}(H_j \cap L_i).$$

Then we obtain two new series :

$$1 = L_{01} \lhd L_{11} \lhd \cdots \lhd L_{s1} = H_1 = L_{02} \lhd L_{12} \lhd \cdots \lhd L_{s2} = H_2 = L_{03} \lhd \cdots$$
$$\cdots \lhd L_{s,r-1} = H_{r-1} = L_{0r} \lhd L_{1r} \lhd \cdots \lhd L_{sr} = H_r = G \qquad (3)$$

and $$1 = H_{01} \lhd H_{11} \lhd \cdots \lhd H_{r1} = L_1 = H_{02} \lhd \cdots \lhd H_{rs} = L_s = G. \qquad (4)$$

Since each term of (1) occurs also in (3), we call (3) a refinement of (1). It is obtained from (1) by the insertion of more terms. Similarly (4) is a refinement of (2).

The number r is called the length of the series (1) and the

r groups H_j / H_{j-1} $(j=1, 2, \dots, r)$ are called factor groups of G : they are the factors of the series (1). The series (2) is of length s and its factors are the s groups L_i/L_{i-1} $(i=1, 2, \dots, s)$. The two series (3) and (4) have the same length rs. Now the factor $L_{ij}/L_{i-1,j}$ of (3) is the projection of L_i/L_{i-1} in H_j/H_{j-1} ; and the factor $H_{ji}/H_{j-1,i}$ is the projection of H_j/H_{j-1} in L_i/L_{i-1}. Hence

$$L_{ij}/L_{i-1,j} \cong H_{ji}/H_{j-1,i}$$

and indeed, by 3·6, these two factor groups of G are incident for all $i=1, 2, \dots, s$ and all $j=1, 2, \dots, r$. Thus we have

Theorem 3·7 Any two series of G possess refinements which are of equal length and with factors which are incident in pairs.

This is known as the refinement theorem : O. Schreier 1901–26.

(F). If $H_{i-1} = H_i$ in (1), the factor H_i/H_{i-1} is called trivial. By omitting repeated terms, we can replace any given series by one which has the same non-trivial factors but has no trivial factors. A series without trivial factors, i.e. without repeated terms, is called proper. A composition series of G is a proper series which has no proper refinements distinct from itself. By 3·5, a composition series may also be defined as one in which all the factors are simple groups. Obviously every proper series can be refined to a composition series. If we apply 3·7 to two given composition series of G and then detrivialise the two refinements, we obtain

Theorem 3·8 The factors of any two composition series of G are incident in pairs.

This is the Jordan–Hölder Theorem : C. Jordan 1838–1922 and O. Hölder 1859–1937.

A <u>soluble</u> group is one which has a series with all the factors Abelian. Since subgroups and quotient groups of Abelian groups are always Abelian, the <u>composition factors</u> of a soluble groups, i.e. the factors of any composition series, are also Abelian. But all subgroups of an Abelian group are normal, and so by 2·5 the only simple Abelian groups are the groups of order a prime. Hence a group G is soluble if and only if all its composition factors are of prime order. Insoluble groups are distinguished by the fact that one at least of their composition factors is a simple group of composite order.

§4. Automorphisms, Representations, Conjugates

(A) An automorphism of a group G is an isomorphic mapping of G onto itself: it is a permutation of G which leaves the group-structure of G invariant.

More generally, let X be any set and let X^n be the set of all ordered multiplets

$$x = (x_1, x_2, \cdots, x_n)$$

with n coordinates $x_i \in X$. The word "multiplet" reminds us that these coordinates need not be distinct. Thus $|X^n| = |X|^n$. Only when $x_1, \cdots, x_n$ are all different shall we call x an ordered set. An n-ary relation connecting the elements of X determines the set R of all $x \in X^n$ for which the given relation holds. Mostly, we can identify the relation with this subset R of X^n. A structured set X can be specified by a certain number of relations $R, R_1, R_2, \cdots$, not necessarily all with the same n. For example we can think of the structure of a group G as specified by a single ternary relation, consisting of all triplets $(\xi, \eta, \zeta) \in G^3$ for which $\xi\eta = \zeta$.

Any $\alpha \in \Sigma(X)$ induces a mapping $x \to x\alpha$ of X^n into itself, defined by the equations $(x\alpha)_i = x_i\alpha$, $i = 1, 2, \cdots, n$. For any relation R, let $R\alpha$ be the set of all $x\alpha$ with $x \in R$. The set of all $\alpha \in \Sigma(X)$ such that $R\alpha = R$, $R_1\alpha = R_1$, $\cdots$ is clearly a subgroup of $\Sigma(X)$: it is called the group of automorphisms of X with respect to the structure defined by the relations $R, R_1, \cdots$. An automorphism is a structure preserving permutation.

For example, let X consist of n real numbers and let R consist of all $x \in X^n$ such that

$$\prod_{i>j} (x_i - x_j) > 0.$$

As group of automorphisms of X with respect to R we obtain the

alternating group $\Sigma^+(X)$ of order $\frac{1}{2}n!$ consisting of all even permutations of X. A permutation of cycle-type $(1^{m_1}, 2^{m_2} \dots)$ is even or odd according as the number $m_2 + m_4 + \cdots$ of cycles of even order is even or odd.

The group of automorphisms of a group G will be denoted by $\mathrm{Aut}\, G$.

(B). Let α, β, ξ, η be elements of a group G. We write

$$\alpha^{-1}\xi\alpha = \xi^\alpha.$$

The element ξ^α is called the transform of ξ by α. Clearly $(\xi\eta)^\alpha = \xi^\alpha \eta^\alpha$. Hence the mapping $t(\alpha) = l(\alpha^{-1})\, r(\alpha) \in \Sigma(G)$ defined by

$$t(\alpha): \quad \xi \to \xi^\alpha \qquad (\xi \in G)$$

is an automorphism of G. Those automorphisms of G which have the form $t(\alpha)$ for some $\alpha \in G$ are called inner automorphisms of G. We also have $\xi^{\alpha\beta} = (\xi^\alpha)^\beta$ and so $t(\alpha\beta) = t(\alpha)\, t(\beta)$. Hence the mapping

$$\alpha \to t(\alpha) \qquad (\alpha \in G)$$

is homomorphic: it is an epimorphism of G onto the group $t(G)$ of all inner automorphisms of G. Now $\xi = \xi^\alpha$ if and only if $\alpha\xi = \xi\alpha$. Hence the kernel of this epimorphism consists of all $\alpha \in G$ which commute with every element of G. This kernel is called the centre of G and denoted by zG. By 3·3, $zG \lhd G$ and $t(G) \cong G/zG$. G is Abelian if and only if $G = zG$. The only inner automorphism of an Abelian group is the identity.

Now let τ be any automorphism of G, and let $\xi \in G$. It is usual to denote the image of ξ under τ by ξ^τ. Calculating the transform $\tau^{-1} t(\alpha)\, \tau$ of the inner automorphism $t(\alpha)$ by τ, we have the scheme

$$\xi^\tau \underset{\tau^{-1}}{\longrightarrow} \xi \underset{t(\alpha)}{\longrightarrow} \alpha^{-1}\xi\alpha \underset{\tau}{\longrightarrow} (\alpha^\tau)^{-1}\xi^\tau\alpha^\tau$$

since $(\alpha^{-1})^\tau = (\alpha^\tau)^{-1}$. But $\tau \in \Sigma(G)$ and so ξ^τ is an arbitrary element of G if ξ is chosen suitably. Hence we obtain the formula

$$t(\alpha)^\tau = t(\alpha^\tau).$$

Summing up, we have

Theorem 4.1 For any group G, with centre zG, we have
$G/zG \cong t(G) \lhd \operatorname{Aut} G$.

The quotient group $\operatorname{Aut} G / t(G)$ is sometimes called the group of outer automorphisms of G. But it is more natural to call any automorphism outer if it is not inner.

(C). If X is any subset of the group G and $\alpha \in G$, then we write $\alpha^{-1} X \alpha = X^{\alpha}$. Thus X is invariant under $t(\alpha)$ if and only if $X\alpha = \alpha X$. Hence a normal subgroup of G is precisely one which is invariant under every inner automorphism of G:

$$K \lhd G \iff K^{\alpha} = K \text{ for all } \alpha \in G.$$

If a subgroup of G is invariant under every automorphism of G both outer and inner, it is called a characteristic subgroup of G. By 2.5, in a cyclic group every subgroup is characteristic. We express that K is a characteristic subgroup of G by writing

$$K \text{ char } G.$$

If $K \lhd G$ and $\alpha \in G$, then the restriction $t_K(\alpha)$ of $t(\alpha)$ to K is an automorphism of K, but in general $t_K(\alpha)$ is not an inner automorphism of K. However we have

Lemma 4.2 If $H \text{ char } K$ and $K \lhd G$, then $H \lhd G$.

If $H \text{ char } K$ and $K \text{ char } G$, then $H \text{ char } G$.

But $H \lhd K$ and $K \lhd G$ do not in general imply that $H \lhd G$.

(D). A homomorphism f of a group G into a permutation group $\Sigma(X)$ is called a representation of G by permutations of X. The number $|X|$ is called the degree of the representation f. We have already noted two such representations: the regular representation of G, and the representation t of G by inner automorphisms. If the kernel of a representation f is 1, it is called faithful, for then

$f(G) \cong G$. t is always faithful by 1·4; but t is faithful only if $G = 1$, by 4·1.

If we are studying one particular representation f of G, it is often convenient to eliminate the ~~symbol~~ symbol f by writing $x\alpha$ instead of $x f(\alpha)$, where $\alpha \in G$, $x \in X$ and $f \in \mathrm{Hom}(G, \Sigma(X))$. We are then left with the set X, the group G and a multiplication $XG \to X$ such that

I^* $\quad x(\alpha\beta) = (x\alpha)\beta$;

II^* $\quad x1 = x$,

for all $x \in X$ and all α, β in G. Here 1 is the unit element of G. The laws I^* and II^* ensure that the mapping

$$f(\alpha) : \quad x \to x\alpha \qquad (x \in X)$$

is a permutation of X and that $f(\alpha\beta) = f(\alpha) f(\beta)$ for all α, β in G. In this way the representation f is recovered.

Two elements x, y in X are <u>related</u> under G if $x\alpha = y$ for some $\alpha \in G$. If $x\alpha = y$ and $y\beta = z$ then $x(\alpha\beta) = z$; also $y\alpha^{-1} = x$. So this is an equivalence relation. If every pair of elements of X are related under G, f is called a <u>transitive</u> representation. ~~In this case~~, we say that G permutes X <u>transitively</u>. In general, however, X will split up into a number of <u>transitivity classes</u> X_i :

$$X = X_1 \cup X_2 \cup \dots \cup X_r$$

each of which is permuted transitively by G. Each X_i consists of all $x \in X$ which are related under G to any given element of X_i. And, of course, $X_i \cap X_j$ is empty if $i \neq j$. ~~The restriction of~~ If $f_i(\alpha)$ is the permutation of X_i induced by $f(\alpha)$, then f_i is a transitive representation of G. $f_1, f_2, \dots, f_r$ are called the <u>transitive components</u> of f. Since they determine f uniquely, we express this decomposition by writing

$$f = f_1 \oplus f_2 \oplus \dots \oplus f_r .$$

If K_i is the kernel of f_i, then the kernel of f is $K = \bigcap_{i=1}^{r} K_i$.

(E). Two elements ξ and η of G are called <u>conjugate</u> in G if and only if $\xi^\alpha = \eta$ for some $\alpha \in G$. Thus conjugate elements are simply elements related under G in the representation t. Therefore G splits into a certain number of mutually disjoint <u>classes of conjugates</u> G_i:

$$G = G_1 \cup G_2 \cup \cdots \cup G_h .$$

The unit element of G is conjugate only to itself, so we may take $G_1 = 1$. The number h is an important numerical invariant of G. We call it the <u>class number</u> of G. If G is Abelian, each G_i consists of a single element of G and so in this case $h = |G|$.

<u>Lemma 4·3</u> In $\Sigma(X)$, two elements ξ and η are conjugate if and only if they have the same cycle-type. If $|X| = n$, the class number of $\Sigma(X)$ is equal to the number of partitions of n.

Proof: Suppose that $\eta = \xi^\tau$ with $\tau \in \Sigma(X)$ and let $(x_1, x_2, \ldots, x_r)$ be any cycle of ξ. Writing $x_{r+1} = x_1$, we have

$$x_i\tau \xrightarrow{\tau^{-1}} x_i \xrightarrow{\xi} x_{i+1} \to x_{i+1}\tau$$

so that $(x_1\tau, x_2\tau, \ldots, x_r\tau)$ is a cycle of η of the same order r. Thus ξ and η have the same cycle-type. Conversely, if ξ and η have the same cycle-type, we can find a permutation τ of X which maps each cycle of ξ into a corresponding cycle of η. If the cycle-type of ξ and η is $(1^{m_1} 2^{m_2} \ldots)$, this τ can be chosen in precisely

$$\prod_{k=1}^{\infty} (k^{m_k} \cdot m_k!)$$

distinct ways. Taking $\xi = \eta$ gives the first part of

<u>Lemma 4·4</u> The number of elements τ of $\Sigma(X)$ which commute with a given element ξ of type $(1^{m_1} 2^{m_2} \ldots)$ is $\prod_k k^{m_k} \cdot m_k!$. There is always an odd τ which commutes with ξ excepting only when the different cycles of ξ have different odd orders i.e. when $m_{2i} = 0$ and $m_{2i-1} \leq 1$ for all $i = 1, 2, \ldots$

For if ξ has two cycles $(x_1 x_2 \cdots x_r)$ and $(y_1 y_2 \cdots y_r)$ of

odd order r, then $\tau = (x_1 y_1)(x_2 y_2) \cdots (x_r y_r)$ commutes with ξ and is odd. If ξ has an cycle of even order, we can take τ to be this cycle. Again τ is odd and commutes with ξ. If $\xi = \tau_1 \tau_2 \cdots \tau_s$ where the τ_i are the cycles of ξ and if these cycles are all of different orders, then the only elements of $\Sigma(X)$ which commute with ξ are those of the form $\tau_1^{m_1} \tau_2^{m_2} \cdots \tau_s^{m_s}$. If the τ_i are all of odd order, these products are all even permutations.

(F) Let $f \in \mathrm{Hom}(G, \Sigma(X))$ and let $x \in X$. The set of all $\alpha \in G$ such that $x\alpha = x$ is a subgroup of G called the <u>stabilizer</u> of x in G. We denote it by $S_G(x)$. Let $\xi \in G$ and suppose that $x\xi = y$. Then every element of the coset $S_G(x)\xi$ maps x into y. Conversely, if $x\eta = y$ then $\xi\eta^{-1} \in S_G(x)$ and $\eta \in S_G(x)\xi$. The cosets of $S_G(x)$ in G correspond one-to-one with the elements $y \in X$ which are related to x under G. In particular, we have

<u>Lemma 4·5</u> If G permutes X transitively, then for all $x \in X$ $|G : S_G(x)| = |X|$. The degree of a transitive representation of G divides the order of G.

Let $\xi \in G$. Then the set of all $\alpha \in G$ which commute with ξ is a subgroup $C_G(\xi)$ called the <u>centralizer</u> of ξ in G. Applying 4·5 to the t-representation of G, we have the

<u>Corollary 1</u>. If $\xi \in G$, then $|G : C_G(\xi)|$ is equal to the number of conjugates of ξ in G. This number always divides $|G|$.

Each $t(\alpha)$, $\alpha \in G$, is an automorphism of G and maps subgroups into subgroups. Two subgroups H and K of G are called <u>conjugate</u> in G if and only if $H^\alpha = K$ for some $\alpha \in G$. If $t^*(\alpha)$ is the permutation induced by $t(\alpha)$ on the subgroups of G, then t^* is a representation of G; the transitivity classes of t^* are the <u>classes of conjugate subgroups</u> of G. Each of these classes consists of all the subgroups of G which are conjugate in G to any particular subgroup

H of the class in question. The set of all $\alpha \in G$ such that $H^\alpha = H$ is a subgroup $N_G(H)$ of G which contains H. It is called the <u>normalizer</u> of H in G. Since $H^\alpha = H$ is equivalent to $\alpha H = H\alpha$, the normalizer of H is the largest subgroup N of G such that $H \lhd N$. Applying 4.5 to the representation t^* of G, we obtain

<u>Corollary 2</u>. If H is any subgroup of G, then $|G : N_G(H)|$ is equal to the number of subgroups conjugate to H in G.

Note that a subgroup is always conjugate to itself. $H \lhd G$ if and only if $N_G(H) = G$. A normal subgroup is conjugate only to itself.

(G) Let G permute X transitively. Then, for given x and y in X, we have $x\alpha = y$. Then $x\xi = x$ if and only if $y\alpha^{-1}\xi\alpha = y$. Hence $S_G(y) = \alpha^{-1} S_G(x)\,\alpha$. In a transitive representation, the stabilizers form a class of conjugate subgroups. Suppose we have a second representation in which G permutes X' transitively. These two representations are called <u>equivalent</u> if and only if there is a one-to-one mapping θ of X onto X' such that $x\theta\alpha = x\alpha\theta$ for all $\alpha \in G$. If this is the case, then $|X| = |X'|$ and $S_G(x\theta) = S_G(x)$ for all $x \in X$. So equivalent representations have the same stabilizers, and of course the same degree.

Conversely, suppose that for some $x \in X$ and $x' \in X'$ we have $S_G(x) = S_G(x') = H$. Let T be a transversal to H in G. Then each element of X is expressible uniquely in the form $x\tau$ with $\tau \in T$. Similary each element of X' is expressible uniquely in the form $x'\tau$ with $\tau \in T$. Hence we have a one-to-one mapping θ of X onto X' defined by $(x\tau)\theta = x'\tau$. Given $\alpha \in G$, $\tau \in T$ there is a unique $\tau_1 \in T$ such that $H\tau\alpha = H\tau_1$. We then have

$$(x\tau)\theta\alpha = x'\tau\alpha = x'\tau_1 = (x\tau_1)\theta = (x\tau\alpha)\theta$$

and so the two representations are equivalent.

Given any subgroup H of G, the regular representation τ of G induces a representation τ_H of G by permutations of the cosets of H. For $\alpha \in G$, $\tau_H(\alpha)$ is by definition the mapping

$$\tau_H(\alpha): \quad H\xi \to H\xi\alpha \qquad (\xi \in G).$$

For any ξ, η in G, $\tau_H(\xi^{-1}\eta)$ maps $H\xi$ into $H\eta$. Thus τ_H is a transitive representation of G. The stabilizer of the coset H in this representation is precisely H itself. Summing up, we have

Theorem 4.6 In any transitive representation f of a group G, the stabilizers form a class of conjugate subgroups of G. Two transitive representations are equivalent if and only if they have the same stabilizers. If H is one of the stabilizers for f, then f is equivalent to τ_H.

In any representation of G, the kernel is the intersection of the stabilizers. In the representation τ_H, the stabilizers are the conjugates of H in G. Hence the kernel of τ_H is the group

$$K = \bigcap_{\xi \in G} H^{\xi} = K_G(H).$$

If $L \lhd G$ and $L \leq H$, then $L = L^{\xi} \leq H^{\xi}$ for all $\xi \in G$. Hence $L \leq K$. Thus $K_G(H)$ is the largest normal subgroup of G contained in H.

Note that $\tau_1 = \tau$ is precisely the regular representation itself.

(H) If H is any subgroup of G and $N = N_G(H)$, we have a representation t_H of N by automorphisms of H. Here $t_H(\alpha)$ is for any $\alpha \in N$ the restriction of $t(\alpha)$ to H. The kernel of this representation t_H is called the centralizer of H in G and denoted by $C_G(H)$. It consists of all elements of G which commute with every element of H. Hence $t_H(N) \cong N_G(H)/C_G(H)$. This group $t_H(N)$ will be called the automizer of H in G and denoted for preference by $A_G(H)$. It consists of all automorphisms of H which can be induced by transforming H by some element of G. Hence

$$A_G(H) \cong N_G(H)/C_G(H).$$

Note that $C_G(G) = z(G)$ is the centre of G and $A_G(G) = t(G)$ is the group of inner automorphisms of G.

If we are given a representation f of a group Γ by automorphisms of another group G, we shall say that G admits Γ as group of operators. If G is a multiplicative group, it is usually convenient to use the notation

$$\xi \to \xi^\alpha \qquad (\xi \in G)$$

for the automorphism $f(\alpha)$ of G. Here $\alpha \in \Gamma$. If G is an additive group, as often happens, we write $\xi\alpha$ instead of ξ^α. The laws which apply are

$$(\xi\eta)^\alpha = \xi^\alpha \eta^\alpha \; ; \; \xi^1 = \xi \; ; \; \xi^{\alpha\beta} = (\xi^\alpha)^\beta$$

or $(\xi + \eta)\alpha = \xi\alpha + \eta\alpha \; ; \; \xi 1 = \xi \; ; \; \xi(\alpha\beta) = (\xi\alpha)\beta$

according to the case. Here $\xi, \eta \in G$ and $\alpha, \beta \in \Gamma$, while 1 is the unit element of Γ.

A subgroup H of G is Γ-admissible if $H^\alpha = H$ for all $\alpha \in \Gamma$. Joins and intersections of admissible subgroups are admissible. A section H/K of G is admissible if both H and K are admissible. If this is the case, then the mapping

$$K\xi \to K\xi^\alpha \qquad (\xi \in H)$$

is an automorphism of H/K for all $\alpha \in \Gamma$. If we denote it by $f_{H/K}(\alpha)$,

then $f_{H/K}$ is a representation of Γ, and H/K admits Γ as group of operators

If G_1 is any other group admitting Γ as group of operators, then we say that G and G_1 are operator-isomorphic, or more precisely Γ-isomorphic if there is an isomorphism $\xi \to \xi_1$ of G onto G_1 such that $(\xi^\alpha)_1 = (\xi_1)^\alpha$ for all $\xi \in G$ and all $\alpha \in \Gamma$. This notion of Γ-isomorphism is analogous to that of equivalent representations. It is clear that if two admissible sections of G are incident, they are necessarily Γ-isomorphic. Hence we may state as a corollary of 3·7 and 3·8

Theorem 4·7 Let the group G admit Γ as group of operators. Then any two Γ-admissible series of G have refinements whose factors are Γ-isomorphic in pairs. In any two Γ-composition series of G, the factors are Γ-isomorphic in pairs.

Here, a Γ-composition series is a proper series whose terms are all Γ-admissible but which cannot be refined any further without losing this property. In other words, each factor group H/K of a Γ-composition series is Γ-simple, in the sense that no admissible subgroup L exists such that $K < L < H$ and $L \lhd H$. This implies that H/K has no characteristic subgroup L/K other than the two obvious ones with $L = K$ and $L = H$. A group G which has exactly two characteristic subgroup is sometimes called characteristically-simple; but this does not mean that G is simple, for G may have normal subgroups M with $1 < M < G$ which are not characteristic.

The most important special case of 4·7, apart from the one already covered in 3·8, is the case $\Gamma = G$. A G-composition series of G is called a chief series of G and its factors are called chief factors of G. H/K is a chief factor of G if and only if $K \lhd G$ and H/K is a minimal normal subgroup of G/K. (M is a minimal normal subgroup of G if $M \neq 1$, $M \lhd G$ and M contains no normal subgroup L of G such that $1 < L < M$.)

§5. p-groups. Sylow subgroups.

(A) Let p be a prime. A group whose order is a power of p is called a p-group.

p-groups have many special properties which do not belong to finite groups generally. A good many of these follow from

Lemma 5.1 Let the p-group G be represented by permutations of a set X and let Y be the set of all elements of X which are left invariant by G. Then $|X| \equiv |Y| \bmod p$.

For by 4.5, if X_i is one of the transitivity classes in this representation of G, then $|X_i|$ divides the order of G. Since $|G|$ is a power of p, either $|X_i| = 1$ or else $|X_i|$ is divisible by p. Hence $|X| = \Sigma |X_i| \equiv |Y| \bmod p$, since $|Y|$ is the number of classes X_i with a single element.

Theorem 5.2 Let G be a p-group.

(i) Let $K \lhd G$ and $K \neq 1$. Then $K \cap zG \neq 1$.

(ii) If $G \neq 1$, then $zG \neq 1$.

(iii) Every minimal normal subgroup of G has order p and lies in zG.

(iv) Let H be a proper subgroup of G. Then $H < N_G(H)$.

(v) Every subgroup of index p is normal in G.

(vi) Every maximal subgroup of G is of index p, hence normal.

(vii) Every chief factor of G has order p.

Proof: (i) Apply 5.1 to the representation t_K of G by automorphism of K. ~~The set of elements of K left invariant is~~ $Y = K \cap zG$ is not empty since it contains 1. But $|X| = |K| = p^r$ with some $r > 0$ by 2.4, since $K \neq 1$. Hence $|Y|$ is at least p, by 5.1.

(ii) is the special case $K = G$ of (i).

(iii) if K is a minimal normal subgroup of G, then $K \neq 1$. Hence $K \cap zG \neq 1$. But every subgroup of zG is normal in G. Hence $K \cap zG = K$ has order p by the minimality of K.

(iv) By 2.4, H is a p-group and $|G:H| = p^r$, with $r>0$ since $H<G$. The representation τ_H of G is of degree p^r. Apply 5.1 to the restriction f of τ_H to H. Then X is the set of all cosets of H in G and among these is H itself, which is invariant under H since $HH=H$. Since $|X| = p^r$, it follows that $|Y|$ is at least p, for it is not zero. Hence $H\xi H = H\xi$ for some element ξ of G which is not in H. This implies that $\xi H \xi^{-1} \leq H$ and so $\xi^{-1} \in N_G(H)$. Since $\xi \notin H$, we thus find $H < N_G(H)$.

(v) and (vi) are immediate corollaries of (iv).

(vii) follows from (iii) since a chief factor H/K of G is a minimal normal subgroup of the p-group G/K.

A section L/M of any group G is called a <u>central factor</u> of G if $M \lhd G$ and $L/M \leq \mathfrak{z}(G/M)$. This implies that $L \lhd G$ and 5.2 (iii) shows that <u>in a p-group G, every chief factor is a central factor</u>.

A group G is called <u>nilpotent</u> if it has a series whose factors are all central factors of G. Hence <u>all p-groups are nilpotent</u>

(B) Apropos the proof of 5.2 (iv), we note here

<u>Lemma 5.3</u> If H is any subgroup of a group G and $N = N_G(H)$, then the centralizer of $\tau_H(G)$ in $\Sigma(G)$ consists of all the ~~transf~~ mappings

$$\ell_H(\alpha): \quad H\xi \longrightarrow \alpha H\xi = H\alpha\xi \qquad (\xi \in G)$$

with $\alpha \in N$. It is isomorphic with N/H and its order $|N:H|$ is the number of invariants of H in the representation τ_H.

We have already noted that $H\xi H = H\xi$ if and only if $\xi \in N$ so that $|N:H|$ is the number of invariants of H in the representatio τ_H. If $\alpha \in N$, then $\alpha H = H\alpha$ and $\ell_H(\alpha)$ is therefore a permutation of the set X of all cosets of H in G. If $\alpha \in H$, $\ell_H(\alpha)$ is the identity on X, but if $\alpha \notin H$ then $\ell_H(\alpha)$ maps H into $H\alpha \neq H$. Further, $\ell_H(\alpha\beta) = \ell_H(\beta)\,\ell_H(\alpha)$ so that $\alpha \to \ell_H(\alpha^{-1})$

$(\alpha \in N)$ is a representation of N with kernel H. Thus $l_H(N) \cong N/H$. It is clear that $l_H(\alpha)$ commutes with $r_H(\eta)$ for all $\alpha \in N$, $\eta \in G$. If τ belongs to the centralizer of $r_H(G)$ in $\Sigma(G)$ and if τ maps H into the coset H^*, then τ must map $H\xi$ into $H^*\xi$ for all $\xi \in G$. Hence $H^*\xi = H^*\eta\xi$ for all $\eta \in H$, so $H^* = H^*H$ and $H^* = H\alpha$ with $\alpha \in N$. Thus $\tau = l_H(\alpha)$ and 5·3 is proved.

(C) Let p be a prime and let G be a group of order $p^n m$ where $(m, p) = 1$. Any subgroup of G of order p^n is called a Sylow p-subgroup of G. Thus S is a Sylow p-subgroup of G if and only if S is a p-group and $|G : S|$ is prime to p. If p does not divide $|G|$, then $n = 0$ and the only Sylow p-subgroup of G is the unit subgroup.

The following theorem, due to L. Sylow 1832–1918, is fundamental

Theorem 5.4 (i) Every group G has at least one Sylow p-subgroup.
(ii) The Sylow p-subgroups of G are all conjugate in G.
(iii) Every p-subgroup of G is contained in at least one Sylow p-subgroup
(iv) The number of Sylow p-subgroups of G is $\equiv 1 \bmod p$.

Proof: (i) due to Wielandt. Let X be a subset of G with $|X| = p^n$ and let $\xi \in G$. Then $|X\xi| = p^n$ by 1·6. Hence the regular representation of G induces a representation f of G:

$$f(\xi) : X \to X\xi \qquad (|X| = p^n)$$

on the $\binom{p^n m}{p^n}$ sets X. Since $(m, p) = 1$, the numbers $p^n m - r$ and $p^n - r$ are divisible by the same highest power of p for each value of $r = 0, 1, 2, \ldots, p^n - 1$. So the degree of f is prime to p and f has at least one transitive component f_1 with degree m_1 prime to p. Let X_1 be any member of the corresponding transitivity class and let S be the stabilizer of X_1 in G. Then $|X_1| = p^n$ and $|G : S| = m_1$, and $X_1 S = X_1$. So X_1 is the union of certain inverse cosets of S and hence $|S| \leq |X_1| = p^n$. But $(m_1, p) = 1$ and $|G : S| = m_1$. Hence p^n divides $|S|$. Thus $|S| = p^n$ and S is a Sylow p-subgroup of G

(ii) and (iii). Let H be any subgroup of G. In the proof of 5·2 (iv) we used the restriction to H of the representation r_H of G. We now need the restriction f of r_H to a second subgroup K of G. The transitivity class of f which contains a given coset $H\xi$ consists of all cosets of H which are contained in $H\xi K$. The set $H\xi K$ is called a <u>double coset</u> of H, K; so two distinct double cosets of H, K in G have no common element. Let T be a transversal to the double cosets of H, K in G, i.e. let T contain exactly one element from each of these double cosets. Then $G = \bigcup_{\tau \in T} H\tau K$ and the terms $H\tau K$ are disjoint in pairs. Hence

$$|G : H| = \sum_{\tau \in T} |H\tau K : H|.$$

The numbers $|H\tau K : H|$ are the degrees of the transitive components of the representation f of K. Now $\tau\xi$ and $\tau\eta$ lie in the same coset of H if and only if $\tau\xi\eta^{-1}\tau^{-1} \in H$ i.e. $\xi\eta^{-1} \in H^\tau$. Taking ξ, η in K we obtain

<u>Lemma 5·5</u>. Let H and K be subgroups of G, let $\xi \in G$ and let T be a transversal to the double cosets of H, K in G. Then

$$|H\xi K : H| = |K : H^\xi \cap K|$$

and

$$|G : H| = \sum_{\tau \in T} |K : H^\tau \cap K|.$$

Now let $H = S$ be a Sylow p-subgroup of G and let K be any p-subgroup of G. Then $|G : S|$ is prime to p and so, by 5·5, $|K : S^\tau \cap K|$ is prime to p for some $\tau \in T$. Since K is a p-group, it follows that $|K : S^\tau \cap K| = 1$ and so $K \leq S^\tau$, which is a Sylow p-subgroup of G. This gives (iv). If K is actually a Sylow p-subgroup of G, then $|K| = |S^\tau|$ and so $K = S^\tau$ is conjugate to S in G. This gives (iii).

(iv) Here we take $H = N_G(S)$ and $K = S$ in 5·5. By 4·5 Cor. 2, the number l of Sylow p-subgroups of G is equal to $|G : H|$, since they are all conjugate to S by (iii). If $S \nleq H^\tau$, then $|S : H^\tau \cap S|$ is a positive power of p. If $S \leq H^\tau$, then

$S_1 = \tau S \tau^{-1} \leq H$ and S_1, S are Sylow p-subgroups of H. But $S \lhd H$ and so $S = S_1$ by (iii). Hence $\tau \in H$ and $H\tau S = HS$. Thus there is exactly one double coset of H, S viz. the product HS, for which $|S : H^\tau \cap S|$ is not divisible by p. For this exceptional one, $\tau \in H$ and $|S : H^\tau \cap S| = 1$. Thus $l \equiv 1 \mod p$ and Sylow's Theorem is completely proved.

(D) A few immediate consequences of Sylow's Theorem are worth recording as corollaries.

Corollary 5.41 If p^r divides $|G|$, then G has subgroups of order p^r

For by 5.2 (vii), a Sylow p-subgroup S of G has subgroups of every order $1, p, p^2, \cdots, p^n = |S|$.

On the other hand, the tetrahedral group Σ_4^+ of order 12 has no subgroups of order 6. (The symmetric and alternating groups $\Sigma(X)$ and $\Sigma^+(X)$ with $|X| = n$ will often be denoted by Σ_n, Σ_n^+ when it is not necessary to indicate the set X. This may be taken as the set of integers $1, 2, \cdots, n$).

Note that a subgroup H of index 2 in G is always normal:

$$|G : H| = 2 \quad \Rightarrow \quad H \lhd G.$$

For $\xi H = H\xi = H$ for all $\xi \in H$; while if $\xi \in G - H$ (in G but not in H), then again $\xi H = H\xi$ since each of these sets coincides with $G - H$.

Corollary 5.42 Every normal p-subgroup M of G is contained in $K_G(S) = \bigcap_{\xi \in G} S^\xi$, where S is a Sylow p-subgroup of G. $K_G(S)$ is the unique maximal normal p-subgroup of G.

~~For by 5.4(iii) $K \leq S^\xi$ for some $\xi \in G$ and so $K \leq K^{\xi^{-1}} \leq S$ for all $\xi \in G$.~~

For by 5.4(iii), $M \leq S^\tau$ for some $\tau \in G$. Since $M \lhd G$, we then have $M = M^{\tau^{-1}\xi} \leq S^\xi$ for all $\xi \in G$. Hence $M \leq K_G(S)$.

Corollary 5.43 If H and K are subgroups of G such that $N \leq H \leq K$, where N is the normalizer in G of the Sylow p-subgroup S of G, then $|K:H| \equiv 1 \mod p$.

For S is a Sylow p-subgroup of both H and K; and $N = N_H(S) = N_K(S)$. Hence $|H:N|$ and $|K:N|$ are the numbers of Sylow p-subgroup of H and K, respectively, by 5.4(ii). So $|H:N| \equiv |K:N| \equiv 1 \mod p$ by 5.4 (iv). Consequently $|K:H| \equiv 1 \mod p$ by 2.6.

More important is

Lemma 5.6 Let $K \lhd G$ and let S be a Sylow p-subgroup of G. Then KS/K is a Sylow p-subgroup of G/K and $S \cap K$ is a Sylow p-subgroup of K.

Proof: By 5.5, $|KS:K| = |S:K \cap S|$ which is a power of p; while the index of KS/K in G/K is $|G:KS|$ by 3.5, and this divides $|G:S|$ by 2.6. Hence $|G:KS|$ is prime to p.

omitted

Again, $|S \cap K|$ is a power of p; while $|K:S \cap K| = |SK:S|$ by 5.5 and $|SK:S|$ is prime to p.

Corollary: If $|G:K|$ is prime to p, then $S \leq K$. If $|G:K|$ is a power of p, then $KS = G$.

Let ϖ be any set of primes. A ϖ-number is a number whose prime factors all lie in ϖ. Let ϖ' be the complementary set of primes. Every positive integer $n = n_\varpi n_{\varpi'}$, where n_ϖ is a ϖ-number and $n_{\varpi'}$ is a ϖ'-number uniquely determined by n. An S_ϖ-subgroup of a group G is any subgroup S of order $|G|_\varpi$ i.e. such that $|S|$ is a ϖ-number and $|G:S|$ is a ϖ'-number. When $\varpi = p$ is a single prime, we come back to the notion of a Sylow p-subgroup which is the same as an S_p-subgroup. G is called a ϖ-group whenever $|G|_\varpi = |G|$ or what is the same $|G|_{\varpi'} = 1$.

Remark: The symbol ϖ should not be confused with ω, the last letter of the Greek alphabet. In fact ϖ is a special form of π

often used by astronomers : it is not omega but pi in the sky.

Clearly the proof of 5.6 applies equally well with p replaced by an arbitrary set of primes. So we may state

Lemma 5.7 Let $K \lhd G$ and let S be any S_π-subgroup of G. Then KS/K is an S_π-subgroup of G/K and $S \cap K$ is an S_π-subgroup of K.

We also need

Lemma 5.8 If G has a normal S_π-subgroup K, then every π-element and every π-subgroup of G is contained in K.

For let H be a π-subgroup of G. Since $K \lhd G$, KH is a subgroup of G. By 5.5, $|KH| = |K| \cdot |H : K \cap H|$. Here $|H : K \cap H|$ is a π-number and $|K| = |G|_\pi$. Hence $|H : K \cap H| = 1$ and $H \leq K$.

Consequences of Sylow's Theorem.

§6. Pronormal Subgroups. Nilpotent Groups

(A) Let H be a subgroup of G.

(i) We call H subnormal in G if and only if it belongs to some series of G i.e. if any only if there exist subgroups H_i such that

$$H = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_r = G. \qquad (1)$$

(ii) We call H pronormal in G if and only if H is conjugate to H^ξ in $\{H, H^\xi\}$ for all $\xi \in G$.

(iii) We call H dinormal in G if and only if $N_G(H) = H$.

(iv) We call H abnormal in G if and only if it is both pronormal and dinormal in G.

These relations will be denoted as follows:

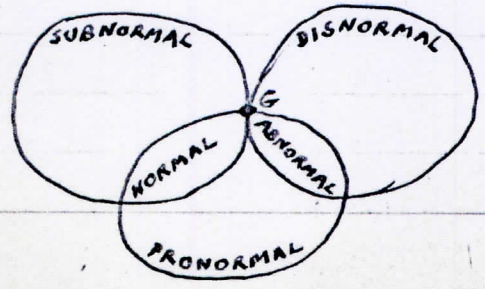
$$H \text{ sbn } G, \quad H \text{ prn } G, \quad H \text{ dsn } G, \quad H \text{ abn } G$$

respectively.

Lemma 6.1 $H \lhd G$ if and only if H is both subnormal and pronormal in G.

Obviously $H \lhd G$ implies H sbn G and also H prn G, for $H = H^\xi = \{H, H^\xi\}$ for all $\xi \in G$. Suppose H sbn G but that H is not normal in G. We may assume that (1) holds and that H is not normal in H_2. Then $H \neq H^\xi$ for some $\xi \in H_2$. Then $H^\xi \leqq H_1^\xi = H_1$ since $H_1 \lhd H_2$ and so $J = \{H, H^\xi\} \leqq H_1$. But $H \lhd H_1$ so $H \lhd J$ and H cannot be conjugate to H^ξ in J. Hence H is not pronormal in G. Thus H sbn G and H prn G imply $H \lhd G$.

The only subgroup of G which is both subnormal and dinormal in G is G itself. So we may picture these five classes of subgroups diagrammatically as follows:



This picture represents a general case.

Lemma 6.2 Let K be a subgroup of G containing H. If H sbn G then H sbn K. Similarly $\not\subseteq$ with prn, dsn, abn and $\lhd$ in place of sbn

This is clear except for sbn, in which case we may state the stronger result:

Lemma 6.3 (i) Let H sbn $K \leq G$ and let L be any subgroup of G. Then $L \cap H$ sbn $L \cap K$.

(ii) If H sbn K and K sbn L, then H sbn L.

(iii) If $H = \bigcap_{\lambda \in \Lambda} H_\lambda$ and each H_λ sbn G, then H sbn G.

Proof: (i) We may assume $H = H_0 \lhd H_1 \lhd \cdots \lhd H_r = K$. Then $L \cap H_{i-1} \lhd L \cap H_i$ for each $i = 1, 2, \cdots, r$ by 3.4 and so $L \cap H$ sbn $L \cap K$ (ii) is clear. (iii) It is sufficient to show that H sbn G and K sbn G implies $H \cap K$ sbn G. By (i), $H \cap K$ sbn $H \cap G = H$ and so this follow from (ii).

(B). Suppose that $J = \{H, H^\xi\}$ is a p-group, $\xi \in G$ and ~~H sbn G. By 6.2, H sbn J~~ H prn G. By 6.2, H prn J. By 5.2 (iv), H sbn J. Hence $H \lhd J$ by 6.1; and so $H = H^\xi$ since H prn J.

Conversely, Let H be a p-subgroup of G. By 5.4 (iii), H is contained in some Sylow p-subgroup S of G. Suppose that no other conjugate of H in G is contained in S. Let $J = \{H, H^\xi\}$, $\xi \in G$. By 5.4 (iii), $H \leq T \leq S_1$, where T is a Sylow p-subgroup of J and S_1 is a Sylow p-subgroup of G. Also by 5.4 (iii) and (i), we have $H^{\xi\eta} \leq T$ for some $\eta \in J$. Since S and S_1 are conjugate in G, by 5.4 (ii), they contain the same number of conjugates of H in G. By hypothesis, this number is one. Hence $H^{\xi\eta} = H$ and H is conjugate to H^ξ in J. Since ξ was arbitrary, H prn G.

Thus we have proved

Theorem 6.4 Let H be a p-subgroup of G. Then H prn G if and only if each Sylow p-subgroup P of G contains exactly one of the conjugates of H in G.

Choosing P to contain H, this situation is expressed by saying that H is *weakly closed in P with respect to G*. This is the Wielandt terminology; but here we shall simply say H is pronormal in G.

Corollary 6.41 If $H \leq P$ where P is a Sylow p-subgroup of G and if H prn G, then $N_G(Q) \leq N_G(H)$ for every subgroup Q such that $H \leq Q \leq P$.

Corollary 6.42 If H_1 and H_2 are pronormal p-subgroups of G contained in the same Sylow p-subgroup P of G, then $H_1 H_2$ is pronormal in G.

Note that H_1 and H_2 are normal in P by 6.41. If $(H_1 H_2)^{\xi} \leq P$, for some $\xi \in G$ then $H_i^{\xi} \leq P$ and so $H_i^{\xi} = H_i$ $(i = 1, 2)$ since H_i prn G. So $(H_1 H_2)^{\xi} = H_1 H_2$. So $H_1 H_2$ prn G.

It follows from 6.42 that if Q is any p-subgroup of G, there is a uniquely determined pronormal subgroup of G which is maximal subject to being contained in Q. If this is H, then $H < K \leq Q$ implies that K is not pronormal in G. By 6.41, $H \leq \bigcap_{\xi \in N_G(Q)} Q^{\xi}$. The pronormal subgroups of G contained in a given Sylow p-subgroup P of G form a lattice $\mathcal{P} = \mathrm{Prn}_G(P)$. But this is not a sublattice of the lattice of all subgroups of P in general. For given H_1, H_2 in $\mathcal{P}$, although $H_1 H_2 \in \mathcal{P}$ by 6.42, in general $H_1 \cap H_2$ does not belong to $\mathcal{P}$, i.e. $H_1 \cap H_2$ is usually smaller than $H_1 \cap H_2$ and even smaller than $[H_1, H_2]$. For example, if G is the octahedral group and $p = 2$, then P is an octic group. The subgroups of order 4 in G are all pronormal, but none of the subgroups of order 2 is pronormal. So $\mathcal{P}$ consists here of P itself, 1 and the three subgroups of order 4 in P.

Corollary 6.43 If $K \trianglelefteq G$, then any Sylow subgroup of K is pronormal in G.

For a Sylow p-subgroup P of G contains only one Sylow p-subgroup of K, viz. $P \cap K$.

Those pronormal subgroups of G which have the form $P \cap K$ with $K \lhd G$ form a special sublattice $\mathcal{P}_0$ of $\mathcal{P}$. Unlike $\mathcal{P}$, $\mathcal{P}_0$ is also a sublattice of the lattice of all subgroups of P. For if K_1 and K_2 are normal in G, so is $K_1 \cap K_2$ and $P \cap (K_1 \cap K_2) = (P \cap K_1) \cap (P \cap K_2)$. Further, $P \cap K_1 K_2 = (P \cap K_1)(P \cap K_2)$.

(C) The pronormal subgroups of a group G can also be characterized by their relation to the transitive permutational representations of G.

Suppose that G is represented transitively by permutations of a set X. Let H be a subgroup of G and let $N = N_G(H)$. Let Y be the set of all $y \in X$ which are invariant under H. If $y \in Y$ and $\xi \in N$, we have $yH = y$ and so $y\xi H = yH\xi = y\xi$. Hence $y\xi \in Y$. Thus N leaves Y invariant: $YN = Y$.

Let S_y be the stabilizer of y in G. If y and z are in Y, we have $y\eta = z$ for some $\eta \in G$ since G permutes X transitively. Since $H \leq S_y \cap S_z$, we have $H^\eta \leq S_y^\eta = S_z$. If H pron G, it is conjugate to H^η in $\{H, H^\eta\}$ and hence also in S_z. So $H^{\eta\zeta} = H$ for some $\zeta \in S_z$. So $\eta\zeta \in N$ and $y\eta\zeta = z$. Thus N permutes Y transitively whenever H is pronormal in G.

Conversely, suppose that in any transitive representation of G, N permutes transitively the symbols left invariant by H. Let $\xi \in G$ and let $J = \{H, H^\xi\}$. Then $JH = J$ and $JH^\xi = J$ or $J\xi^{-1}H = J\xi^{-1}$. Hence, in the transitive representation τ_J of G, H leaves fixed the cosets J and $J\xi^{-1}$. By hypothesis, $J = J\xi^{-1}\eta$ for some $\eta \in N$. Then $\xi^{-1}\eta \in J$ and transforms H^ξ into $H^\eta = H$. This is true for all $\xi \in G$. Hence H pron G.

Thus we have proved the first part of

Theorem 6.6 Let H be a subgroup of G and let $N = N_G(H)$. Then (i) H pron G if and only if, in every transitive representation of G, N permutes transitively the symbols left invariant by H.

(ii) H abn G if and only if, in every transitive representation of G, H leaves at most one of the symbols invariant.

To prove (ii), let H abn G and let G permute X transitively. Then by (i) N permutes transitively the set Y of elements of X which are left invariant by H. But $H = N$. Hence $|Y| \leq 1$.

Conversely, if $|Y| \leq 1$ for every transitive representation of G, then H pm G by (i). If we take the representation of G to be τ_H, then $|Y| = |N : H|$ by 5.3 and so $N = H$ is dinormal in G. Hence H abn G.

By 4.6, every transitive representation of G is equivalent to τ_K for some subgroup K of G. In τ_K, H leaves the coset $K\xi$ invariant if and only if $H \leq K^\xi$. Thus $|Y| = 0$ unless H is contained in some conjugate of K. We may therefore restate the criterion for abnormal subgroups in the following two forms:

Corollary 6.61 Let H be a subgroup of G. Then the following conditions are equivalent.

(i) H abn G.

(ii) For any subgroup K of G and any $\xi \in G$, $H \leq K \cap K^\xi$ implies $\xi \in K$.

(iii) Every subgroup of G containing H is dinormal in G, and H is not contained in the intersection of any two distinct conjugate subgroups of G.

We note also the following

Lemma 6.7 (i) If H pm G and $K \lhd G$, then HK pm G.

(ii) If $K \lhd G$ and $K \leq H$, then H pm G if and only if H/K pm G/K.

~~(iii) If $K \lhd G$, H pm HK and HK pm G, then H pm G.~~

~~(i) and (ii) are clear. To prove (iii), let $\xi \in G$ and $J = \{H, H^\xi\}$ Since HK pm G, there is an element $\eta\xi \in JK$, where $\eta \in J$ and $\xi \in K$ such that~~ Sorry!

(D) We note next some easy corollaries of 6·6.

Lemma 6·61 The normalizers of pronormal subgroups are abnormal. In particular, normalizers of Sylow subgroups are abnormal.

Lemma 6·62 Any subgroup containing an abnormal subgroup is abnormal

Lemma 6·63 Let H prn G and let $N = N_G(H)$. If two elements of the centre of H are conjugate in G, they are conjugate in N. If two normal subgroups of H are conjugate in G, they are conjugate in N.

Lemma 6·64 Let H abn G. Then no two distinct elements of the centre of H can be conjugate in G; and no two distinct normal subgroups of H can be conjugate in G.

Lemma 6·65 Let H prn G, let $N = N_G(H)$ and let $K = \{H^G\}$ be the normal closure of H in G. Then $KN = G$. Further, if $H \leq L \trianglelefteq$ sbn G, then $K \leq L$, and so $LN = G$.

Proof of 6·65. Let $\xi \in G$. Then $J = \{H, H^\xi\} \leq K$ and so $H^{\xi\eta} = H$ for some $\eta \in K$. Hence $\xi = (\xi\eta)\eta^{-1} \in NK = KN$, and so $KN = G$.

Let $L = L_0 \lhd L_1 \lhd \cdots \lhd L_r = G$. Since $H \leq L_{r-1} \lhd G$, we have $K \leq L_{r-1}$. Since H prn G, we have $K = \{H^K\}$ and hence $H \leq L_{r-2} \lhd L_{r-1}$ gives $K \leq L_{r-2}$ and so on.

By 6·3(iii), given any subgroup H of G, there is a uniquely determined smallest subnormal subgroup of G which contains H; this is the subnormal closure of H in G. By 6·65, the subnormal closure of a pronormal subgroup coincides with its normal closure.

Lemma 6·66 A pronormal subgroup cannot be permutable with any of its conjugates (other than itself).

For let H prn G and $H^\xi \neq H$, $\xi \in G$. Then we can choose $\xi \in J = \{H, H^\xi\}$. But $HH^\xi = H^\xi H$ would imply $J = HH^\xi$ by 2·7, contrary to 9·6(ii), sorry!

Lemma 6·67 Let H prn G and let $H \leq K \leq N = N_G(H)$. Then $N_G(K) \leq N$; and K prn G if and only if K/H prn N/H.

Suppose $K^\xi = K$, $\xi \in G$. Since $K \leq N$, we have $H^\xi \lhd K$. But H^ξ is conjugate to H in $J = \{H, H^\xi\}$ which is contained in K. Hence $H^\xi = H$ and $\xi \in N$.

If K prn G, then K prn N by 6.2 and so K/H prn N/H. Conversely, if K/H prn N/H, then K prn N. For any $\eta \in G$, there is an element ξ in $\{H, H^\eta\} \leq J = \{K, K^\eta\}$ such that $H^{\eta\xi} = H$, since H prn G. Then $H \lhd K^{\eta\xi}$ and so $K^{\eta\xi} \leq N$. Since K prn N, we have $K^{\eta\xi\zeta} = K$ for some $\zeta \in J_1 = \{K, K^{\eta\xi}\}$. But $\forall\ \xi \in J$ and so $J_1 \leq J$ and hence $\xi\zeta \in J$. Thus K and K^η are conjugate in J. This holds for all $\eta \in G$ and so K prn G.

Lemma 6.6 Let $K \lhd G$ and let H/K be a pronormal p-subgroup of G/K. Then any Sylow p-subgroup P of H is pronormal in G.

Proof: Since H/K is a p-group, we have $H = KP$. Let $\xi \in G$ and let $J = \{P, P^\xi\}$. Then $\{H, H^\xi\} = JK$ and since H prn G, we have $H^{\xi\eta\zeta} = H$ for some $\eta \in J$, $\zeta \in K$. Then P and $P^{\xi\eta}$ are Sylow p-subgroups of $H = H^{\xi\eta}$ and hence they are conjugate in their join $J_1 = \{P, P^{\xi\eta}\}$. But $J_1 \leq J$ since $\eta \in J$. Hence P and P^ξ are conjugate in J. This holds for all $\xi \in G$ and so P prn G.

This lemma shows that every pronormal p-subgroup of G/K is the image in the natural epimorphism of G onto G/K of some pronormal p-subgroup of G.

Lemma 6.6 Let $G = LM$ where M is a normal p-subgroup of G and $L \cap M = 1$. Let P be a Sylow p-subgroup of L, $P_1 = [M, P]$ and $H = PP_1$. Then H is pronormal in G.

Proof: $Q = PM$ is a Sylow p-subgroup of G. Let $N = N_L(P)$. Since G and G/M have the same number of Sylow p-subgroups, we have $N_G(Q) = NM$. Let $H^\xi \leq Q$. Then $Q^\xi = P^\xi M$ since $M \lhd G$ and $P^\xi \leq Q$, $P^\xi \cap M = 1$. Hence $Q^\xi = Q$ and $\xi = \eta\zeta$ with $\eta \in N$, $\zeta \in M$. But $P^\eta = P$ and so $P_1^\eta = P_1$ and hence $H^\eta = H$. Thus $H^\xi = H^\zeta$. But $P_1 \lhd M$ by 7.1(iv) and $P^\zeta \leq P[P, M] = H$. Hence $H^\zeta = H$, and so Q contains only one conjugate of H in G. So H prn G as stated.

(E). **Theorem 6.8** The following conditions on a group G are equivalent

(i) G is nilpotent.

(ii) No proper subgroup of G is dinormal in G.

(iii) Every subgroup of G is subnormal in G.

(iv) Every pronormal subgroup of G is normal in G.

(v) Every maximal subgroup of G is normal in G and therefore contains G'.

(vi) Every Sylow subgroup of G is normal in G.

Proof: (i) $\Rightarrow$ (ii). For let H be a proper subgroup of G and let $1 = G_0 < G_1 < \cdots < G_r = G$ be a central series of G. Let G_i be the first term in this series which does not contain H, let $\xi \in H$ and $\eta \in G_i$. Since G_i/G_{i-1} is in the centre of G/G_{i-1}, we have $G_{i-1}\xi\eta = G_{i-1}\eta\xi$. Hence $G_{i-1}\eta\xi\eta^{-1} = G_{i-1}\xi \leq H$, since $G_{i-1} \leq H$ by definition of i. Therefore $\eta\xi\eta^{-1} \in H$. This holds for all $\xi \in H$ and $\eta \in G_i$. Hence $G_i \leq N_G(H)$. Since $G_i \not\leq H$, we conclude that H is not dinormal in G.

(ii) $\Rightarrow$ (iii) is clear.

(iii) $\Rightarrow$ (iv) follows from 6.1.

(iv) $\Rightarrow$ (v). For by 6.7, a maximal subgroup is either normal or abnormal, and in the second case it is pronormal. Alternatively, (ii) $\Rightarrow$ (v) is clear.

(v) $\Rightarrow$ (vi). For by 6.61 and 6.62 a maximal subgroup which contains the normalizer of a non-normal Sylow subgroup is abnormal and therefore not normal. Alternatively, (iv) $\Rightarrow$ (vi) since Sylow subgroups are pronormal.

(vi) $\Rightarrow$ (i). By induction on $|G|$. We need the following easy

Lemma 6.9. Let $H \lhd G$, $K \lhd G$ and $H \cap K = 1$. Then every element of H commutes with every element of K.

For let $\xi \in H$, $\eta \in K$ and $\zeta = \xi^{-1}\eta^{-1}\xi\eta$. Then $\xi^{-1}\eta^{-1}\xi \in K$ and so $\zeta \in K$, while $\eta^{-1}\xi\eta \in H$ and so $\zeta \in H$. Since $H \cap K = 1$, we have $\zeta = 1$ and $\xi\eta = \eta\xi$.

Suppose now that $G \neq 1$ and let S be a Sylow p-subgroup of G, $S \neq 1$ and $Z = \zeta S$. Then $Z \neq 1$ by 5.2(ii). Let T be a Sylow q-subgroup of G with $q \neq p$. Then $Z \cap T = 1$. By hypothesis $T \trianglelefteq G$. Also $S \trianglelefteq G$ and Z char S, so $Z \trianglelefteq G$ by 4.2. Hence T centralizes Z by 6.9. Also S centralizes $Z = \zeta S$. Thus $C = C_G(Z)$ contains a Sylow q-subgroup of G for all primes q, including $q = p$. So $C = G$ and $Z \leq \zeta G$. By 5.6, ZT/Z is a Sylow q-subgroup of G/Z. Since $Z \trianglelefteq G$ and $T \trianglelefteq G$, we have $ZT \trianglelefteq G$ and so $ZT/Z \trianglelefteq G/Z$. Hence the Sylow subgroups of G/Z are all normal, by 5.4(ii). By the induction hypothesis, G/Z has a central series with terms G_i/Z where $Z = G_1 < G_2 < \cdots < G_r = G$. Since $Z \leq \zeta G$, $1 = G_0 < Z = G_1 < \cdots < G_r = G$ is a central series of G. Thus G is nilpotent.

Upper & Lower Central Series

§7 [illegible]

(A). Let ξ and η be elements of a group G. We define

$$[\xi,\eta] = \xi^{-1}\eta^{-1}\xi\eta = \xi^{-1}\xi^{\eta}$$

to be the <u>commutator</u> of ξ with η. Note that

$$[\eta,\xi] = [\xi,\eta]^{-1}$$

and that $[\xi,\eta] = 1$ if and only if ξ and η commute.

Let H and K be subgroups of G. We define

$$[H,K] = \{\,[\xi,\eta]\,;\ \xi\in H,\ \eta\in K\}.$$

Hence $[H,K] = [K,H]$ and $[H,K] = 1$ if and only if every element of H commutes with every element of K.

The group

$$G' = [G,G]$$

is called the (first) <u>derived group</u> of G. The second, third, ... derived groups of G are $G'' = (G')'$, $G''' = (G'')'$ and so on.

Besides 6.9, we have the following easy results concerning commutator

<u>Lemma 7.1</u>

(i) $[\xi\eta,\zeta] = [\xi,\zeta]^{\eta}[\eta,\zeta]$.

(ii) $[\xi,\eta\zeta] = [\xi,\zeta][\xi,\eta]^{\zeta}$.

(iii) $[H,K] \lhd \{H,K\}$.

(iv) If G admits a group of operators Γ, then $[H,K]^{\alpha} = [H^{\alpha},K^{\alpha}]$ for all $\alpha\in\Gamma$. In particular, if $H\lhd G$ and $K\lhd G$, then $[H,K]\lhd G$ and $[H,K]\leq H\cap K$.

(v) H normalizes K if and only if $[H,K]\leq K$.

(vi) A section L/M of G is a central factor of G, if and only if $[L,G]\leq M$.

(vii) $K\lhd G$ and G/K is Abelian if and only if $G'\leq K$.

(viii) Let H,K and L be normal subgroups of G. Then $[HK,L] = [H,L][K,L]$ and $[H,KL] = [H,K][H,L]$

Proof: (i) $\xi^\eta = \xi[\xi,\eta]$. Hence $(\xi\eta)^\zeta = \xi\xi\eta\,[\xi\eta,\zeta]$ but also $\xi^\zeta\eta^\zeta = \xi[\xi,\zeta]\,\eta[\eta,\zeta] = \xi\eta\,[\xi,\zeta]^\eta[\eta,\zeta]$ and comparing gives (i).

(ii) follows from (i) by inversion, using (1).

(iii) In (i), let $\xi,\eta \in H$ and $\zeta \in K$. Then $[\xi,\zeta]^\eta = [\xi\eta,\zeta][\eta,\zeta]^{-1} \in [H,K]$. This is true for all such ξ,η,ζ. Hence $H \leq N_G([H,K])$. Similarly, in (ii), let $\xi \in H$ and $\eta,\zeta \in K$. We obtain $K \leq N_G([H,K])$. Hence $\{H,K\}$ normalizes $[H,K]$; and also contains it. So (iii) follows.

(iv) $[\xi,\eta]^\alpha = [\xi^\alpha,\eta^\alpha]$ for all ξ,η in G and $\alpha \in \Gamma$. Hence $[H,K]^\alpha = [H^\alpha, K^\alpha]$. If H and K are normal in G, the fact that $[H,K] \leq H \cap K$ follows from (v).

(v) Let $\xi \in H$, $\eta \in K$. If H normalizes K, then $[\xi,\eta] = \xi^{-1}\eta^{-1}\xi\cdot\eta$ lies in K, since $\xi^{-1}\eta^{-1}\xi \in K$ and $\eta \in K$. Hence $[H,K] \leq K$. Conversely, the latter relation implies that $\xi^{-1}\eta^{-1}\xi \in K$ for all $\xi \in H$, $\eta \in K$. So H normalizes K.

(vi) Let $\xi \in L$ and $\eta \in G$. If L/M is a central factor of G, then $M\xi$ commutes with $M\eta$, so $[M\xi, M\eta] = M$. But $M \lhd G$ and so $[M\xi, M\eta] = M[\xi,\eta]$ and $[\xi,\eta] \in M$. Thus $[L,G] \leq M$.

Conversely, let $[L,G] \leq M$. Since $M \leq L$, it follows that $[M,G] \leq M$ and so $M \lhd G$ by (v). Further, $[\xi,\eta] \in M$ and so $[M\xi, M\eta] = M$. Hence $L/M \leq Z(G/M)$ and L/M is a central factor of G.

(vii) If $K \lhd G$ and G/K is Abelian, then G/K is a central factor of G and so $G' \leq K$ by (vi). Conversely, if $G' \leq K$, then $[K,G] \leq K$ and $K \lhd G$ by (v); and G/K is a central factor of G by (vi), hence G/K is Abelian.

(viii) Take ξ,η,ζ in (i) and (ii) to be arbitrary elements of H,K,L respectively and use (iv) which ensures the normality of $[H,L]$, $[K,L]$, ... in (

$$\zeta(G \bmod K) = L.$$

The <u>upper central series</u> of G consists of the groups $\zeta^n G$ defined inductively as follows:

$$\zeta^1 G = \zeta G, \quad \zeta^{n+1} G = \zeta(G \bmod \zeta^n G), \ (n = 1, 2, \cdots).$$

Also we write $\zeta^0 G = 1$. Hence

$$1 = \zeta^0 G \leq \zeta^1 G \leq \zeta^2 G \leq \cdots$$

and $\zeta^n G / \zeta^{n-1} G$ is the centre of $G/\zeta^{n-1} G$. Thus we have

$$\zeta^n G \ \text{char}\ G$$

for all n. $\zeta^2 G, \zeta^3 G, \cdots$ are called the second, third, ... centres of G. We define

$$\zeta^\infty G = \bigcup_{n=1}^{\infty} \zeta^n G$$

to be the <u>hypercentre</u> of G. If r is the least non-negative integer such that $\zeta^r G = \zeta^{r+1} G$, then

$$1 = \zeta^0 G < \zeta^1 G < \cdots < \zeta^r G = \zeta^\infty G.$$

Suppose that $1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots$ and that each G_i/G_{i-1} is a central factor of G. Then we have an <u>ascending central series</u> of G. By induction on n, we obtain

$$G_n \leq \zeta^n G \qquad (n = 0, 1, 2, \cdots).$$

The upper central series is the uppermost ascending central series of G. Hence G is nilpotent if and only if $G = \zeta^\infty G = \zeta^r G$ for some $r \geq 0$. The least such r is called the <u>class</u> of G, following W.B. Fite. Abelian groups are the same as nilpotent groups of class 1.

<u>Lemma 7.2</u>. (i) If $H \lhd G$ and $H \cap \zeta^r G > H \cap \zeta^{r-1} G$ for some r, then $H \cap \zeta^s G > H \cap \zeta^{s-1} G$ for $s = 1, 2, \cdots, r$.

(ii) If G is non-Abelian, then $G/\zeta G$ is not cyclic.

(iii) If $|G| = p^n$, then the class of G is at most $n-1$, if $n > 1$.

Proof: (i) Let $\xi \in H \cap \zeta^r G$, $\xi \notin \zeta^{r-1} G$. Then there is an element η of G such that $[Z\xi, Z\eta] \neq Z$ where $Z = \zeta^{r-2} G$. Since $H \lhd G$, $\gamma = [\xi, \eta] \in H$. Also $\gamma \in \zeta^{r-1} G$, but $\gamma \notin Z = \zeta^{r-2} G$. Hence the result.

Lemma 7·2. (i) If $H \lhd G$ and $H \cap Z^r G > H \cap Z^{r-1} G$ for some $r \geq 1$, then $H \cap Z^s G > H \cap Z^{s-1} G$ for all $s = 1, 2, \ldots, r$.

(ii) If $|G| = p^n$ and $|H| = p^r$ and $H \lhd G$, then $H \leq Z^r G$.

(iii) If $G' \neq 1$, then G/ZG is not cyclic.

(iv) If $|G| = p^n$, then, for $n > 1$, the class of G is at most $n-1$.

In particular, groups of order p^2 are Abelian.

Proof: (i) Let $\xi \in H \cap Z^r G$, $\xi \notin H \cap Z^{r-1} G$ and let $r > 1$, $Z = Z^{r-2} G$. Then there is an element η of G such that $[Z\xi, Z\eta] \neq Z$. Since $H \lhd G$, $\gamma = [\xi, \eta] \in H$ by 7·1 (v). Also $\gamma \in Z^{r-1} G$ since $\xi \in Z^r G$. But $Z\gamma \neq Z$ and so $\gamma \notin Z^{r-2} G = Z$. Hence $H \cap Z^{r-1} G > H \cap Z^{r-2} G$.

(ii) follows from (i).

(iii) If G/ZG is cyclic, then $G = \{ZG, \xi\}$ for some ξ and $[\xi, \gamma] = 1$ for all $\gamma \in ZG$. Hence G is Abelian.

(iv) Let $G = Z^c G > Z^{c-1} G > \cdots > ZG > 1$ so that c is the class of G. If $c = 1$, the result follows from $n > 1$. If $c > 1$, then $G/Z^{c-1} G$ is of order at least p^2 and so $|G| \geq p^{c+1}$.

(C) If X is any subset of the group G, we denote by X^G the set of all ξ^α with $\xi \in X$, $\alpha \in G$. Then $\{X^G\}$ is the least normal subgroup of G containing X. It is called the normal closure of X in G. Note that any subgroup of G which is generated by the union of a certain number of classes of conjugates in G is normal in G.

Theorem 7·3 Let H be a subgroup of G and let $H_1, H_2, \ldots, H_r$ be in any order the conjugates of H in G, so that $r = |G : N_G(H)|$. Then

$$\{H^G\} = H_1 H_2 \cdots H_r.$$

This theorem is due to Ito.

Proof. Let $K = \{H_1, H_2, \ldots, H_r\}$ so that $K = \{H^G\}$. Every element $\xi \in K$ can be expressed in the form

$$\xi = \xi_1 \xi_2 \cdots \xi_s \qquad (1)$$

where $\xi_\lambda \in H_{i_\lambda}$, $\lambda = 1, 2, \ldots, s$. We say that the expression (1) then

belongs to the ordered multiplet $i = (i_1, i_2, \dots, i_s)$. Choose (1) so that s is as small as possible; and among the possible expressions for ξ with minimum s, choose (1) so that i comes as early as possible in the lexicographic ordering of ordered multiplets. Suppose if possible that for some $\lambda < \mu$, we have $i_\lambda \geq i_\mu$. Then we have

$$\xi = \xi_1' \xi_2' \cdots \xi_s' \qquad (2)$$

where $\xi_\nu = \xi_\nu'$ for $\nu < \lambda$ and also for $\nu > \mu$; $\xi_\lambda' = \xi_\mu$; and for $\lambda < \alpha \leq \mu$ $\xi_\alpha' = \xi_\mu^{-1} \xi_{\alpha-1} \xi_\mu$. Then (2) belongs to the ordered multiplet $j = (i_1, \dots, i_{\lambda-1}, i_\mu, \dots)$ of length s; and j precedes i in lexicographic order since $i_\mu < i_\lambda$. This contradicts the definition of i. Hence $i_1 \leq i_2 \leq \dots \leq i_s$. But if $i_\lambda = i_{\lambda+1}$, the two neighbouring factors $\xi_\lambda, \xi_{\lambda+1}$ in (1) can be coalesced to a single factor which likewise belongs to $H_{i_\lambda} = H_{i_{\lambda+1}}$, contrary to the minimality of s. Hence $i_1 < i_2 < \dots < i_s$ and so $\xi \in H_1 H_2 \cdots H_r$. Since ξ was any element of K, we thus obtain $K = H_1 H_2 \cdots H_r$ as stated.

(D). **Lemma 7.4** Let $G = \{X\}$ and let $H = \{Y^G\}$. Then $[H, G] = \{Z^G\}$ where Z is the set of all commutators $[\eta, \xi]$ with $\eta \in Y$, $\xi \in X$.

Proof: By 7·1 (iv), $K = [H, G] \lhd G$; also $Z \leq K$. Hence $K_1 = \{Z^G\}$ is contained in $K \leq H$. Let $H_1 = \zeta(G \bmod K_1)$. Since $[\eta, \xi] \in Z \leq K_1$ for all $\eta \in Y$ and all $\xi \in X$, we have $[K_1\eta, K_1\xi] = K_1$. Also G/K_1 is generated by the cosets $K_1\xi$, $\xi \in X$. Hence $K_1\eta \in \zeta(G/K_1)$ i.e. $\eta \in H_1$ for all $\eta \in Y$. But $H_1 \lhd G$ and so $H_1 \geq H = \{Y^G\}$. Thus H/K_1 is a central factor of G and so $K = [H, G] \leq K_1$ by 7·1 (vi). Since $K_1 \leq K$, we obtain $K = K_1$ as required.

We define inductively

$$[\xi_1, \xi_2, \dots, \xi_n] = [[\xi_1, \dots, \xi_{n-1}], \xi_n],$$
$$[H_1, H_2, \dots, H_n] = [[H_1, \dots, H_{n-1}], H_n],$$

for $n = 3, 4, \dots$, where the ξ's and H's are respectively elements and subgroups of G.

The groups $\gamma_n G$ defined inductively by

$$G = \gamma_1 G\,, \quad [\gamma_n G, G] = \gamma_{n+1}(G)\,, \quad n = 1, 2, \cdots$$

are characteristic subgroups of G, by 7·1 (iv) and the series

$$G = \gamma_1 G \geqslant G' = \gamma_2 G \geqslant \gamma_3 G \geqslant \cdots$$

is called the <u>lower central series</u> of G.

Suppose that $G = G_1 \rhd G_2 \rhd G_3 \rhd \cdots$ and that each G_i/G_{i+1} is a central factor of G. Then we have a <u>descending central series</u> of G. By induction on n, we obtain

$$G_n \geqslant \gamma_n G \qquad (n = 1, 2, 3, \cdots).$$

The lower central series of G is the lowermost descending central series of G.

G is nilpotent if and only if $\gamma_{r+1} G = 1$ for some $r \geqslant 0$ and the least such r is the class of G. If c is the class of G, then

$$\zeta^n G \geqslant \gamma_{c-n+1} G \qquad (n = 0, 1, \cdots, c).$$

<u>Lemma 7·5</u> (i) If $G = \{X\}$, then $\gamma_n G$ is generated by all the commutators $[\xi_1, \xi_2, \cdots, \xi_n]$ with $\xi_i \in X$ together with their conjugates in G.

(ii) If $H \lhd G$ and $\gamma_r G \leqslant H(\gamma_{r+1} G)$, then $\gamma_s G \leqslant H(\gamma_{s+1} G)$ for $s = r+1, r+2, \cdots$ and so $\gamma_r G \leqslant H(\gamma_{r+k} G)$ for all $k \geqslant 1$.

(iii) If G is nilpotent and H is any subgroup such that $HG' = G$, then $H = G$.

(iv) If H is a subgroup of the nilpotent group G, then $\gamma_n H \subseteq \gamma_n G$, $n = 1, 2, \cdots$. In particular, H is nilpotent.

Proof: (i) follows from 7·4 by induction on n.

(ii) By hypothesis, every element of $\gamma_r G$ has the form $\eta\zeta$ with $\eta \in H$ and $\zeta \in \gamma_{r+1} G$. Hence $\gamma_{r+1} G$ is generated by elements of the form $[\eta\zeta, \xi] = [\eta, \xi]^{\zeta}[\zeta, \xi]$ with $\xi \in G$. Hence $[\eta, \xi]^{\zeta} \in H$ since $H \lhd G$ and $[\zeta, \xi] \in K = \gamma_{r+2} G$. Since $K \lhd G$, we thus have $\gamma_{r+1} G \leqslant HK$.

(iii). This is a consequence of 6·8. If $H < G$, let M be a maximal subgroup of G containing H. Then by 6·8 (v), $M \lhd G$ and so G/M is cyclic of prime order, and $M \geqslant G'$ by 7·1 (vii). Hence $HG' \leqslant MG' = M < G$, contrary to hypothesis.

(iv) is obvious by induction on n.

(E) Let $H_i \lhd G$, $K_j \lhd G$, $\cdots$, $M_r \lhd G$ for $i=1,\cdots,h$; $j=1,\cdots,k$; $\cdots$; $r=1,\cdots,m$. Then 7·1 (viii) gives the general distributive law of commutation,

$$[\prod_{i=1}^{h} H_i, \prod_{j=1}^{k} K_j, \cdots, \prod_{r=1}^{m} M_r] = \prod_{i,j,\cdots,r} [H_i, K_j, \cdots, M_r], \qquad (1)$$

by induction. The order of the factors is irrelevant since all the groups are norm
In particular, if $H \lhd G$ and $K \lhd G$, we obtain

$$\gamma_n(HK) = \prod [L_1, L_2, \cdots, L_n], \qquad (2)$$

where the product is taken over all 2^n terms having each L_i equal to either H or K. Suppose that in $L = [L_1, L_2, \cdots, L_n]$ just r terms are equal to H and s terms equal to K. By 7·1 (v) and induction, we then obtain $L \leqq \gamma_r(H) \cap \gamma_s(K)$. Here we must interpret $\gamma_0(H) = \gamma_0(K) =$. Consequently (2) gives

$$\gamma_n(HK) \leqq \prod_{r=0}^{n} (\gamma_r(H) \cap \gamma_{n-r}(K)) \qquad (3)$$

Here again the $n+1$ factors are normal in G since e.g. $\gamma_r(H)$ char $H \lhd G$

Suppose now that H and K are nilpotent, of class a and b respecti If we take $n = a+b+1$ in (3), we then have in each factor either $r \geqslant a+1$ or $n-r \geqslant b+1$. But $\gamma_{a+1} H = \gamma_{b+1} K = 1$. Hence γ_{a+b+1} $= 1$ and we obtain

Theorem 7·6. *If H and K are normal subgroups of G and if H and K are nilpotent, of class a and b respectively, then HK is nilpotent of class at most $a+b$.* (Fitting)

Note / The theorem that the product of two normal nilpoten subgroups H and K is nilpotent follows also, as noted by Wendt, fro 6·8 (vi). For if $L = HK$ and $M = H \cap K$, then $|L| = |H| \cdot |K : M|$ by 5·5 (or equally 3·4) and so $|L|_p \, |M|_p = |H|_p \, |K|_p$. If S and are the unique Sylow p-subgroups of H and K respectively, then S char H and so $S \lhd G$. Similarly $T \lhd G$ and so $ST \lhd G$. Now $|S \cap T| \leq |$ Hence $|ST| = |S| \cdot |T : S \cap T| \geqslant |H|_p \, |K|_p / |M|_p = |L|_p$. So $|ST| = |L$ and ST is a Sylow p-subgroup of L. Hence the Sylow subgroups of L are all normal and so L is nilpotent by 6·8 (vi).

Corollary 7.61. Every group G has a normal nilpotent subgroup $\mathfrak{N}G$ which contains every other normal nilpotent subgroup of G. $\mathfrak{N}G$ is called the Fitting subgroup of G. If H sbn G, then $\mathfrak{N}H = H \cap \mathfrak{N}G$. In particular every subnormal nilpotent subgroup of G is contained in the Fitting subgroup of G.

Proof: By 7.6, a normal nilpotent subgroup of maximal order in G contains every normal nilpotent subgroup of G and hence is unique. Clearly $\mathfrak{N}G$ char G. Hence, if $H \trianglelefteq G$, $\mathfrak{N}H \trianglelefteq G$ and so $\mathfrak{N}H \leq H \cap \mathfrak{N}G$. But $H \cap \mathfrak{N}G \trianglelefteq G$ and is nilpotent*, so $H \cap \mathfrak{N}G \leq \mathfrak{N}H$. Thus $\mathfrak{N}H = H \cap \mathfrak{N}$ if $H \trianglelefteq G$. This extends at once to the case of subnormal H. If H is itself nilpotent, then $H = \mathfrak{N}H$.

* Note that a subgroup L of a nilpotent group M of class c is nilpotent of class not exceeding c, since $\gamma_{c+1}L \leq \gamma_{c+1}M = 1$. This remark should have been inserted before.

(F) Let ξ, η, ζ be elements of any group G, let $\alpha = \xi\zeta\xi^{-1}\eta\xi$ and let β and γ be obtained from α by cyclic permutation of ξ, η, ζ. Then $[\xi, \eta^{-1}, \zeta]^\eta = \eta^{-1}(\eta\xi^{-1}\eta^{-1}\xi)\zeta^{-1}(\xi^{-1}\eta\xi\eta^{-1})\zeta\eta = \alpha^{-1}\beta$. Thus we obtain the first part of

Theorem 7.7 (i) $[\xi, \eta^{-1}, \zeta]^\eta\,[\eta, \zeta^{-1}, \xi]^\zeta\,[\zeta, \xi^{-1}, \eta]^\xi = 1$.

(ii) Let H, K and L be subgroups of G. Then any normal subgroup M of G which contains two of the groups $U = [K, L, H]$, $V = [L, H, K]$ and $W = [H, K, L]$ also contains the third.

(iii) In particular, if H, K and L are normal in G, then $U \leq VW$, $V \leq WU$, $W \leq UV$.

(iv) If $L \leq \{H, K\}$ and if $[H, K, L] = 1$, then $[L, H, K] = [L, K, H] \lhd \{H, K\}$.

Proof: (ii). In (i), let $\xi \in H$, $\eta \in K$ and $\zeta \in L$, and suppose that M contains U and V. The three factors in (i) belong respectively to W^η, U^ζ and V^ξ. Since $M \lhd G$, $U^\zeta \leq M^\zeta = M$ and similarly $V^\xi \leq M$. Hence $[\xi, \eta^{-1}, \zeta] \in \eta M \eta^{-1} = M$, and so $M\zeta$ commutes with $M[\xi, \eta^{-1}]$ for all $\xi \in H$, $\eta \in K$. Therefore the centralizer of $M\zeta$ in G/M contains $M[H, K]/M$. This is true for all $\zeta \in L$. Hence $[H, K, L] = W \leq 1$ as required. (iii) is a corollary of (ii), by 7.1 (iv).

(iv) Let C be the centralizer of $[H, K]$ in $J = \{H, K\}$. By 7.1 (iii), $C \lhd J$ and by hypothesis $L \leq C$. Hence $[L, H] \leq C$ by 7.1 (v). Let $\xi \in H$, $\eta \in K$ and $\tau \in [L, H]$. Then $\tau \in C$ and $[\xi, \eta^{-1}] \in [H, K]$ so that τ commutes with $[\xi, \eta^{-1}]$. But $\eta^\xi = [\xi, \eta^{-1}]\eta$ and so 7.1 (ii) gives $[\tau, \eta^\xi] = [\tau, \eta]$. Hence $[L, H, K^\xi] = [L, H, K]$. Since $\xi \in H$, we also have $[L, H] = [L, H]^\xi$ by 7.1 (iii). Hence $[L, H, K]^\xi = [[L, H]^\xi, K^\xi] = [L, H, K^\xi] = [L, H, K]$. Thus H normalizes $[L, H, K]$. By 7.1 (iii), K also normalizes $[L, H, K]$. So $[L, H, K] \lhd J$. But $[K, H, L] = [H, K, L] = 1$ by hypothesis. Interchanging H and K, we therefore find that $[L, K, H] \lhd J$ also. Since $[L, K, H] = [K, L, H]$, (iv) now follows from (iii).

(G) As a corollary of 7·7 (iii), we have

Theorem 7·8 (i) Let $G = H_0 \geq H_1 \geq H_2 \geq \cdots$ be a series of normal subgroups of G and let K be a subgroup of G such that $[H_i, K] \leq H_{i+1}$ for all $i = 0, 1, 2, \ldots$. Then $[H_i, \gamma_n K] \leq H_{i+n}$ for all $i \geq 0$ and $n \geq 1$.

(ii) In any group G, $[\gamma_\ell G, \gamma_m G] \leq \gamma_{\ell+m} G$ and, for $\ell \geq m$, $[\zeta^\ell G, \gamma_m G] \leq \zeta^{\ell-m} G$.

(iii) If $G^{(n)}$ is the n-th derived group of G, then $G^{(n)} \leq \gamma_{2^n} G$.

Proof: (i) by induction on n. For $n=1$, the theorem is true by hypothesis. Let $n > 1$. In 7·7 (ii), take $H = \gamma_{n-1} K$, $L = H_i$ and $M = H_{i+1}$. Then $U = [K, H_i, \gamma_{n-1} K] = [H_i, K, \gamma_{n-1} K] \leq [H_{i+1}, \gamma_{n-1} K]$ by hypothesis and so $U \leq M$ by induction. On the other hand, $V = [H_i, \gamma_{n-1} K, K] \leq [H_{i+n-1}, K]$ by induction and so $V \leq M$ by the hypothesis. Since $M \lhd$ it follows that $W = [\gamma_{n-1} K, K, H_i] = [\gamma_n K, H_i] = [H_i, \gamma_n K] \leq M = H_{i+n}$, as required.

(ii) If each of the sections H_i / H_{i+1} is a central factor of G, we can take $K = G$ in (i). Applying this remark to the lower and upper central series of G gives (ii).

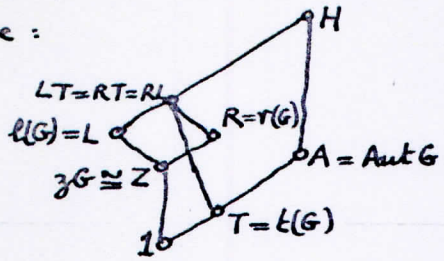
(iii) By induction on n, we may assume $G^{(n)} \leq \gamma_{2^n} G$ for some n, since $G^{(0)} = G = \gamma_1 G$. Then $G^{(n+1)} = [G^{(n)}, G^{(n)}] \leq [\gamma_{2^n} G, \gamma_{2^n} G] \leq \gamma_{2^{n+1}} G$ by (ii).

(H) If $\alpha \in A = \mathrm{Aut}\, G$ and $\xi \in G$, then $r(\xi^\alpha) = r(\xi)^\alpha = \alpha^{-1} r(\xi) \alpha$. Thus A normalizes $R = r(G)$. The group

$$H = AR$$

is called the holomorph of G. Note that H is a transitive subgroup of $\Sigma(G)$ and that A is the stabilizer of 1 in H. By 5·3, the centralizer of R in $\Sigma(G)$ is $L = l(G)$. Both R and L are isomorph with G and $R \cap L = Z$ consists of all the permutations $r(\zeta) = l(\zeta)$ with $\zeta \in \zeta G$. The stabilizer of 1 in RL is $T = t(G)$ the group of

inner automorphisms of G. Hence $A \cap RL = T$. The general picture is as shown here:



Given a group Γ of automorphisms of G, i.e. any subgroup of A, it is often convenient to think of Γ and G as subgroups of a larger group ΓG with $\Gamma \cap G = 1$, $G \lhd \Gamma G$, and $\xi^\alpha = \alpha^{-1}\xi\alpha$ for $\xi \in G$, $\alpha \in \Gamma$. Such a group can be obtained from $\Gamma . r(G)$ by identifying $r(\xi)$ with ξ. We call ΓG the <u>holomorphic extension</u> of G by Γ. This device gives a meaning to the commutators $[\xi, \alpha]$ with $\xi \in G$, $\alpha \in \Gamma$ viz. $\xi^{-1}\xi^\alpha$. Note that the device is purely a notational one.

<u>Theorem 7.9</u> Let Γ be a group of automorphisms of G and suppose that there exists a chain of subgroups $G = G_0 > G_1 > G_2 > \cdots > G_m = 1$ such that $[G_{i-1}, \Gamma] \leq G_i$ for each $i = 1, 2, \cdots, m$. Then:

(i) Every prime divisor p of $|\Gamma|$ also divides $|G_1|$.

(ii) Γ is nilpotent of class at most $\frac{1}{2}m(m-1)$.

(iii) $[G, \Gamma]$ is a normal nilpotent subgroup of G and $\Gamma[G, \Gamma]$ is a normal nilpotent subgroup of ΓG.

(iv) If each $G_i \lhd G$, then the class of Γ is at most $m-1$.

Proof: (i). By induction on m, since $\Gamma = 1$ when $m = 1$. Let α be any element of Γ of prime order p. If $[G_1, \alpha] \neq 1$, then p divides $|G_1|$ by induction. If $[G_1, \alpha] = 1$, there is an element $\xi \in G - G_1$ such that $\zeta = [\xi, \alpha] \neq 1$, since otherwise $\alpha = 1$, which is not the case. Then $\zeta \in G_1$ and so $\zeta^\alpha = \zeta$ by hypothesis. Also $\xi^\alpha = \xi\zeta$, hence $\xi^{\alpha^r} = \xi\zeta^r$ by induction on $r = 1, 2, \cdots$. Since $\alpha^p = 1$, it follows that $\zeta^p = 1$. Hence p divides $|G_1|$ in this case also.

(ii) Define $G_0^* = G$, $G_{i+1}^* = [G_i^*, \Gamma]$, $i = 0, 1, 2, \cdots$. Then by induction on i, we have $G_i^* \leq G_i$ for all i. By 7.1 (iii), $G_{i+1}^* \lhd \{G_i^*, \Gamma\}$.

Hence there is no loss of generality in assuming that $G_{i+1} \lhd \{G_i, \Gamma\}$ for $i = 0, 1, \cdots, m-1$. Since $m = 1$ implies $\Gamma = 1$, we use induction on m and suppose $m > 1$. Hence if $l = \frac{1}{2}(m-1)(m-2)$, we may assume that $\gamma_{l+1}\Gamma$ centralizes G_1. Write $\Gamma_r = \gamma_r\Gamma$, so that $[G, \Gamma, \Gamma_r] = 1$ for all $r > l$; and therefore, by 7·7 (iv), $[\Gamma_r, G, \Gamma] = [\Gamma_r, \Gamma, G] = [\Gamma_{r+1}, G]$ for all $r > l$. Hence $[\Gamma_{l+m}, G] = [\Gamma_{l+m-1}, G, \Gamma] = [\Gamma_{l+m-2}, G, \Gamma, \Gamma] = \cdots$

$$= [\Gamma_{l+1}, G, \underbrace{\Gamma, \Gamma, \cdots, \Gamma}_{m-1}] \leqq [G_1, \underbrace{\Gamma, \Gamma, \cdots, \Gamma}_{m-1}] \leqq [G_2, \underbrace{\Gamma, \cdots, \Gamma}_{m-2}] \leqq G_m = 1.$$

Thus Γ_{l+m} centralizes G and so $\Gamma_{l+m} = 1$ and Γ is nilpotent of class at most $l+m-1 = \frac{1}{2}m(m-1)$ as required.

(iii). By 7·1 (iii), $[G, \Gamma] \lhd G$. Hence $\overline{\Gamma} = \Gamma[G, \Gamma]$ is the normal closure of Γ in ΓG. Taking $G_1 = [G, \Gamma]$, $G_2 = [G_1, \Gamma]$, $\cdots$ we find that ΓG_{i+1} is the normal closure of Γ in ΓG_i. Thus we have

$$\Gamma = \Gamma G_m \lhd \Gamma G_{m-1} \lhd \cdots \lhd \Gamma G_1 = \overline{\Gamma} \lhd \Gamma G.$$

Hence Γ sbn ΓG. By (ii), Γ is nilpotent. Hence by 7·61, $\Gamma \leqq \mathfrak{N}(\Gamma G)$ the Fitting subgroup of ΓG. Hence $\overline{\Gamma} \leqq \mathfrak{N}(\Gamma G)$ and so $\overline{\Gamma}$ is nilpotent. A fortiori, $[G, \Gamma]$ is nilpotent.

(iv) is a corollary of 7·8 (i).

§ 8 Direct Products, Central Products, Residual Products; Abelian groups, Semisimple groups, Wedderburn components of irreducible groups

(A) A group G is called the *direct product* of its subgroups $G_1, G_2, \cdots, G_n$ if (i) each element $\xi \in G$ is uniquely expressible in the form

$$\xi = \xi_1 \xi_2 \cdots \xi_n \quad \text{with } \xi_i \in G_i \quad (i = 1, 2, \cdots, n)$$

and (ii) $[G_i, G_j] = 1$ for $i \neq j$.

If $\eta = \eta_1 \eta_2 \cdots \eta_n$ with $\eta_i \in G_i$, it follows from (ii) that $\xi\eta = \zeta$ has the expression $\zeta_1 \zeta_2 \cdots \zeta_n$ with $\zeta_i = \xi_i \eta_i$. Also $\xi^{-1} = \xi_1^{-1} \xi_2^{-1} \cdots \xi_n^{-1}$. Thus G is determined to within isomorphism by the direct factors $G_1, \cdots, G_n$.

Given n groups $G_1, \cdots, G_n$ not necessarily distinct, the set of all ordered multiplets $\xi = (\xi_1, \xi_2, \cdots, \xi_n)$ with $\xi_i \in G_i$ becomes a group if we define multiplication by the rule $\xi\eta = (\xi_1\eta_1, \cdots, \xi_n\eta_n)$. This implies that $\xi^{-1} = (\xi_1^{-1}, \cdots, \xi_n^{-1})$. This group is called the *Cartesian product* of $G_1, \cdots, G_n$ and is denoted by $G_1 \times G_2 \times \cdots \times G_n$. If G is the direct product of subgroups $G_1, \cdots, G_n$ we have a natural isomorphism of G onto the Cartesian product $G_1 \times \cdots \times G_n$.

In a direct product, the order of the direct factors is irrelevant. In a Cartesian product, any permutation of the factors determines an isomorphism onto another Cartesian product.

If G is the direct product of the subgroups $(G_\alpha)_{\alpha \in \Lambda}$ and if Λ is expressed as the union of a number of disjoint subsets $\Lambda_1, \cdots, \Lambda_r$, then G is the direct product of the subgroups $G_1, \cdots, G_r$, where G_i is the product (also direct) of the G_α with $\alpha \in \Lambda_i$.

Lemma 8.1 Let G be generated by the subgroups $G_1, \cdots, G_n$. In order that G shall be the direct product of these subgroups it is necessary and sufficient that (i) each $G_i \triangleleft G$ and (ii) $G_i \cap G_1 G_2 \cdots G_{i-1} = 1$ for $i = 2, 3, \cdots, n$.

Proof: By (i), $G_i^* = G_1 G_2 \cdots G_{i-1}$ is a normal subgroup of G for each i. By (ii) and 6.9, it follows that $[G_i, G_i^*] = 1$ and so $[G_i, G_j] = 1$ for $i \neq j$. Then (ii) further ensures that each $\xi \in G$ is uniquely expressible in

the form $\xi_1 \xi_2 \cdots \xi_n$ with $\xi_i \in G_i$.

(B) **Lemma 8.2** (i) A nilpotent group is the direct product of its Sylow subgroups.

(ii) If G is the direct product of subgroups $G_1, \cdots, G_n$ whose orders $m_1, \cdots, m_n$ are coprime in pairs, and if H is any subgroup of G, then H is the direct product of the subgroups $H_i = H \cap G_i$ $(i = 1, 2, \cdots, n)$ and $\operatorname{Aut} G \cong \operatorname{Aut} G_1 \times \cdots \times \operatorname{Aut} G_n$.

(iii) If in (ii), the subgroups G_i are all cyclic, then G is cyclic.

(iv) If G is any group and ξ is any element of G of order $l = l_1 l_2 \cdots l_n$ where $(l_i, l_j) = 1$ for $i \neq j$, then $\xi = \xi_1 \xi_2 \cdots \xi_n$ with $[\xi_i, \xi_j] = 1$ for $i \neq j$ and with ξ_i of order l_i for each $i = 1, 2, \cdots, n$; moreover the elements $\xi_i \in G$ are uniquely determined by these conditions and are powers of ξ.

Proof: (i) Let $G_1, \cdots, G_n$ be the distinct Sylow subgroups $\neq 1$ of the nilpotent group G. Then $G_i \lhd G$ for each i, by 6.8 (vi). Also $|G| = \prod_i |G_i|$ and so $G = G_1 G_2 \cdots G_n$, and we have uniqueness in the expression $\xi = \xi_1 \cdots \xi_n$ of the elements $\xi \in G$ with $\xi_i \in G_i$. Also $[G_i, G_j] = 1$ for $i \neq j$, by 6.9. The result now follows.

(ii) If ϖ_i is the set of primes dividing m_i, then G_i is a normal S_{ϖ_i}-subgroup of G. We have $H_i \lhd H$ and $H_i \leq G_i$ so $[H_i, H_j] = 1$ for $i \neq j$, since then $[G_i, G_j] = 1$. $H/H_i \cong G_i H / G_i$ and so $|H : H_i|$ is a ϖ_i'-number since $|G_i H : G_i|$ divides $|G : G_i| = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_n$. Hence H_i is a normal S_{ϖ_i}-subgroup of H. Since $|H|$ divides $|G| = m_1 m_2 \cdots m_n$ it follows that $H = H_1 H_2 \cdots H_n$ and uniqueness for the expression of the elements of H in the form $\xi = \xi_1 \cdots \xi_n$ with $\xi_i \in H_i$ follows from the corresponding result for G. Hence H is the direct product of $H_1, \cdots, H_n$.

Let $\alpha \in A = \operatorname{Aut} G$. Since G_i char G by 5.8, α leaves each G_i invariant and induces in G_i an automorphism α_i. α is uniquely determined by $\alpha_1, \alpha_2, \cdots, \alpha_n$ since $G = G_1 G_2 \cdots G_n$. Given $\xi = \xi_1 \cdots \xi_n \in G$ with $\xi_i \in G_i$ and given $\alpha_i \in A_i = \operatorname{Aut} G_i$, the mapping $\xi \to \xi^\alpha$ of G

defined by $\xi^\alpha = \xi_1^{\alpha_1} \cdots \xi_n^{\alpha_n}$ is an automorphism of G which induces α_i on G_i. If α and $\beta \in A$, then $(\alpha\beta)_i = \alpha_i\beta_i$ for each i. Hence $A \cong A_1 \times \cdots \times A_n$, as stated.

(iii) If H is cyclic of order $m_1 m_2 \cdots m_n$ with $(m_i, m_j) = 1$ for $i \neq j$, then H has a subgroup H_i of order m_i and H_i is cyclic by 2.5. By (ii) H is the direct product of $H_1, \ldots, H_n$. Hence $H \cong H_1 \times \cdots \times H_n$ and any direct product of cyclic subgroups of orders $m_1, \ldots, m_n$ is isomorphic with H, hence cyclic.

(iv). Take $H = \{\xi\}$ with $m_i = l_i$, $i = 1, 2, \ldots, n$. Then $\xi = \xi_1 \cdots \xi_n$ with $\xi_i \in H_i$, $|H_i| = l_i$. The order of ξ_i is precisely l_i since otherwise the order of ξ would be less than $l = l_1 l_2 \cdots l_n$. Each ξ_i is a power of H, hence $[\xi_i, \xi_j] = 1$ for all i, j. Conversely, given elements $\xi_1, \ldots, \xi_n$ in G with these properties, we have $\xi^r = \xi_1^r \cdots \xi_n^r$ and so $\xi^{l/l_i} = \xi_i^{l/l_i}$, which has order l_i since otherwise ξ would be of order less than l. Hence ξ_i is a power of ξ_i^{l/l_i} and therefore $\xi_i \in H$ for each i. Thus $\xi_1, \ldots, \xi_n$ are uniquely determined by ξ.

(C) 8.2 (ii) indicates that the properties of direct products of groups whose orders are coprime are easily reducible to a study of the structure of the direct factors. ~~This is not the case in general.~~ In particular, the theory of nilpotent groups reduces trivially to the theory of p-groups. When the direct factors are not of coprime orders, however, more difficult questions arise. For example, in this case, the direct factors need not be characteristic subgroups.

Consider the subgroups H of the direct product $G = G_1 G_2$ of two groups G_1, G_2. Let $H_i = H \cap G_i$ $(i = 1, 2)$ and let $\overline{H}_1 = G_1 \cap HG_2$, $\overline{H}_2 = G_2 \cap HG_1$. Let $\xi = \eta\gamma_2 \in \overline{H}_1$ where $\eta \in H$, $\gamma_2 \in G_2$ and let $\alpha \in H_1$. Then $\alpha^\eta \in H_1 = H \cap G_1$ since $\alpha \in G_1 \lhd G$, and $\alpha^\xi = \alpha^\eta$ since $[G_1, \gamma_2] = 1$. Hence $H_1 \lhd \overline{H}_1$ and similarly $H_2 \lhd \overline{H}_2$. If $\xi = \xi_1\xi_2 \in G$ with $\xi_i \in G_i$, then the mapping $\xi \to \xi_i$ is homomorphic. Call this mapping θ_i $(i = 1, 2)$. We have $\theta_i(H) = \overline{H}_i$ and the restriction of

θ_i to H has kernel H_2, so that $\overline{H}_1 \cong H/H_2$; and similarly $\overline{H}_2 \cong H/H_1$. Suppose $\xi = \xi_1\xi_2$ and $\eta = \eta_1\eta_2$ lie in H where ξ_i, η_i are in G_i and hence in $\overline{H}_i$. Then $\xi\eta^{-1} = (\xi_1\eta_1^{-1})(\xi_2\eta_2^{-1}) \in H$. Hence $\xi_1\eta_1^{-1} \in H_1$ implies $\xi_2\eta_2^{-1} \in H_2$ and conversely. Hence the correspondence $H_1\xi_1 \to H_2\xi_2$ is one-to-one and is an isomorphism mapping $\overline{H}_1/H_1$ onto $\overline{H}_2/H_2$.

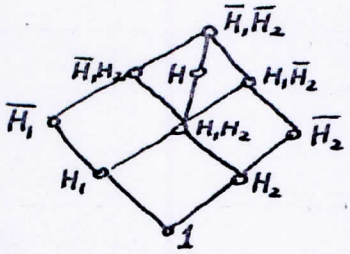
Conversely, let $\overline{H}_1/H_1$ and $\overline{H}_2/H_2$ be any two isomorphic sections of G_1 and G_2 respectively and let θ be any isomorphism of the first onto the second. Let H be the set of all $\xi = \xi_1\xi_2 \in G$ such that $\xi_i \in \overline{H}_i$ and $(H,\xi_1)^\theta = H_2\xi_2$. If $\eta = \eta_1\eta_2$ also lies in H, then $\xi_i\eta_i \in \overline{H}_i$ and $(H,\xi_1\eta_1)^\theta = (H,\xi_1)^\theta(H,\eta_1)^\theta = (H_2\xi_2)(H_2\eta_2) = H_2\xi_2\eta_2$ and so $\xi\eta \in H$. Thus H is a subgroup of G. Thus we can state

Theorem 8.3 Let G be the direct product of the subgroups G_1 and G_2. Then there is a one-to-one correspondence between the subgroups H of G and the set of all isomorphisms θ of a section $\overline{H}_1/H_1$ of G_1 onto a section $\overline{H}_2/H_2$ of G_2. In this correspondence, $H_i = H \cap G_i$ and $\overline{H}_1 = G_1 \cap HG_2$, $\overline{H}_2 = G_2 \cap HG_1$. An element $\xi = \xi_1\xi_2$ of G with $\xi_i \in G_i$ lies in H if and only if $\xi_i \in \overline{H}_i$ $(i=1,2)$ and $(H,\xi_1)^\theta = H_2\xi_2$. (Goursat)

(D). It is important to consider the case in which G admits a group of operators Γ leaving the direct factors G_1 and G_2 of G invariant. We wish to know in this case which subgroups H of G are Γ-invariant. If H is Γ-invariant, then so are the subgroups H_i and $\overline{H}_i$. Hence any $\alpha \in \Gamma$ induces an automorphism in each of the two ~~first~~ sections $\overline{H}_1/H_1$ and $\overline{H}_2/H_2$. If $\xi_1\xi_2 = \xi \in H$ with $\xi_i \in \overline{H}_i$, we then have also $\xi^\alpha = \xi_1^\alpha\xi_2^\alpha \in H$ and hence $(H,\xi_1^\alpha)^\theta = H_2\xi_2^\alpha = (H,\xi_1)^{\theta\alpha}$. In other words, the isomorphism θ of 8.3 must commute with every $\alpha \in \Gamma$. Conversely, if this condition is fulfilled in addition to the Γ-invariance of the $H_i, \overline{H}_i$, then H is clearly Γ-invariant. This gives, as an essential supplement to 8.3,

Theorem 8.4 If in 8.3 the group G admits a group of operators Γ leaving G_1 and G_2 invariant, then the subgroup H of G is Γ-invariant if and only if the subgroups $\overline{H}_i$, H_i $(i=1,2)$ are also Γ-invariant and in addition $(H,\xi_1)^{\alpha\theta} = (H,\xi_1)^{\theta\alpha}$ for all $\alpha \in \Gamma$ and $\xi_1 \in \overline{H}_1$. In particular, $H \lhd G$ if and only if $\overline{H}_i/H_i$ is a central factor of G_i for $i=1,2$.

In the case $H \lhd G$, we have $\Gamma = G$ and so the H_i and $\overline{H}_i$ must be normal in G or, what is equivalent, normal in G_i $(i=1,2)$. In addition, taking $\alpha \in G_1$ we find that $(H,\xi_1^{\alpha})^{\theta} = (H,\xi_1)^{\theta\alpha} = (H,\xi_1)^{\theta}$ since then $[G_2,\alpha] = 1$. Hence $H,\xi_1^{\alpha} = H,\xi_1$ for all $\alpha \in G_1$ and $\xi_1 \in \overline{H}_1$ so that $\overline{H}_1/H_1$ is a central factor of G_1. Similarly, taking $\beta \in G_2$, we have $(H,\xi_1)^{\theta\beta} = (H,\xi_1)^{\beta\theta} = (H,\xi_1)^{\theta} = H_2\xi_2$ say, so that $H_2\xi_2^{\beta} = H_2\xi_2$ for all $\beta \in G_2$ and $\xi_2 \in \overline{H}_2$. Thus $\overline{H}_2/H_2$ is a central factor of G_2. Conversely, these conditions are sufficient to ensure that $(H,\xi_1)^{\gamma\theta} = (H,\xi_1)^{\theta\gamma}$ for all $\gamma \in G$, and so they imply $H \lhd G$.



Note that $H \lhd G$ implies $H_1H_2 \lhd G$ and G/H_1H_2 is the direct product of G_1H_2/H_1H_2 with G_2H_1/H_1H_2. It is therefore isomorphic with the Cartesian product $G_1/H_1 \times G_2/H_2$. In this Cartesian product $\overline{H}_1/H_1 \times \overline{H}_2/H_2$ is a subgroup of the centre $\mathfrak{z}(G_1/H_1) \times \mathfrak{z}(G_2/H_2)$. Thus the step from G to G/H may be thought to take place in two steps. First we form the direct product $\overline{G}_1\overline{G}_2$ where $\overline{G}_i \cong G_i/H_i$. Then $H \cong \overline{G}_1\overline{G}_2/K$, where K is a subgroup of the centre of $\overline{G}_1\overline{G}_2$ consisting of all elements $\overline{\xi}_1\overline{\xi}_2$ with $\overline{\xi}_i \in K_i \leq \mathfrak{z}\overline{G}_i$ with $\overline{\xi}_2 = \overline{\xi}_1^{\theta}$, where θ is an isomorphism of K_1 onto K_2, K_1 and K_2 being necessarily isomorphic subgroups of $\mathfrak{z}\overline{G}_1$, $\mathfrak{z}\overline{G}_2$ respectively. The group $\overline{G}_1\overline{G}_2/K \cong$ is thus obtained from the direct product $\overline{G}_1\overline{G}_2$ by "identifying" correspondi

$\overline{\xi}_1 = (\overline{\xi}_2)^{-1}$ is an isomorphism $\overline{\xi}_1 \to (\overline{\xi}_2)^{-1}$ of a subgroup K_1 of $\mathfrak{Z}\overline{G}_1$ onto a subgroup K_2 of $\mathfrak{Z}\overline{G}_2$. A group constructed in this way is often called a central product of the two groups $\overline{G}_1$ and $\overline{G}_2$.

The last part of 8.4 may now be stated as follows: any homomorphic image G/H of the direct G of two groups G_1 and G_2 is isomorphic with some central product of homomorphic images $\overline{G}_1 = G_1/H_1$ and $\overline{G}_2 = G_2/H_2$ of G_1 and G_2

($\mathfrak{E}$). Let H be a subgroup of the Cartesian product $G = G_1 \times G_2 \times \cdots \times G_n$ If for each $i = 1, 2, \cdots, n$ and each $\xi_i \in G_i$, there is an element of H whose i-th coordinate is precisely ξ_i, then H is called a residual product of $G_1, G_2, \cdots, G_n$; or sometimes though less appropriately a subdirect product of the G_i. If $\xi = (\xi_1, \cdots, \xi_n) \in G$, the mapping $\theta_i : \xi \to \xi_i$ is a homomorphism of G onto G_i. H is a residual product of the G_i if and only if $H^{\theta_i} = G_i$ for each i.

Lemma 8.5 Let $K_i \lhd G$ $(i = 1, 2, \cdots, n)$ and let $K = \bigcap_{i=1}^{n} K_i$. Then G/K is isomorphic with a residual product of the groups G/K_i $(i = 1, 2, \cdots, n$

The mapping

$$K\xi \to (K_1\xi, \cdots, K_n\xi) \qquad (\xi \in G)$$

is the isomorphism in question. For this mapping is homomorphic owing to $K_i \lhd G$ for each i. If $K\xi$ and $K\eta$ have the same image, then $K_i\xi = K_i\eta$ for all i and so $\xi\eta^{-1} \in K = \bigcap_i K_i$, whence $K\xi = K\eta$. Thus the mapping is an isomorphism. The image group is obviously a residual product of the G/K_i.

(F) **Lemma 8.6** Let G be an Abelian p-group and let ξ be any element of G whose order is as large as possible. Then G is the direct product of $X = \{\xi\}$ and Y, where Y is any subgroup of G which is maximal with respect to the condition $X \cap Y = 1$.

Proof: We have only to show that $XY = G$ since G is Abelian. Let $\overline{G} = G/Y$, $\overline{X} = XY/Y \cong X$. By the maximal property of Y, every subgroup $\overline{H} \neq 1$ in $\overline{G}$ contains elements $\neq 1$ of the cyclic subgroup $\overline{X} = \{\overline{\xi}\}$. Let $\overline{\eta}$ be any element of $\overline{G}$ and let $\overline{\eta}^{p^r}$ be the first positive power of $\overline{\eta}$ to lie in $\overline{X}$, i.e. $\{\overline{\eta}^{p^r}\} = \{\overline{\eta}\} \cap \overline{X}$. Since $|\overline{X}| = |X|$, the order of $\overline{\eta}$ cannot exceed the order of $\overline{\xi}$, by our choice of ξ. Hence $\{\overline{\eta}^{p^r}\} = \{\overline{\xi}^{p^s}\}$ for some $s \geq r$, and so for a suitable integer m, the element $\overline{\eta}\,\overline{\xi}^{m}$ has order p^r and $\overline{H} = \{\overline{\eta}\,\overline{\xi}^{m}\}$ then has intersection 1 with $\overline{X}$. Hence $\overline{\eta}\,\overline{\xi}^{m} = 1$ and so $\overline{\eta} \in \overline{X}$. Thus $\overline{G} = \overline{X}$ and $G = XY$ as required.

In an Abelian p-group G, the elements ξ such that $\xi^{p^m} = 1$ form a characteristic subgroup $\Omega_m G$ and the elements η of the form $\eta = \xi^{p^m}$ fo some $\xi \in G$ form another characteristic subgroup $U_m G$.

An immediate corollary of 8.6 is

Theorem 8.7 (i) Every Abelian p-group G is the direct product of a certain number of cyclic subgroups $X_i = \{\xi_i\}$ $(i = 1, 2, \cdots, r)$. If $|X_i| = p^{\lambda_i}$, we can arrange that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0$. The partition λ whose parts are $\lambda_1, \lambda_2, \cdots, \lambda_r$ is called the <u>type</u> of G and the numbers λ_i are the <u>invariants</u> of G. The ordered set $\xi_1, \cdots, \xi_r$ is called a <u>basis</u> of G.

(ii) Two Abelian p-groups are isomorphic if and only if they have the same type.

Proof: (i) follows from 8.6 by induction on $|G|$, since we can then assum $X_1 = X$ and that Y is the direct product of suitable cyclic subgroups $X_2, \cdots$.

(ii) Every element of G is uniquely expressible in the form

$$\xi = \xi_1^{\alpha_1} \xi_2^{\alpha_2} \cdots \xi_r^{\alpha_r} \quad \text{with} \quad 0 \leq \alpha_i < p^{\lambda_i}.$$

$\xi \in \Omega_m G$ if and only if $\alpha_i p^m \equiv 0 \bmod p^{\lambda_i}$ for each i, which means p^m choices for α_i if $\lambda_i \geq m$ and p^{λ_i} choices if $\lambda_i \leq m$. Hence $|\Omega_m G| = p^{\rho_1 + \rho_2 + \cdots + \rho_m}$, where ρ_m is the number of values of i for which $\lambda_i \geq m$. We have $\rho_1 \geq \rho_2 \geq \cdots \geq \rho_\ell > \rho_{\ell+1} = 0$, where $\ell = \lambda_1$, $r = l$. The partition ρ whose parts are $\rho_1, \cdots, \rho_\ell$ is the <u>conjugate partition</u> to λ and the relation between ρ and λ is symmetrical: $\rho = \lambda'$, $\rho' = \lambda$. Now G determines ρ uniquely because $|\Omega_m G : \Omega_{m-1} G| = p^{\rho_m}$ for $m = 1, 2, \ldots$. Hence G determines λ uniquely.

Note that the mapping $\xi \to \xi^{p^m}$ $(\xi \in G)$ is a homomorphism of G onto $U_m G$ with kernel $\Omega_m G$. Hence

$$G/\Omega_m G \cong U_m G \quad \text{and} \quad |U_{m-1} G : U_m G| = p^{\rho_m} = |\Omega_m G : \Omega_{m-1} G|.$$

<u>Corollary 8.71</u> Every finite Abelian group G is the direct product of cyclic subgroups of orders $h_1, h_2, \ldots, h_r$ such that $h_r > 1$ and h_{i+1} divides h_i for each $i = 1, \ldots, r-1$. The numbers $h_1, \ldots, h_r$ are uniquely determined by G subject to these conditions. They are called the <u>elementary divisors</u> of G.

Note that if G is an Abelian p-group of type λ, then the elementary divisors of G are the numbers $p^{\lambda_1}, p^{\lambda_2}, \ldots, p^{\lambda_r}$ where $\lambda_1, \ldots, \lambda_r$ are the parts of λ.

Proof: By 8.2 (i), G is the direct product of its Sylow subgroups $=$ say $G_1, \ldots, G_s$ where $|G_j| = p_j^{n_j}$. Let the invariants of G_j be $\lambda_{j1} \geq \lambda_{j2} \geq \cdots \geq \lambda_{jr_j} > 0$ and let $r = \max r_j$ $(j = 1, 2, \ldots, s)$. Let $\xi_{j1}, \ldots, \xi_{jr_j}$ be a basis of G_j and define $\xi_{jk} = 1$ if $r_j < k \leq r$. Let $\xi_i = \xi_{1i} \xi_{2i} \cdots \xi_{si}$ $(i = 1, 2, \ldots, r)$. Then $X_i = \{\xi_i\}$ is of order $h_i = p_1^{\lambda_{1i}} p_2^{\lambda_{2i}} \cdots p_s^{\lambda_{si}}$ where $\lambda_{ji} = 0$ if $r_j < i \leq r$. Also X_i is the direct product of the cyclic groups $\{\xi_{1i}\}, \{\xi_{2i}\}, \cdots, \{\xi_{si}\}$. Hence G is the direct product of $X_1, \ldots, X_r$ and by construction the numbers $h_1, \ldots, h_r$ satisfy the conditions of 8.71. Conversely, these conditions ensure that $\lambda_{j1} \geq \lambda_{j2} \geq \cdots \geq \lambda_{jr} \geq 0$ for each $j = 1, 2, \ldots, s$ and therefore imply that the Sylow p_j-subgroup G_j of G has type $\lambda^{(j)}$ where

$\lambda^{(j)}$ is the partition whose parts are those λ_{ji} which are positive. Hence the elementary divisors $h_1, \cdots, h_r$ are uniquely determined by G.

(G). An Abelian p-group G of type (1^n) is called <u>elementary</u>. An Abelian p-group G is elementary if and only if it has no elements of order p^2.

If $\xi_1, \cdots, \xi_r$ is a basis of the Abelian p-group G and if $\alpha \in \mathrm{Aut}\, G$ then $\xi_1^\alpha, \cdots, \xi_r^\alpha$ is also a basis of G. $\xi_i^\alpha = \xi_i$ for all $i = 1, 2, \cdots, r$ implies that α is the identity on G. If $\eta_1, \cdots, \eta_r$ is an arbitrary basis of G, then the mapping $\xi_i \to \eta_i$ $(i = 1, 2, \cdots, r)$ determines uniquely an automorphism β of G via

$$\xi_1^{\alpha_1} \xi_2^{\alpha_2} \cdots \xi_r^{\alpha_r} \to \eta_1^{\alpha_1} \eta_2^{\alpha_2} \cdots \eta_r^{\alpha_r} \qquad (0 \le \alpha_i < p^{\lambda_i})$$

where λ is the type of G. Hence the number $|\mathrm{Aut}\, G|$ of automorphisms of G is equal to the number of bases of G.

When G is elementary, $\eta_1, \eta_2, \cdots, \eta_n$ is a basis of G if and only if $Y_s = \{\eta_1, \eta_2, \cdots, \eta_s\}$ is of order p^s for each $i = 1, 2, \cdots, n$. Given Y_{s-1}, this leaves precisely $p^n - p^{s-1}$ choices for η_s. Hence $|\mathrm{Aut}\, G|$ is equal to $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Suppose next that G has n invariants all equal to m, so that $|G| = p^{nm}$ and $G/\mho_1 G$ is elementary of order p^n. If $\xi_1, \cdots, \xi_n$ is a basis of G, then $H\xi_1, \cdots, H\xi_n$ generates G/H where H is any subgroup of G. Taking $H = \mho_1 G$, this implies that $H\xi_1, \cdots, H\xi_n$ is then a basis of G/H. Conversely, if this is so, then each ξ_i has order p^m and the group $X = \{\xi_1, \cdots, \xi_n\}$ coincides with G. For if $X < G$, then there is a subgroup Y of index p in G such that $X \le Y$ and we have $H = \mho_1 G \le Y$, whence $HX \le G$ and $H\xi_1, \cdots, H\xi_n$ could not be a basis of G/H. Since $|H| = p^{n(m-1)}$, we thus have $|\mathrm{Aut}\, G| = p^{n^2(m-1)}(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$ in this case. Note that the automorphisms α of G which transform the characteristic quotient group $G/\mho_1 G$ identically form a normal subgroup A_1 of $A = \mathrm{Aut}\, G$, that $|A_1| = p^{n^2(m-1)}$ and that A/A_1 is isomorphic with

Aut G/U_1G.

Now let G be any Abelian p-group, let $\xi_1, \cdots, \xi_r$ and $\eta_1, \cdots, \eta_r$ be any two bases of G and suppose that G has exactly n invariants equal to m. Let $\xi_{a+1}, \xi_{a+2}, \cdots, \xi_{a+n}$ be those ξ's which have order p^m and let $X = \{\xi_1, \xi_2, \cdots, \xi_a, \xi_{a+n+1}, \cdots, \xi_r\}$ be the subgroup generated by the remaining ξ's. Then no element of order p in X can belong to the set $U_{m-1}G - U_mG$. On the other hand, every element of order p in $Y = \{\eta_{a+1}, \eta_{a+2}, \cdots, \eta_{a+n}\}$ lies in $U_{m+1}G - U_mG$. Hence $X \cap Y = 1$ and so G is the direct product of the two subgroups X and Y. It follows that

$$\xi_1, \xi_2, \cdots, \xi_a, \eta_{a+1}, \eta_{a+2}, \cdots, \eta_{a+n}, \xi_{a+n+1}, \cdots, \xi_r$$

is a basis of G. In other words, we can exchange the elements of given order p^m in the ξ-basis for the corresponding elements of the η-basis and obtain a new basis. This is called the <u>exchange property</u> of the bases of an Abelian p-group.

Now the number of different subgroups $Y, Y_1, Y_2, \cdots$ of G such that G is the direct product of X with Y_i, i.e. the number of subgroups Y_i such that $X \cap Y_i = 1$ and $XY_i = G$, is equal to the number of distinct homomorphisms of Y into X. This is a particular case of 8.2. Hence the number of different ordered sets $\eta_{a+1}, \cdots, \eta_{a+n}$ of elements of order p^m which can occur in some basis or other of G is equal to

$$a_m = |\mathrm{Hom}(Y, X)| \cdot |\mathrm{Aut}\, Y|. \qquad (1)$$

And by the exchange property, $|\mathrm{Aut}\, G| = \prod_{m=1}^{\infty} a_m$, where $a_k = 1$ if G has no invariants equal to k.

<u>Lemma 8.8</u> Let X and Y be Abelian groups, let α and β be homomorphisms of Y into X and define the sum $\alpha+\beta$ to be the mapping $\eta \to \eta^{\alpha+\beta} = \eta^\alpha \eta^\beta$ $(\eta \in Y)$. Then $\alpha+\beta \in H = \mathrm{Hom}(Y, X)$ and with this addition, H becomes an additive (Abelian) group. If X and Y are Abelian p-groups of types λ and μ respectively, then H is an Abelian p-group of type $\lambda \otimes \mu$, where the parts of $\lambda \otimes \mu$ are the numbers $\min(\lambda_i, \mu_j)$, $(i = 1, 2, \cdots, r\,;\ j = 1, 2, \cdots, s)$, and where

λ and μ have r and s parts respectively.

Note that if $\nu = \lambda \otimes \mu$, then the parts of the conjugate ν' of ν are the numbers $\lambda_1'\mu_1'$, $\lambda_2'\mu_2'$, $\cdots$, $\lambda_t'\mu_t'$, where $t = \min(\lambda_1, \mu_1)$ and λ', μ' are the partitions conjugate to λ, μ respectively.

The verification that H is an additive Abelian group is immediate. The zero element of H maps Y into the unit subgroup of X. In the p-group case, if $\xi_1, \cdots, \xi_r$ and $\eta_1, \cdots, \eta_s$ are bases of X and Y respectively, then the elements α_{ij} $(i = 1, \cdots, r\,;\ j = 1, \cdots, s)$ of H defined by

$$\alpha_{ij} : \eta_j \to \xi_i^{\,p^{\max(0,\lambda_i - \mu_j)}} \quad ; \quad \eta_k \to 1 \quad (k \neq j)$$

form a basis of H. The order of α_{ij} is precisely $p^{\min(\lambda_i, \mu_j)}$. The number of pairs (i,j) such that $\min(\lambda_i, \mu_j) \geq m$ is equal to $\lambda_m'\mu_m'$.

Note that $\mathrm{Hom}(Y, X)$ and $\mathrm{Hom}(X, Y)$ have the same type. An Abelian group isomorphic with $H = \mathrm{Hom}(Y, X)$ is often called the <u>tensor product</u> of X and Y.

We now use 8.8 and equation (1) to calculate $|\mathrm{Aut}\, G|$ for an Abelian p-group G of arbitrary type $\lambda = (1^{r_1} 2^{r_2} 3^{r_3} \cdots)$. Here Y is of type (m^{r_m}) with r_m invariants equal to m. Define the polynomial f_n by the equation

$$f_n(x) = (1-x)(1-x^2)\cdots(1-x^n) \qquad (n = 1, 2, \cdots)$$

and understand $f_0(x) = 1$. Then we have seen that $|\mathrm{Aut}\, Y| = p^{m r_m^2} f_{r_m}(\tfrac{1}{p})$. The conjugate of the partition (m^{r_m}) is the partition $(r_m, r_m, \cdots, r_m)$ with m parts all equal to r_m. The conjugate of the type of X has parts $\lambda_1' - r_m$, $\lambda_2' - r_m$, $\cdots$, $\lambda_m' - r_m$, $\lambda_{m+1}', \cdots$. Hence $H = \mathrm{Hom}(Y, X)$ has type ν where ν' has the parts $r_m(\lambda_1' - r_m)$, $r_m(\lambda_2' - r_m)$, $\cdots$, $r_m(\lambda_m' - r_m)$. Now $r_m = \lambda_m' - \lambda_{m+1}'$ and $|H| = p^{-m r_m^2 + \sum_{i=1}^{m} r_m \lambda_i'}$. Hence $|\mathrm{Aut}\, G| = p^g \prod_{m=1}^{\infty} f_{r_m}(\tfrac{1}{p})$ where $g = \sum_{i \leq m} r_m \lambda_i' = \sum_{i=1}^{\infty} (\lambda_i')^2$. Thus we obtain

$$i, m = 1, 2, 3, \cdots$$

<u>Corollary 8.81</u> Let G be an Abelian p-group of type λ, let g be the sum of the squares of the parts of the partition conjugate to λ and let $f_n(x) = (1-x)(1-x^2)\cdots(1-x^n)$, with $f_0(x) = 1$. Then

$|\mathrm{Aut}\, G| = p^{g} \prod_{m=1}^{\infty} f_{r_m}(\tfrac{1}{p})$, where $\lambda = (1^{r_1} 2^{r_2} \dots)$ and so the numbers r_m are the multiplicities of the different parts of λ.

(H) A group is called <u>semisimple</u> if it is the direct product of one or more simple subgroups each of composite order, or if it is 1.

<u>Lemma 8.91</u> (i) Let H be a semisimple group. Then every subnormal subgroup of H is normal and is a direct factor of H and is itself semisimple.

(ii) Let H and K be normal semisimple subgroups of G, let $M = H \cap K$ and let $L = C_{HK}(M)$. Then HK is semisimple and is the direct product of L and M.

Proof: (i) Let the direct factors of H be $H_1, H_2, \dots, H_n$, each H_i being simple of composite order, and let $\xi = \xi_1 \xi_2 \cdots \xi_n$ with $\xi_i \in H_i$. Then if $\eta_i \in H_i$, we have $[\xi, \eta_i] = [\xi_i, \eta_i]$. If $\xi_i \neq 1$, it follows that $X = \{\xi^H\}$ contains H_i, since H_i is simple but not Abelian. Hence every normal subgroup M of H is the product of certain of the simple direct factors H_i. Thus M is also semisimple. It then follows that every subnormal subgroup of H is a direct factor of H. Clearly H has exactly 2^n distinct direct factors.

(ii) Since $K \trianglelefteq G$, we have $M \trianglelefteq H$ and so $H = ML_1$ is the direct product of M with a subgroup L_1 and both M and L_1 are semisimple. Similarly K is the direct product of M with a semisimple subgroup L_2. We have $L_1 \leq L$ and $L_2 \leq L$ and so $[L_1, L_2] \leq [H, K] \cap L$. But $[H, K] \leq M$, by the normality of H and K; while $M \cap L = 1$ since $\mathfrak{z} M = 1$. Hence $[L_1, L_2] = 1$. But $L_1 \cap L_2 \leq L \cap M = 1$ and so the product $L_1 L_2$ is direct. Since $|HK| = |M| \cdot |L_1| \cdot |L_2|$, we have $HK = ML_1L_2$; and $L \cap M = 1$ ensures that $L = L_1 L_2$ is the direct product of the semisimple groups L_1 and L_2, hence itself semisimple; while HK is the direct product of L and M, since L and M are normal in G.

Let $\mathfrak{X}$ be any class of groups, such that (i) all groups of order 1 belong to $\mathfrak{X}$; and (ii) if $G \in \mathfrak{X}$ and $G \cong G_1$, then $G_1 \in \mathfrak{X}$. We shall always understand the expression "class of groups" to imply (i) and (ii').

Lemma 8.92 Suppose that in every group G the product of two normal $\mathfrak{X}$-subgroups always belongs to $\mathfrak{X}$; and that every normal subgroup of an $\mathfrak{X}$-group is an $\mathfrak{X}$-group. Then every group G has a uniquely determined maximal normal $\mathfrak{X}$-subgroup $\mathfrak{X}G$. If H sbn G, then $\mathfrak{X}H = H \cap \mathfrak{X}G$. In particular, $\mathfrak{X}G$ contains every subnormal $\mathfrak{X}$-subgroup of G.

The argument is the same as for 7.61, which is the special case $\mathfrak{X} = \mathfrak{N}$ the class of all nilpotent groups. 8.91 shows that $\mathfrak{X} = \mathfrak{S}$ the class of all semisimple groups is another admissible choice. A third choice would be $\mathfrak{X} = \mathfrak{O}_\varpi$ the class of all ϖ-groups. This is admissible by 5.5 or 3.4, which shows that products of normal ϖ-subgroups are ϖ-groups.

The subgroup $\mathfrak{X}G$ is characteristic in G and may be called the $\mathfrak{X}$-radical of G. Here "radical" is equivalent to "uniquely determinal maximal normal subgroup" of the appropriate class.

(I). A semisimple group will be called isotypic if its simple direct factors are all isomorphic.

Lemma 8.93 A characteristically-simple group G is either (i) an elementary Abelian p-group for some prime p or else (ii) an isotypic semisimple group.

Proof: let G_1 be a minimal normal subgroup of G and let H be the direct product of $G_1, G_2, \cdots, G_n$ where each $G_i = G_1^{\alpha_i}$ for some $\alpha_i \in A = \mathrm{Aut}\, G$. Choose H as large as possible and let $\beta \in A$. If $H^\beta \neq H$, then $G_i^\beta \not\leq H$ for some i. But $H \lhd G$ and G_i^β is a minimal normal subgroup of G. Hence $H \cap G_i^\beta = 1$ and the product HG_i^β is direct by 6.9, contrary to the definition of H. It follows that $H^\beta = H$ for all $\beta \in A$ and so H char G. Since G is characteristically

simple and $H \geq G_1 \neq 1$, it follows that $H = G$. Each $G_i \cong G_1$ and every normal subgroup of G_1 is normal in G. Hence G_1 is simple. If $|G_1| = p$ is prime, then G is elementary. Otherwise G is isotypic and semisimple.

(J) Let V be an elementary p-group which admits G as a group of operators. We use the additive notation for V. V is called G-irreducible if $V \neq 0$ and if V and 0 are the only G-invariant subgroups of V. In any case if $V \neq 0$, a minimal G-invariant subgroup $X \neq 0$ in V is necessarily G-irreducible.

Theorem 8.9. Let V be G-irreducible and let $H \lhd G$. Then $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ is the direct sum of a certain number $r \geq 1$ of H-invariant subgroups V_i with the following properties:

(i) Each V_i is the direct sum of a certain number $e \geq 1$ of H-irreducible subgroups $X_{i1}, X_{i2}, \cdots, X_{ie}$, where e is independent of i

(ii) X_{is} and X_{jt} are H-isomorphic if and only if $i = j$.

(iii) If Y is any H-invariant subgroup of V, then $Y = Y_1 \oplus \cdots \oplus Y_r$ where $Y_i = Y \cap V_i$. In particular, if Y is H-irreducible, then Y is H-isomorphic with X_{i1} for some i and in that case $Y \leq V_i$.

(iv) If $\xi \in G$, then the mapping $V_i \to V_i\xi$ $(i = 1, 2, \cdots, r)$ is a permutation of $V_1, \cdots, V_r$ and G is represented transitively by these permutations.

Proof: Let $W = W_1 \oplus \cdots \oplus W_n$ be a direct sum of H-irreducible subgroups W_i of V, and choose W as large as possible. Let $\xi \in G$. Every subgroup of $W_i\xi$ has the form $Z\xi$ where Z is a subgroups of W_i. If $\eta \in H$, $u \in Z$ then $u\xi\eta = u(\xi\eta\xi^{-1})\xi$ and, since $H \lhd G$, $Z\xi$ is H-invariant only if Z is H-invariant. Hence $W_i\xi$ is H-irreducible If $W\xi \neq W$, then $W_i\xi \not\leq W$ for some i and hence $W \cap W_i\xi = 0$ and the sum $W + W_i\xi$ is direct, contrary to the choice of W. It follows that $W\xi = W$ for all $\xi \in G$. Since V is G-irreducible, we must

therefore have $W = V$.

We now relabel the subgroups W_j as X_{is} so that (ii) is satisfied and define V_i as the direct sum of the X_{is} $(s = 1, 2, \cdots)$, so that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ if there are r classes of H-isomorphic H-irreducible subgroups among the W_j. To prove (iii), suppose $W_j \not\leq Y$. Then $Y \cap W_j = 0$ since W_j is H-irreducible and Y is H-invariant; and so the sum $Y + W_j$ is direct. It follows that $V = Y \oplus W_{j_1} \oplus \cdots \oplus W_{j_t}$ for some $t \geq 0$ and suitable $j_1, \cdots, j_t$. Hence Y is H-isomorphic with $V / \sum_{\alpha=1}^{t} W_{j_\alpha}$ and so with $W_{i_1} \oplus \cdots \oplus W_{i_s}$, where $i_1, \cdots, i_s$ (the complementary set of suffixes to $j_1, \cdots, j_t$. Thus Y is a direct sum of H-irreducible subgroups and we need therefore only consider the case in which Y itself is H-irreducible. Let $\overline{W}_j = W_1 \oplus \cdots \oplus W_j$ and let j be the first integer $\leq n$ such that $Y \leq \overline{W}_j$. Then $\overline{W}_{j-1} \cap Y = 0$ by the irreducibility of Y and $\overline{W}_j = \overline{W}_{j-1} \oplus Y$ by the irreducibility of W_j. So Y is H-isomorphic with $W_j = X_{is}$ say. By the same argument applied with the W_j's rearranged so that all those H-isomorphic with Y come first (viz. $X_{i1}, X_{i2}, \cdots$), we obtain $Y \leq V_i$, as required.

If $\xi \in G$, then as we have seen $X_{i1}\xi$ is H-irreducible. If $X_{i1}\xi$ is H-isomorphic with X_{j1}, then $X_{i1}\xi \leq V_j$ by (iii). If $u \to u'$ is an H-isomorphism of X_{i1} onto X_{is}, $u \in X_{i1}$, then $u\xi \to u'\xi$ is an H-isomorphism of $X_{i1}\xi$ onto $X_{is}\xi$, since $u\xi\eta = u(\xi\eta\xi^{-1})\xi \to u'(\xi\eta\xi^{-1})\xi = u'\xi\eta$ for $\eta \in H$, owing to $\xi\eta\xi^{-1} \in H$. Hence $X_{is}\xi \leq V_j$ for each $s = 1, 2, \cdots$ and so $V_i\xi \leq V_j$. Here $j = j(i, \xi)$ depends only on i and on the automorphism $t_H(\xi)$ induced in H by transforming with ξ. It now follows that $V_i\xi = V_{j(i,\xi)}$ and the mapping $V_i \to V_i\xi$ $(i = 1, \cdots, r)$ is a permutation of $V_1, \cdots, V_r$. The representation of G by these permutations must be transitive, since otherwise V would not be G-irreducible. Hence each V_i is the direct sum of the same number ρ of H-irreducible subspaces and 8.9 is completely proved.

We call $V_1, \cdots, V_r$ the <u>Wedderburn components</u> of V with respect to H.

§9. Frattini subgroups. Split extensions. π-soluble groups. S_π-subgroups

(A). We consider next how to construct larger groups from smaller ones. Let $K \lhd G$ and suppose that $1 < K < G$. If there exists in G a proper subgroup H such that $KH = G$, we say that K is partially complemented in G. If in addition $K \cap H = 1$, so that H is transversal to K in G, we say that K is complemented in G.

The intersection of the maximal subgroups of G is called the Frattini subgroup of G and denoted by $\varphi(G)$. Clearly $\varphi(G)$ char G.

Theorem 9.1 Let $F = \mathfrak{N}G$ and $\Phi = \varphi(G)$ be respectively the Fitting and the Frattini subgroups of G. Then

(i) $G = \{\xi_1, \cdots, \xi_n\}$ if and only if $G = \{\Phi, \xi_1, \cdots, \xi_n\}$.

(ii) Let $K \lhd G$. Then K is partially complemented in G if and only if $K \not\leq \Phi$.

(iii) $F' \leq \Phi \leq F$, so that Φ is nilpotent and F/Φ is Abelian. Moreover, $F/\Phi = \mathfrak{N}(G/\Phi)$ the Fitting subgroup of G/Φ.

Proof: (i) Let $H = \{\xi_1, \cdots, \xi_n\} < G$. Then there exists a maximal subgroup M of G such that $H \leq M$. Since $\Phi \leq M$, it follows that $\{\Phi, \xi_1, \cdots, \xi_n\} \leq M < G$.

(ii) Let H be a proper subgroup of G such that $KH = G$. If $K \leq \Phi$, we should have $\Phi H = G$ and so $H = G$ by (i), contrary to $H < G$. Hence $K \not\leq \Phi$. Conversely, suppose $K \not\leq \Phi$. Then there is a maximal subgroup M of G which does not contain K. Since $K \lhd G$, it follows that KM is a group with M as a proper subgroup, hence $KM = G$ and K is partially complemented in G.

(iii) Let $K = \mathfrak{N}(G \bmod \Phi)$ so that K/Φ is the Fitting subgroup of G/Φ. Let S be a Sylow p-subgroup of K. Since K/Φ is nilpotent, $\Phi S/\Phi$ is a characteristic subgroup of K/Φ. Also $K \lhd G$, $\Phi \lhd G$. Hence $\Phi S \lhd G$. As a Sylow subgroup of a normal subgroup of G, S is pronormal in G and so, if $N = N_G(S)$, we have $\Phi N = \Phi S N = G$ by 6.64.

Hence $N = G$ by (i) and so $S \lhd G$. It follows that K is nilpotent, $K \leq F = \mathfrak{N}G$. A fortiori Φ is nilpotent. Since F/Φ is nilpotent and normal in G/Φ, we have $F \leq \mathfrak{N}(G \bmod \Phi) = K$. Combining gives $F = K$.

We show that F/Φ is Abelian by proving a more precise result.

Theorem 9.2 Let M be a maximal subgroup of G, let $L = K_G(M) = \bigcap_{x \in G} M^x$ and let $N = \mathfrak{N}(G \bmod L)$. Then either $N = L$ or else N/L is a chief factor of G. In the latter case, N/L is an elementary Abelian p-group for some p and is the only minimal normal subgroup of G/L. Further, $N = C_G(N/L)$ and $M \cap N = L$, so that M/L is represented faithfully by automorphisms of N/L. Also $MN = G$ so that $|G:M| = |N:L| = p^n$ for some n.

Corollary. In a soluble group, every maximal subgroup is of index a power of a prime.

Proof: Suppose that $N > L$ and let P/L be any chief factor of G such that $P \leq N$. P/L cannot be semisimple since N/L is nilpotent. Hence P/L is an elementary p-group for some p, by 8.93. Let $Q = M \cap P$ so that $L \leq Q \lhd M$. Since L is the greatest normal subgroup of G contained in M, and $L < P \lhd G$, we have $P \not\leq M$ and so $PM = G$ by the maximality of M. Since P/L is Abelian, $Q \lhd P$ and so $Q \lhd PM = G$. But $L \leq Q < P$ and P/L is a chief factor of G. Hence $Q = L$.

Since N/L is nilpotent and $P \lhd G$, we have $L_1 = L[P,N] < P$ and $L_1 \lhd G$, hence $L_1 = L$. So $N \leq C = C_G(P/L)$. Let $D = C \cap M$. Then $[D,P] \leq L \leq D$ and so $D \lhd PM = G$. Hence $D = L$ and so $N = P = C$. Thus we obtain $N = C_G(N/L)$, $M \cap N = L$, $MN = G$. If R/L is any minimal normal subgroup of G/L distinct from N/L, we should have $[R,N] \leq R \cap N = L$ and so $R \leq C_G(N/L) = N$, a contradiction. Thus the Fitting subgroup N/L of G/L is the only minimal normal subgroup of G/L and all is proved.

If $F = \mathfrak{N}G$, then $LF/L \cong F/L \cap F$ which is nilpotent and so $F \leq N$ and $F' \leq N' \leq L \leq M$. This is true for every maximal subgroup M

of G. Hence $F' \leq \mathfrak{L} = \varphi(G)$ and the proof of 9·1 is now also complete. Indeed we see that the Sylow subgroups of $F/\mathfrak{L}$ are all elementary Abelian. 9·1 and 9·2 are due to E. Galois 1811-32, G. Frattini 1852-1925 and W. Gaschütz.

Def. Let us say 9·3 Let H/K be a chief factor of G and suppose that $|H:K| = p^n$. Then (i) $\mathfrak{N}(G \bmod K) \leq C = C_G(H/K)$ and (ii) its automizer $A = A_G(H/K) \cong G/C$ of H/K in G has no normal p-subgroup $\neq 1$.

Proof: (i) The proof that $N = \mathfrak{N}(G \bmod K) \leq C$ has already occurred in the course of proving 9·2.

(ii) Let B be any p-subgroup of A. Since B leaves invariant the unit element of H/K and $|H:K| = p^n$, B must also leave invariant further elements of H/K, by 5·1. In the isomorphism of A with G/C, let B correspond to D/C. If $B \lhd A$, then $D \lhd G$ and the set of all elements $\xi \in H$ such that $K\xi$ is invariant under B, or equivalently $[\xi, D] \leq K$, is also a normal subgroup H_1 of G. Since $K < H_1 \leq H$, it follows that $H_1 = H$ and so $[H, D] \leq K$, $D \leq C$, $B = 1$.

(B). Let f be any representation of a group H by automorphisms of another group K, so that $f(\eta) \in \mathrm{Aut}\, K$ for $\eta \in H$ and $f(\eta_1\eta_2) = f(\eta_1)f(\eta_2)$. It is convenient to write the ordered pairs (η, ξ) with $\eta \in H$, $\xi \in K$ as *formal products* $\eta\xi$, the force of 'formal' being that $\eta_1\xi_1 = \eta_2\xi_2$ if and only if $\eta_1 = \eta_2$ and $\xi_1 = \xi_2$. If we define in the set G of all such formal products a multiplication $(\eta_1\xi_1)(\eta_2\xi_2) = \eta_3\xi_3$ by the rule that

$$\eta_3 = \eta_1\eta_2 \quad \text{and} \quad \xi_3 = \xi_1^{f(\eta_2)}\xi_2, \tag{1}$$

then G becomes a group. If we identify the formal product $\eta 1$ with the element η of H and similarly 1ξ with the element ξ of K, then H and K become subgroups of G such that

$$HK = G, \quad H \cap K = 1 \quad \text{and} \quad K \lhd G. \tag{2}$$

Moreover in G, the automorphism $t_K(\eta)$ of K induced by transforming K by the element η of H is precisely $f(\eta)$.

G is called the *split* (or complemented) *extension* of K by H

determined by the representation f, and we shall denote it by

$$G = \langle H, K; f \rangle. \tag{3}$$

Given $\alpha \in \mathrm{Aut}\, K$ and $\beta \in \mathrm{Aut}\, H$, we obtain from f a new representation f^* of H by automorphisms of K, defined by

$$\xi^{f^*(\eta)} = \xi^{\alpha^{-1} f(\eta^\beta)\alpha} \qquad (\eta \in H,\ \xi \in K). \tag{4}$$

And we have

$$G^* = \langle H, K; f^* \rangle \cong \langle H, K; f \rangle, \tag{5}$$

the mapping $\eta\xi \to \eta^\beta \xi^{\alpha^{-1}}$ of G^* onto G being an isomorphism.

However, it is sometimes possible for there to be an isomorphism of the form (5) even when f and f^* are not related as in (4). The reason for this is twofold. First, it may happen that G has a normal subgroup $K_1 \neq K$ such that $K_1 \cong K$ and $G/K_1 \cong G/K$, and such that K_1 is complemented in G by a subgroup H_1. Then $H_1 \cong H$. If $\xi \to \xi_1$ and $\eta \to \eta_1$ are isomorphisms of K onto K_1 and H onto H_1, and if we define f^* by the equation $\xi_1^{\eta_1} = (\xi^{f^*(\eta)})_1$, then f^* is a representation of H by automorphisms of K and $\langle H, K; f^* \rangle \cong \langle H, K; f \rangle$. However, this possibility can be excluded if K is an S_π-subgroup of G i.e. if $|H|$ and $|K|$ are coprime, for then $K_1 = K$ by 5.8.

If there is no such subgroup $K_1 \neq K$, we have only to consider the subgroups H_1 which are complementary to K in G. Every such H_1 contains exactly one element $\eta\, k(\eta)$ in the coset $\eta K = K\eta$ of K in G. Here η is any element of H and $k(\eta) \in K$. Since H_1 is a subgroup, we have $\eta_1 \eta_2\, k(\eta_1 \eta_2) = \eta_1\, k(\eta_1)\, \eta_2\, k(\eta_2)$ and so

$$k(\eta_1 \eta_2) = (k(\eta_1))^{\eta_2} k(\eta_2) \qquad (\eta_1, \eta_2 \in H). \tag{6}$$

Any mapping k of H into K satisfying (6) is called a <u>cocycle</u> with respect to f. The subgroups H_1 complementary to K in G are therefore in one-to-one correspondence with the cocycles. Among these subgroups those occur the conjugates of H in G. Every such conjugate has the form H^κ with $\kappa \in K$ and for this case the cocycle is defined by

$$k(\eta) = [\eta, \kappa]; \tag{7}$$

and the representation f^* of H which we obtain by replacing each $\eta \in H$ by $\eta^k \in H$, is one of those given by (4), viz. with $\alpha = t_K(k)$ and $\beta = 1$.

We define

$$c_1 = c_1(H, K; f) \qquad (8)$$

to be the number of classes of conjugates in G into which the subgroups H_1 complementary to K split up. If G has no subgroup $K_1 \neq K$ of the kind considered above and if in addition $c_1 = 1$, then we can affirm that $G = \langle H, K; f\rangle \cong \langle H, K; f^*\rangle$ if and only if f^* is related to f by (4), for some choice of α and β. If this <u>simple case</u> occurs for all choices of the representation f, then it is an easy matter to determine in principle how many non-isomorphic split extensions of K by H exist; although in practise this involves a good understanding of the structure of H and $\mathrm{Aut}\, K$.

(C). We now prove an important result due to H. Zassenhaus, then attributed by him to Schur. This is

<u>Theorem 9.4</u> Let K be a normal S_ϖ-subgroup of G. (i) Then G contains an $S_{\varpi'}$-subgroup H, so that $K \cap H = 1$, $HK = G$, $H \cong G/K$. If either H or K is soluble, then every $S_{\varpi'}$-subgroup of G is conjugate to H in G.

Proof: (i) Suppose that G is a group of least order for which the result is not true, and let S be a Sylow p-subgroup of K and $N = N_G(S)$. Then $KN = G$ since $K \lhd G$, and $K \cap N$ is a normal S_ϖ-subgroup of N. If $N < G$, there is a subgroup H complementary to $K \cap N$ in N, by choice of G. Since $KN = G$, H is an $S_{\varpi'}$-subgroup of G, contrary to hypothesis. Hence $N = G$. This is true for all p, so that K is nilpotent. Let $Z = \zeta K$. Then Z char K and so $Z \lhd G$. K/Z is a normal S_ϖ-subgroup of G/Z and, since $Z \neq 1$, there is a subgroup $G_1 \geq Z$ such that $G = G_1 K$, $Z = G_1 \cap K$. Then Z is a normal S_ϖ-subgroup of G_1 and, if $G_1 < G$, there is a complement H to Z in G_1. Since $G = G_1 K$, H is an $S_{\varpi'}$-subgroup of G contrary to hypothesis.

Hence $G_1 = G$ and $K = Z$ is Abelian.

Now T be any transversal to K in G. We label the elements $t_\alpha \in$ by the coset $\alpha \in G/K$ to which they belong. Then $t_\alpha t_\beta \in \alpha\beta$ and $t_\alpha t_\beta = t_{\alpha\beta}\, k(\alpha,\beta)$ where $k(\alpha,\beta) \in K$ for all $\alpha, \beta \in G/K$. If $\gamma \in G/K$ also, we have $(t_\alpha t_\beta) t_\gamma = t_\alpha (t_\beta t_\gamma)$. But K is Abelian and so the automorphism $\xi \to t_\alpha^{-1} \xi\, t_\alpha$ $(\xi \in K)$ depends only on α. Writing ξ^α for $t_\alpha^{-1} \xi\, t_\alpha$, we find that the function $k(\alpha,\beta)$ satisfies

$$k(\alpha\beta,\gamma)\, k(\alpha,\beta)^\gamma = k(\alpha,\beta\gamma)\, k(\beta,\gamma) \qquad (9)$$

for all α, β, γ in G/K. Defining $k_1(\beta) = \prod_{\alpha \in G/K} k(\alpha,\beta)$ and forming the products of the two sides of (9) as α runs through G/K, with β and γ kept fixed, we obtain

$$k_1(\gamma)\, k_1(\beta)^\gamma = k_1(\beta\gamma)\, k(\beta,\gamma)^n \qquad (10)$$

where $n = |G:K|$. If $m = |K|$, then $(m,n) = 1$ by hypothesis. Hence there is an integer l such that $ln \equiv 1 \bmod m$. We then have $k(\beta,\gamma) = k(\beta,\gamma)^{nl} = k_2(\beta\gamma)\, k_2(\gamma)^{-1} (k_2(\beta)^\gamma)^{-1}$ where $k_2(\beta) = k_1(\beta)^{-l}$. Hence if $s_\beta = t_\beta\, k_2(\beta)$ for $\beta \in G/K$, we obtain $s_\beta s_\gamma = t_{\beta\gamma}\, k(\beta,\gamma)\, k_2(\beta)^\gamma$ $= t_{\beta\gamma}\, k_2(\beta\gamma) = s_{\beta\gamma}$. Hence the set S of all s_β $(\beta \in G/K)$ is a subgroup complementary to K in G. This final contradiction proves (i).

(ii) Let H and H_1 be two subgroups complementary to K in G. We assume that H and H_1 are not conjugate in G and choose G as small as possible subject to this hypothesis. Let $L \lhd G$ and $1 < L < K$. Then either $H \cong G/K \cong (G/L)/(K/L)$ is soluble or else K/L is soluble. Hence, by our minimal choice of G, HL and $H_1 L$ are conjugate in G and we may assume $HL = H_1 L = G_1$. Since either H or L is soluble, H and H_1 are conjugate in G_1, again by choice of G. This is a contradiction. Hence K is a minimal normal subgroup of G.

Let $M = O_{\pi'} G$ be the maximal normal π'-subgroup of G. Then H and H_1 both contain M. If $M \neq 1$, it follows that H/M and H_1/M are conjugate in G/M by choice of G; and hence H and H_1 are conjugate in G, contrary to hypothesis. Hence $M = 1$.

Suppose first that H is soluble and let P/K be a minimal normal subgroup of $G/K \cong H$. Then P/K is an elementary p-group and $P = KQ$ where $Q \overset{=P\cap H}{\underset{L}{}}$ is a Sylow p-subgroup of P. $Q_1 = P \cap H$, is also a Sylow p-subgroup of P. These are conjugate in P and so we may assume that $Q = Q_1$. Then H and are $S_{\infty'}$-subgroups of $N = N_G(Q)$. If $N < G$, H and H_1 are conjugate in N, since N has the normal S_{∞}-subgroup $N \cap K$. Hence $N = G$ and so P is the direct product of K and Q. But then Q char P and so $Q \lhd G$. This contradicts $M = 1$ and we conclude that H must be insoluble.

It now follows from the hypothesis that K is soluble. As a minimal normal subgroup of G, K is therefore an elementary Abelian q-group for some prime q. Let $\eta \in H$ and let $\eta k(\eta)$ be the element of H, in ηK so that k is a cocycle satisfying equation (6); or

$$k(\eta\zeta) = k(\eta)^{\zeta} k(\zeta) \qquad (\eta, \zeta \in H). \qquad (11)$$

We then have $\alpha = \prod_{\eta \in H} k(\eta) = \prod_{\eta \in H} k(\eta\zeta) = \alpha^{\zeta} k(\zeta)^n$, where $n = |H|$. As in (i) we choose l so that $ln \equiv 1 \bmod m = |K|$ and obtain α^l. $\beta = \beta^{\zeta} k(\zeta)$ for all $\zeta \in H$, whence $\zeta^{\beta} = \zeta k(\zeta)$ and so $H_1 = H^{\beta}$. Hence $\beta \in K$. This final contradiction proves (ii').

(D) We now consider some corollaries of 9.4.

Corollary 9.41. Let Γ be a group of automorphisms of G of order prime to $|G|$. If either G or Γ is soluble, then for each prime p, Γ leaves invariant some Sylow p-subgroup of G.

We apply 9.4 (ii) to the split extension ΓG. If S is any Sylow p-subgroup of G and $N = N_{\Gamma G}(S)$, then $NG = \Gamma G$ and so by 9.4 (i), N contains a subgroup Γ_1 complementary to $N \cap G$. By 9.4 (ii), Γ_1 is conjugate to Γ in ΓG. Hence Γ also leaves invariant some Sylow p-subgroup of G.

A group G is called π-<u>seperable</u> if the composition factors of G are all either π-groups or π'-groups. G is called π-soluble if the composition factors of G are all either $\leq$ p-groups for some $p \in \pi$ or else π'-groups. Note that π-seperable $\Leftrightarrow$ π'-separable, π-soluble $\Rightarrow$ π-seperable and p-soluble $\Leftrightarrow$ p-seperable. Also, in the above definitions the composition factors could be replaced by the chief factors. G is π-seperable if & only if it has a series whose factors are all either π-groups or π'-groups. G is π-soluble if and only if it has a series whose factors are all either p-groups with some $p \in \pi$ or else π'-groups. Subgroups, quotient groups and sections of π-separable groups are π-seperable. Similarly for π-soluble.

<u>Lemma 9.51</u> Let $p \in \pi$, $q \in \pi'$ and let G be π-seperable. Then G has S_π-subgroups, $S_{\pi q}$-subgroups and S_{pq}-subgroups.

Since π-separable $\Rightarrow$ π'-seperable, it follows that G also has $S_{\pi'}$-subgroups and $S_{p\pi'}$-subgroups.

Proof by induction on $|G|$. We may assume $G \neq 1$. Let M be a minimal normal subgroup of G, and let H/M be an S_ψ-subgp of G/M with $\psi = \pi$, πq or pq. H exists by the induction hypothesis, and if $H < G$ the result follows at once for G. Hence we may assume G/M is a ψ-group.

First let M be a π-group. If $\psi = \pi$ or πq, the result follow at once. If S is a Sylow p-subgroup of M and $G_1 = N_G(S) < G$, then $MG_1 = G$ and an S_{pq}-subgroup of M is an S_{pq}-subgroup of G. Hence we may assume $G_1 = G$, $S \lhd G$, $M = S$ and again the result is immediate.

If M is not a π-group, it must be a π'-group. When $\psi = \pi$, then M is an $S_{\pi'}$-subgroup of G and the result follows from 9.4. When $\psi = \pi$ let T be a Sylow q-subgroup of M and $G_2 = N_G(T)$. If $G_2 < G$, an $S_{\pi q}$-subgroup of G_2 exists by induction and is an $S_{\pi q}$-subgroup of G since $MG_2 = G$. If $G_2 = G$, then $T \lhd G$, $T = M$ and the result is

immediate. The case $\psi = pq$ is symmetrical as between π and π' and has already been dealt with.

Lemma 9.52 Let G be either π-soluble or π'-soluble, let H be any S_π-subgroup of G and let L be any π-subgroup of G. Then $L^g \leq H$ for some $g \in G$. In particular, any two S_π-subgroups of G are conjugate in G.

Proof by induction on $|G|$. We can assume $G \neq 1$. Let M be a minimal normal subgroup of G. Then MH/M is an S_π-subgroup of G/M and ML/M is a π-subgroup. By induction, $L^y \leq MH$ for some $y \in G$. The theorem follows by a second induction if $MH < G$, since H is an S_π-subgroup of MH. So we may assume $MH = G$. Then G/M is a π-group. If M is a π-group, then $H = G$ and there is nothing left to prove. If M is not a π-group, it is a normal $S_{\pi'}$-subgroup of G, since G is π-seperable. Further, $H \cap M = 1$, $H \cong G/M$ and by hypothesis at least one of the groups M and H is soluble. Also $L \cap M = 1$ and if $G_1 = LM$, $L_1 = H \cap G_1$, then L and L_1 are S_π-subgroups of G_1. Either L or M is soluble. Hence $L_1 = L^x$ for some $x \in M$ by 9.4 (ii) and the lemma follows.

For soluble groups, we may now state a result analogous to Sylow Theorem but with the prime p replaced by an arbitrary set of primes π. This is

Theorem 9.5 Let G be soluble and let π be any set of primes. Then (i) G contains S_π-subgroups.

(ii) Any two S_π-subgroups of G are conjugate in G

(iii) Every π-subgroup of G is contained in some S_π-subgroup of G

By 9.52, if G is either π-soluble or π'-soluble, the S_π-subgroups of G may be described alternatively as the maximal π-subgroups of G. It also follows that <u>any S_π-subgroup H of G is pronormal in G and $N = N_G(H)$ is abnormal in G</u>.

(E) Lemma 9.6 Let H and K be subgroups of G, and $L = H \cap K$. Then (i) $|K:L| \leq |G:H|$ and so $|G:L| \leq |G:H| \cdot |G:K|$

(ii) If H and K are conjugate in G, and distinct, then $|K:L| < |G:H|$ and $HK < G$

(iii) If $|G:H| = m$ and $|G:K| = n$ are coprime, then $|G:L| = mn$ and $HK = G$.

Proof: (i) $|K:L| = |HK:H|$ by 5.5.

(ii) If $\eta \in H$, $\zeta \in K$, then $H^{\eta\zeta} = H^{\zeta} \neq K^{\zeta} = K$. Hence if H and K are conjugate in G, and distinct, then $HK < G$ and so $|K:L| < |G:H|$

(iii) Since $L \leq H \leq G$, $|G:L|$ is a multiple of m. Similarly it is a multiple of n. Since $(m,n) = 1$, $|G:L|$ is a multiple of mn. But $|G:L| \leq mn$ by (ii). Hence $|G:L| = mn$ and so $|K:L| = m$ and $HK = G$.

Theorem 9.7 Suppose that G has three soluble subgroups H_1, H_2, H_3 whose indices m_1, m_2, m_3 in G are coprime in pairs. Then G is soluble.

Proof: If $H_1 = 1$, then $H_2 = H_3 = G$ and there is nothing to prove. So we can assume $H_1 \neq 1$. Let M be a minimal normal subgroup of H_1. Then $|M| = p^m$ for some prime p. Since $(m_2, m_3) = 1$, we may assume that p does not divide m_2. By 9.6 (iii), if $L_{12} = H_1 \cap H_2$, then $|H_1 : L_{12}| = m_2$. Hence L_{12} contains a Sylow p-subgroup of H_1 and so $M \leq L_{12}$. Also $G = H_1 H_2$ and so every element of G has the form $\xi\eta$ with $\xi \in H_1$, $\eta \in H_2$. This shows that every conjugate $M^{\xi\eta} = M^{\eta}$ of M in G is contained in H_2. Hence $K = \{M^{\eta}; \eta \in H_2\}$ is normal in G and soluble. In G/K, the subgroups $KH_i/K \cong H_i/K \cap H_i$ are soluble and their indices m_i' are coprime in pairs since $m_i' = |G:KH_i|$ divides $m_i = |G:H_i|$. By induction on $|G|$, we may assume that G/K is soluble. Hence G is soluble.

(F). The proof of the following theorem of Burnside depends on the theory of group characters and will be postponed to § .

Theorem 9.8 If the group G has a class of $p^n > 1$ conjugate elements, then G is not simple.

Corollary. If $|G|$ is divisible by only two primes p and q, then G is soluble.

Proof by induction on $|G|$. We may assume that $G \neq 1$ and that $\mathfrak{z}G = 1$. Then G is not a p-group. Let Q be a Sylow q-subgroup of G. Then $Q \neq 1$ and so $\mathfrak{z}Q \neq 1$. Let $\xi \in \mathfrak{z}Q$, $\xi \neq 1$. Since $\mathfrak{z}G = 1$, we have $|G : C_G(\xi)| = p^n > 1$. Hence G is not simple by 9.4. So there is a subgroup $K \lhd G$ with $1 < K < G$. By induction both K and G/K are soluble. Hence G is soluble.

Theorem 9.9 A group G is soluble if and only if it has an $S_{p'}$-subgroup for every prime p.

Proof: The condition is necessary by 9.5. Let $|G| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where $p_1 < p_2 < \cdots < p_k$ are primes. If $k \leq 2$, then G is soluble by 9.8. Suppose that G has an $S_{p_i'}$-subgroup H_i for each $i = 1, 2, \cdots, k$. If $k =$ each H_i is soluble by 9.8 and so G is soluble by 9.7. Let $k > 3$. By 9.6(iii), if $i \neq j$, $H_i \cap H_j$ is an $S_{p_j'}$-subgroup of H_i. So we may assume each H_i is soluble by induction on k. It now follows that G is soluble by 9.7 again.

§10. Systemizers and Carter Subgroups of Soluble Groups

(A) Let G be a soluble group and let $p_1, \cdots, p_k$ be the distinct primes which divide $|G|$. By 9·5, G has for each $i = 1, 2, \cdots, k$ at least one $S_{p_i'}$ subgroup H_i. By 9.6 (iii), the 2^k intersections of sets of subgroups chosen from $H_1, \cdots, H_k$, including the empty intersection G, are S_ϖ-subgps of G for various ϖ. In particular $P_i = \bigcap_{j \neq i} H_j$ is a Sylow p_i-subgp of G. Since for $i \neq l$

$$|P_i P_l| = |\bigcap_{j \neq i,l} H_j| = |P_l P_i|,$$

we must have $P_i P_l = \bigcap_{j \neq i,l} H_j = P_l P_i$, so that the Sylow subgroups $P_1, P_2, \cdots, P_k$ of G are permutable in pairs. And if Λ is any subset of $1, 2, \cdots, k$ and Λ' is the complementary set, we have more generally

$$\prod_{i \in \Lambda} P_i = \bigcap_{j \in \Lambda'} H_j .$$

Thus the 2^k intersections of sets of H_j coincide with the 2^k products of sets of P_i, including the empty product 1. This set of 2^k subgroups is called an S-system of G. Given any S-system $\underset{\sim}{T}$ of G, and any set of primes ϖ, just one member of $\underset{\sim}{T}$ is an S_ϖ-subgroup of G and this will be denoted by T_ϖ. If ϖ and ψ have the same intersection with the set $p_1, \cdots, p_k$, then $T_\varpi = T_\psi$. $\underset{\sim}{T}$ is determined uniquely by the T_p and equally well by the $T_{p'}$. For any two sets of primes ϖ and ψ, we have

$$T_\varpi T_\psi = T_\psi T_\varpi = T_{\varpi \cup \psi}$$

and

$$T_\varpi \cap T_\psi = T_{\varpi \cap \psi} .$$

In particular, $T_\varpi T_{\varpi'} = G$ and $T_\varpi \cap T_{\varpi'} = 1$.

Lemma 10·1 Let $\underset{\sim}{S}$ and $\underset{\sim}{T}$ be any two S-systems of the soluble group G. Then there is an element $\xi \in G$ such that $S_\varpi^\xi = T_\varpi$ for all ϖ.

Proof. Suppose that $S_{p_i'} = T_{p_i'}$ for $i = 1, 2, \cdots, r-1$ ($0 \leq r \leq k$) while $S_{p_r'} \neq T_{p_r'}$. Since $S_{p_r'}$ and $T_{p_r'}$ are conjugate in G by 9·5 and $S_{p_r'} S_{p_r} = G$, there is an element $\eta \in S_{p_r}$ such that $S_{p_r'}^\eta = T_{p_r'}$. But

$S_{p_r} \leq S_{p_i'}$ for $i = 1, 2, \ldots, r-1$. Hence the S-system $\underset{\sim}{S}^\eta$ of G coincides with $\underset{\sim}{T}$ in its first r Sylow complements $T_{p_1'}, \ldots, T_{p_r'}$. By induction on r, $\underset{\sim}{S}^\xi = \underset{\sim}{T}$ for some $\xi \in G$.

(B). The normalizers in G of the S-systems $\underset{\sim}{T}$ of G will be called the systemizers of G. By definition,

$$N_G(\underset{\sim}{T}) = \bigcap_\varpi N_G(T_\varpi) = \bigcap_p N_G(T_p) = \bigcap_p N_G(T_{p'}).$$

If H is any subgroup of G and $\underset{\sim}{V}$ is an S-system of H, then

$$N_G(\underset{\sim}{V}) = \bigcap_\varpi N_G(V_\varpi) = \bigcap_p N_G(V_p) = \bigcap_p N_G(V_{p'})$$

will be called a relative systemizer of H in G. Since $H = \prod_p V_p$, it is clear that $N_G(\underset{\sim}{V}) = N_L(\underset{\sim}{V})$, where $L = N_G(H)$. $H \cap N_G(\underset{\sim}{V}) = N_H(\underset{\sim}{V})$ is a syste

Lemma 10.2 Let G be a soluble group and let $H \lhd G$.

(i) The relative systemizers L of H in G are all conjugate in G and $LH = G$. In particular any two systemizers of G are conjugate in G.

(ii) The systemizers of G are nilpotent.

Proof: (i) Let $L = N_G(\underset{\sim}{V})$ and $M = N_G(\underset{\sim}{W})$ where $\underset{\sim}{V}$ and $\underset{\sim}{W}$ are S-syste of H. By 10.1, $\underset{\sim}{W} = \underset{\sim}{V}^\xi$ for some $\xi \in H$. Hence $M = L^\xi$. If $\eta \in G$ then $\underset{\sim}{V}^\eta$ is an S-system of H since $H \lhd G$. Hence $\underset{\sim}{V}^{\eta\zeta} = \underset{\sim}{V}$ for some $\zeta \in$ by 10.1 and so $\eta\zeta \in L$, $\eta \in LH$. This is true for all $\eta \in G$ so $G = L$

(ii) Take $H = L$ and let P be a Sylow p-subgroup of L. Then P normalizes V_p which is now a Sylow p-subgroup of G. Hence $P \leq V_p$, $P = L \cap V_p$ and so $P \lhd L$ since L normalizes V_p. Thus L is nilpotent.

(C) Now let M be a minimal normal subgroup of the soluble group G so that $|M| = q^m$ for some prime q; and let $\underset{\sim}{T}$ be an S-system of G and $H = N_G(\underset{\sim}{T})$ the corresponding systemizer. The groups MT_ϖ/M are permutable in pairs and by 5.7, MT_ϖ/M is an S_ϖ-subgroup of G/M. Since $MT_\varpi = \prod_{p \in \varpi} MT_p$, the groups $T_\varpi^* = MT_\varpi/M$ form an S-system $\underset{\sim}{T}^*$ of G/M. Let $H^*/M = N_{G/M}(\underset{\sim}{T}^*)$. Thus $H^* = \bigcap_p N_G(MT_{p'})$, and so $HM \leq H^*$. Conversely let $\xi \in H^*$. If $p \neq q$, then $MT_{p'} = T_{p'}$. Also $T_{q'}^{\ \xi}$ is an $S_{q'}$-subgroup of $MT_{q'}$ and hence it is conjugate to $T_{q'}$ in $MT_{q'} = T_{q'}M$. Thus $T_{q'}^\xi = T_{q'}^\eta$ for some $\eta \in M$. Hence $\eta \in$

for all $p \neq q$ and so $\xi\eta^{-1} \in H$, $\xi \in HM$. Thus $H = H^*$.

By repeated application of this argument we obtain

Lemma 10.3 Let G be a soluble group, $K \lhd G$ and let $\underset{\sim}{T}$ be an S-system of G, $T_\omega^* = KT_\omega/K$. The the set $\underset{\sim}{T}^*$ of groups T_ω^* is an S-system of G/K; and if $L = N_G(\underset{\sim}{T})$, $L^* = N_{G/K}(T^*)$, then $L^* = KL/K$

In other words, in any epimorphism of a soluble group G onto another group G^*, the S-systems of G map into the S-systems of G^* and the systemizers of G map into the systemizers of G^*.

Now let M be once more a minimal normal subgroup of G with $|M| = q^m$, q prime; and let $C = C_G(M)$. If $C = G$, so that $M \leq \mathfrak{z} G$ it is clear that every systemizer of G contains M. If $C < G$, let D/C be a chief factor of G. Then by 9.3 (ii), D/C is a q'-group. If $\underset{\sim}{T}$ is any S-system of G and $L = D \cap T_{q'}$, it follows that $LC = D$ by 5.7. Let $H = N_G(\underset{\sim}{T})$ and $N = H \cap M$. Then N normalizes L and we have $[L, N] \leq L \cap M = 1$. Hence L centralizes N. But C also centralizes N. Hence $N \leq \mathfrak{z} D \lhd G$. If $N \neq 1$, it would follow that $M \leq \mathfrak{z} D$ since M is a minimal normal subgroup of G, contrary to the definition of $C = C_G(M)$. Hence $N = 1$.

Using 10.3, this gives

Theorem 10.4 Let H/K be any chief factor of the soluble group G and let L be any systemizer of G. Then $H \leq LK$ or $H \cap L \leq K$ according as H/K is a central factor of G or not.

We may express this result by saying that <u>the systemizers of G cover every central chief factor of G and avoid every non-central chief factor of G</u>. Now the index $|G : L|$ of a systemizer of G in G is equal to the number of distinct S-systems of G. Hence we have

Corollary 10.4.1 Let $G = G_0 > G_1 > \cdots > G_n = 1$ be a chief series of the soluble group G. Then the number of distinct S-systems of G is equal to $\prod |G_{i-1} : G_i|$ taken over all the non-central factors G_{i-1}/G_i of the given chief series.

Subgroups and direct products of nilpotent groups are nilpotent. By 8.5, it follows that every group G has a uniquely determined normal subgroup

$$G^{\mathfrak{N}} = \gamma_\infty G,$$

the limit of the lower central series of G, with the property that a quotient group G/K of G is nilpotent if and only if $K \geq G^{\mathfrak{N}}$.

Corollary 10.42 If L is a systemizer of the soluble group G, then $G = LG^{\mathfrak{N}} = \{L^x ; x \in G\}$.

For every chief factor H/K of G with $K \geq G^{\mathfrak{N}}$ is a central factor of G and so $H \leq LK$ by 10.4. Hence $G = LG^{\mathfrak{N}}$. If M is a maximal normal subgroup of G, then G/M is cyclic of prime order and so $M \geq G^{\mathfrak{N}}$. It follows that $L \not\leq M$. Hence G is the normal closure of L in G.

(C) We consider next the relations between the systemizers of a soluble group G and the abnormal maximal subgroups of G. First we need

Lemma 10.43 Let $\underset{\sim}{T}$ be an S-system of the soluble group G, let $H = N_G(\underset{\sim}{T})$ and let $N = N_G(T_{p'})$. Then the Sylow p-subgroup P of H is a Sylow p-subgroup of N and $|P|$ is equal to the product of the orders of the central p-factors in any chief series of G.

Proof: Let P^* be any Sylow p-subgroup of N. For $q \neq p$, there is an $S_{q'}$-subgroup $T_{q'}^*$ of G which contains P^*, by 9.5. Let $T_{p'}^* = T_{p'}$ and let $\underset{\sim}{T}^*$ be the S-system of G determined by the $T_{p'}^*$. Then $P^* \leq H^* = N_G(\underset{\sim}{T}^*) = \bigcap_q N_G(T_{q'}^*)$ so $|N|_p = |P^*| \leq |H^*|_p = |H|_p = |P|$ and $|P| \leq |N|_p$ since $P \leq N$. Hence $|P| = |P^*|$.

The second part of 10.43 follows from 10.4.

Now let M be an abnormal maximal subgroup of the soluble group G and suppose first that $K_G(M) = \bigcap_{x \in G} M^x = 1$. By 9.2, G has a unique minimal normal subgroup $L = \mathfrak{A}G$ of order p^m, p prime, and $M \cap L = 1$, $ML = G$. Hence M contains an $S_{p'}$-subgroup $T_{p'}$ of G. If $q \neq p$ and $T_{q'}$ is any $S_{q'}$-subgroup of G, then $L \leq T_{q'}$ and so $M \cap T_{q'} = S_{q'}$ is an $S_{q'}$-subgroup of M. Taking $S_{p'} = T_{p'}$, we thus obtain an S-syste

$\underset{\sim}{S}$ of M and an S-system $\underset{\sim}{T}$ of G. Since M is not normal in G, we have $M \neq$ and so $L/1$ is a non-central chief factor of G by 9.2. Since M and G/L incident sections of G, it follows that the product of the orders of the central p-factors in a chief series is the same for M as for G. Hence $N_G(T_{p'})$ and $N_M(T_{p'})$ have Sylow p-subgroups of the same order. Therefore $N_G(T_{p'}) = N_M(T_{p'})$ and $H = N_G(\underset{\sim}{T}) \leq M$.

In the general case where $K = K_G(M) \neq 1$, we can apply this result to the group G/K. Let $\underset{\sim}{S}$ and $\underset{\sim}{T}$ be S-systems of M and G respectively, such that $S_{p'} = T_{p'}$. Here as before we assume $|G : M| = p^m$. For $q \neq p$ we have $|T_{q'} : S_{q'}| = p^m$ and so $MT_{q'} = G$, $M \cap T_{q'} = S_{q'}$. Since $N_G(T_{p'}) \leq N_G(KT_{p'}) = N_M(KT_{p'})$ by the above particular case, the result $N_G(T_{p'}) = N_M(T_{p'})$ holds in general. Hence again $H = N_G(\underset{\sim}{T}) \leq M$ and therefore $H \leq N_M(\underset{\sim}{S})$.

A subgroup H of a group G is called <u>subabnormal</u> in G if there a chain of subgroups H_i such that

$$H = H_1 \text{ abn } H_2 \text{ abn } \cdots H_{r-1} \text{ abn } H_r = G.$$

Since every subgroup containing an abnormal subgroup is abnormal, we may also say that H is subabnormal in G if and only if H can be linked to G by a chain of subgroups each of which is maximal but not normal in the next.

We can now state

<u>Theorem 10.5</u>. Let G be a soluble group and let L be a subabnorm subgroup of G. Then

(i) every systemizer of L contains a systemizer of G.

(ii) If $|G : L| = p^m$, p prime, then L contains the normalizer in G of some $S_{p'}$-subgroup of G and L is abnormal in G.

(iii) The systemizers of G are the minimal subabnormal subgroups of G

Proof: (i) $L = L_0 < L_1 < \cdots < L_r = G$ where each L_{i-1} is an abnormal maximal subgroup of L_i. As we have seen, this implies that every systemizer of L_{i-1} contains a systemizer of L_i.

(ii) In this case $|L_i : L_{i-1}| = p^{m_i}$ say and if T is any $S_{p'}$-subgroup of L, then T is an $S_{p'}$-subgroup of G and we have $N_{L_{i-1}}(T) = N_{L_i}(T)$ for each i since L_{i-1} is abnormal and maximal in L_i. Hence $N_L(T) = N_G(T)$. But $N_G(T)$ is abnormal in G, since T prn G by 9.5. Hence L is abnormal in G.

(iii) By (i), we have only to show that $H = N_G(S_m)$ is subabnormal in G, where S_m is any S-system of G. Let $G = G_0 > G_1 > \cdots > G_m = 1$ be a chief series of G and let $H_i = N_G(S_m^{(i)})$, where $S_m^{(i)} = S_m \cap G_i$, so that $S_m^{(i)}$ is an S-system of G_i by 5.7 and H_i is the corresponding relative systemizer in G_i. Clearly $H = H_0 \leq H_1 \leq \cdots \leq H_m = G$. Now $|G_{i-1} : G_i| = p^n$ for some prime $p = p(i)$ and some $n = n(i)$. Hence $S_q^{(i)} = S_q^{(i-1)}$ for $q \neq p$, and so H_{i-1} is the normalizer of $S_p^{(i)}$ in H_i. Now $H_i \cap G_i = N_{G_i}(S_m^{(i)})$ is a systemizer of G_i and so $H_i \cap S_p^{(i)} = P_i$ is the Sylow p-subgroup of the nilpotent group $H_i \cap G_i$. Hence $H_{i-1} \leq N_{H_i}(P_i)$. But $S_p^{(i-1)} = S_p^{(i)}$ since G_{i-1}/G_i is a p-group and $H_i G_i \geq G_{i-1}$. Hence every element of $N_{H_i}(P_i)$ normalizes $S_p^{(i-1)}$, and also $S_q^{(i-1)} = S_q^{(i)}$ for all $p \neq q$. It follows that $N_{H_i}(P_i) \leq H_{i-1}$. Consequently $H_{i-1} = N_{H_i}(P_i)$. [Now P_{i-1} is a Sylow subg of the normal subgroup $H_i \cap G_{i-1}$ of H_i, so that P_{i-1} prn H_i] It follows that H_{i-1} abn H_i and, since this is true for each i, H is subabnormal in G.

The argument in (iii) shows rather more viz.

Lemma 10.51 Let $K \lhd G$, let K be soluble and let T_m be any S-system of K. Then the relative systemizer $N_G(T_m)$ is subabnormal in G.

Note that although systemizers are subabnormal subgroups, not every subgroup which contains a systemizer of the soluble group G need be subabnormal in G. For example, if G is the octahedral group and if H is one of the three elementary non-normal subgroups of order 4, then H contains two of the six systemizers of G (which are of order 2) but H is not subabnormal in G since the only proper subgroup of G which contains H is one of the Sylow 2-subgroups S and $H \lhd S$. However H prn G.

H_{i-1} is the normalizer of $S_p^{(i-1)}$ in H_i. Since $G_{i-1} = G_i(S_p^{(i-1)} \cap H_i)$, it follows that $|S_p^{(i-1)} \cap H_i| = |G_{i-1} : G_i| \, |S_p^{(i)} \cap H_i|$. If P^* is a Sylow p-subgroup of $G_{i-1} \cap H_i$, then $P^* = |G_{i-1} : G_i| \, |P^* \cap G_i$ Since $P^* \cap G_i$ is in a systemizer of G_i, it follows that $|P^*| \leq |S_p^{(i-1)} \cap H_i|$. Thus, $S_p^{(i-1)} \cap H_i$ is a Sylow p-subgroup of $G_{i-1} \cap H_i$. Since $S_p^{(i-1)} = S_p^{(i)}(S_p^{(i-1)} \cap H_i)$, it follows that $H_{i-1} = N_{H_i}(S_p^{(i-1)} \cap H_i)$. Since $S_p^{(i-1)} \cap H_i$ is a Sylow p-subgroups of $G_{i-1} \cap H_i \lhd H_i$, it follows that $S_p^{(i-1)} \cap H_i$ prm H_i, so H_{i-1} abn H_i.

(D) A group G is called <u>metanilpotent</u> if it has a normal subgroup K such that both K and G/K are nilpotent. For such a K, clearly $G^{\mathfrak{N}} \leq K \leq \mathfrak{N}G$. G is metanilpotent if and only if $G/\mathfrak{N}G$ is nilpotent or equivalently if and only if $G^{\mathfrak{N}}$ is nilpotent.

<u>Theorem 10.6</u> Let G be metanilpotent and let H be a systemizer of G. Then H is a systemizer of every subgroup L of G which contains it. Also H is abnormal in G.

Proof: Let $F = \mathfrak{N}G$ be the Fitting subgroup of G. Since G is metanil G/F is nilpotent and so $HF = G$ by 10.42. The group $L \cap F$ is nilpot and so also is H by 10.2 (ii). Let R_p and S_p be the Sylow p-subgro of $L \cap F$ and H respectively. Then R_p char $L \cap F \lhd L$ and so $R_p \lhd L$. Hence $T_p = R_p S_p$ is a p-subgroup of L. Since $HF = G$, we have $H(L \cap F) = L$ and so T_p is a Sylow p-subgroup of L. Since $R_p \lhd L$ and $S_p \lhd H$, we have $T_p T_q = T_q T_p$ for any two primes p and q. Hence the groups T_p and their products form an S-system $\underset{\sim}{T}$ of L and $H \leq H^* = N_L(\underset{\sim}{T})$.

Now let C/D be any chief factor of G such that $C \leq F$. By 9.3 (i), F centralizes C/D. ~~If $H < N = N_G(H)$, then~~ Let $N = N_G(H)$. If $H < N$, there exists such a chief factor C/D with $H \cap C \leq D$ and $D(N \cap C) > D$, by 9.4. Then $[H, N \cap C] \leq H \cap C \leq D$ and since $HF = G$, it follows that $[G, N \cap C] \leq D$. Hence $D(N \cap C) \lhd G$ and consequently $C = D(N \cap C)$ and C/D is a central factor of G. But in that case $C \leq HD$ by 9.4, contrary to $H \cap C \leq D$. This contradiction shows that $H = N$ is abnormal in G. It now follows that $H = H^*$ is a systemizer of L, since H^* is nilpotent by 10.2 (ii).

Finally, let $H \leq L \cap L^{\xi}$, where $\xi \in G$. Then $\xi H \xi^{-1}$ and H are two systemizers of L and hence they are conjugate in L. Hence there is some element η of L such that $H^{\xi^{-1}\eta} = H$. Then $\xi^{-1}\eta \in N_G(H) = H$ and so $\xi \in L$. Since L is any subgroup of G containing H, it follows that H is abnormal in G.

This theorem like the next is due to R. Carter.

In any group G, a nilpotent subgroup which is dinormal in G will be called a Carter subgroup of G.

Theorem 10.7 Let G be a soluble group. Then

(i) G contains at least one Carter subgroup.

(ii) The Carter subgroups of G are all conjugate in G.

(iii) If H is a Carter subgroup of G and if L is any subgroup of G containing H, then H is a Carter subgroup of L.

(iv) The Carter subgroups of G are abnormal in G.

(v) If $K \lhd G$, and if H is a Carter subgroup of G, then KH/K is a Carter subgroup of G/K.

(vi) The Carter subgroups of G coincide with the systemizers of G if and only if the latter are dinormal in G, and this is the case in particular when G is metanilpotent.

Proof by induction on $|G|$. ~~First note if G is metanilpotent then the systemizers of G are Carter subgroups.~~ By If G is nilpotent, then the only Carter subgroup of G is G itself and the results (i) – (vi) are immedia Hence we suppose that G is not nilpotent. Let M be a minimal normal subgroup of G, $|M| = p^m$.

(i) By induction G/M has a Carter subgroup L/M. Since L/M is nilpotent, L is metanilpotent. Let H be a systemizer of L and let $\xi \in N_G(H)$. Since $M \lhd G$ and $HM = L$, we have $\xi \in N_G(L) = L$ and so $\xi \in N_L(H) = H$ by 10.6. But H is nilpotent. Hence H is a Carter subgroup of G.

(ii) Let H^* be any Carter subgroup of G and let $L^* = H^*M$. Then $L^*/M \cong H^*/M \cap H^*$ is nilpotent and so L^* is metanilpotent. If $L^* < G$, it follows from (ii) by induction that H^* is a systemizer of L^*, since H^* is a Carter subgroup of L^* and the systemizers of metanilpotent groups are also Carter subgroups. If $L^* = G$, then $H^* \cap M \lhd G$ and so is either 1 or M. But G is not nilpotent. Hence $H^* \cap M = 1$. H^* normalizes

$MS_{q'} = T_{q'}$ where $S_{q'}$ is the unique $S_{q'}$-subgroup of H^* for each prime $q \neq p$ and H^* also normalizes $S_{p'} = T_{p'}$. Since $T_{q'}$ is an $S_{q'}$-subgroup of $G = H^*M$ it follows that $H^* \leq N_G(T_m)$ where T_m is the S-system of G determined by the $T_{q'}$. But M is a non-central chief factor of G and so $N_G(T_m) \cap M = 1$ by 9.4. Since $G = H^*M$, it follows that $H^* = N_G(T_m)$ is a systemizer of $G = L$ in this case also.

Let $\xi \in N_G(L^*)$. Then $H^{*\xi}$ is also a systemizer of L^*, hence conjugate to H^* in L^* and so $H^{*\xi\eta} = H^*$ for some $\eta \in L^*$. Therefore $\xi\eta \in N_G(H^*) = H^*$ and so $\xi \in L^*$. Thus $N_G(L^*) = L^*$ and since L^*/M is nilpotent it follows that L^*/M is a Carter subgroup of G/M. By induction, L^* is conjugate to L in G and hence H^* is conjugate to H.

(iii) is clear.

(iv) Let $H \leq L \cap L^\xi$, where $\xi \in G$ and L is a subgroup of G containing the Carter subgroup H of G. Then H and $\xi H \xi^{-1}$ are Carter subgroups of L, hence conjugate in L by (ii), so that $\xi^{-1}\eta \in N_G(H) = H$ for some $\eta \in L$. It follows that $\xi \in L$. Thus H is abnormal in G.

(v) This has been shown in proving (i) and (ii) for the case $K = M$, a minimal normal subgroup of G. The general result follows at once.

(vi) Since Carter subgroups are dinormal by definition and systemizers are nilpotent by 10.2 (ii), this is clear.

(E) Following Wielandt, we call a subgroup H of G intravariant in G if H^α is conjugate to H in G for every $\alpha \in \mathrm{Aut}\, G$. Equivalently H is intravariant in G if and only if the class of conjugates to which H belongs is a characteristic class of conjugates in G i.e. is invariant under $\mathrm{Aut}\, G$. A normal subgroup is intravariant if and only if it is characteristic.

Lemma 10.8 (i) If H is intravariant in K and K is intravariant in G then H is intravariant in G.

(ii) If H is intravariant in G, so also are $N_G(H)$ and $C_G(H)$.

(iii) If H is intravariant in K and $K \lhd G$, then $K N_G(H) = G$.

(iv) Sylow subgroups are intravariant.

(v) In a soluble group, S_{π}-subgroups, systemizers and Carter subgroups are intravariant.

The proofs are immediate for (i), (ii), (iii). (iv) follows from Sylow's Theorem and (v) from 9.5, 10.1 and 10.7.

§11. Subnormal Subgroups (Wielandt)

(A). If H is any subgroup of G, we denote by $H^{\cdot\cdot G}$ the subnormal closure of H in G i.e. the intersection of all the subnormal subgroups of G which contain H. By 6.3 (iii), we have

$$H^{\cdot\cdot G} \text{ sbn } G .$$

The normal closure of H in $H^{\cdot\cdot G}$ is $H^{\cdot\cdot G}$ itself. Define $H_0 = G$ and $H_{n+1} = \{H^{H_n}\}$ inductively for $n \geq 0$. Then for some $r \geqslant 0$, we have

$$G = H_0 > H_1 > \cdots > H_r = H_{r+1} .$$

Since $H_{n+1} \lhd H_n$ for all n, we have H_r sbn G and so $H^{\cdot\cdot G} \leq H_r$. By 6.
$H^{\cdot\cdot G}$ sbn H_r. But $H_r = \{H^{H_r}\} = \{(H^{\cdot\cdot G})^{H_r}\}$. Hence $H_r = H^{\cdot\cdot G}$.

H sbn G if and only if $H = H^{\cdot\cdot G}$. In this case we call

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_r = H \qquad (1)$$

the canonical series from G to H and write $r = m(G,H)$. If we have any series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = H$ from G to H, then we obtain $G_i \geqslant H_i$ for all i by induction on i, and so $s \geqslant m(G,H)$.
$m(G,H)$ is the minimal length of a series from G to H.

Theorem 11.1 Let H and K be subnormal in G. Then $J = \{H,K\}$ is subnormal in G.

Proof: Suppose first that $H \lhd J$. Then K normalizes not only H but also, by induction on i, every term H_i of the canonical series (1). Hence $K_i = H_i K$ is a subgroup of G. Since K sbn G, we have K sbn K_i by 6.2. But $H_{i+1} \lhd H_i$ and K normalizes H_{i+1}. Hence $H_{i+1} \lhd K_i$. Now the product of a normal subgroup with a subnormal subgroup is a subnormal subgroup, since epimorphisms preserve the normality relation. Hence $K_{i+1} = H_{i+1}K$ sbn K_i. By 6.3 (ii), it follows that $J = K_r = HK$ sbn $G = K_0$ as required.

We prove the general result by induction on $m(G,H) = r$. If $r = 1$, then $H \lhd G$ and so $J = HK$ sbn G. Suppose $r > 1$, and let $\overline{H} = \{H^J\}$. For any $j \in J$, we have H^j sbn $H_1^j = H_1$ and $m(H_1, H^j) = m(H_1, H) = r-$

By the induction on r, all the groups $M = \langle H^{\xi_1}, H^{\xi_2}, \ldots, H^{\xi_n} \rangle$ with $\xi_1, \ldots, \xi_n$ in J are subnormal in H, and hence in G. This follows by induction on n. But for a suitable choice of the ξ's, $M = \overline{H}$. Hence $\overline{H}$ sbn G. But $J = \overline{H}K$ and $\overline{H} \lhd J$, K sbn G. So by the special case already considered we obtain J sbn G as required.

In view of 6.3 (iii), we may now state as a corollary that the subnormal subgroups of any group G form a sublattice of the lattice of all subgroups of G.

(B). By 7.61, every subnormal nilpotent subgroup of G is contained in the Fitting subgroup $\mathfrak{N}G$ of G. Conversely, if H is any subgroup of $\mathfrak{N}G$, then H sbn $\mathfrak{N}G$ by 6.8 (iii). Since $\mathfrak{N}G$ char G, it follows that H sbn G. Thus the subnormal nilpotent subgroups of G are precisely the subgroups of the Fitting subgroup of G.

Theorem 11.2 (i) Let H sbn G and let P be a Sylow p-subgroup of G. Then $H \cap P$ is a Sylow p-subgroup of H.

(ii) Let H be a soluble subgroup of G and suppose that, for all primes p and every Sylow p-subgroup P of G, $H \cap P$ is always a Sylow p-subgroup of H. Then H sbn G.

Proof: (i) is a corollary of 5.6.

(ii) Assuming $H \neq 1$, let M be a minimal normal subgroup of H. Since H is soluble, $|M| = p^n$ for some prime p and every Sylow p-subgroup of H contains M. Hence every Sylow p-subgroup of G contains M and $M \leq \overline{M}$, the maximal normal p-subgroup of G. Let $L = H\overline{M}$ and let Q_1 be a Sylow q-subgroup of L where $q \neq p$. Then $Q_1 \leq Q$, where Q is some Sylow q-subgroup of G and we have $H \cap Q \leq L \cap Q = Q_1$. By hypothesis, $H \cap Q$ is a Sylow q-subgroup of H. But $\overline{M} \lhd L$ and $Q \cap \overline{M} = 1$, since $q \neq p$. Since $L = H\overline{M}$, it follows that $H \cap Q$ is a Sylow q-subgroup of L. Hence $H \cap Q = Q_1 \leq H$. Thus H contains all p'-elements of L. These form a normal subgroup K of L and L/K is a p-group. Since $K \leq H \leq L$ it follows that

H sbn L, (since L/K is nilpotent by 6.8.)

The Sylow subgroups of $G/\overline{M}$ have the from $\overline{M}S/\overline{M}$ where S is a Sylow subgroup of G, by 5.6. Since $H \cap S$ is a Sylow subgroup of H by hypothesis, it follows that $(L \cap \overline{M}S)/\overline{M}$ is a Sylow subgroup of $L/\overline{M}$. This is true for every Sylow subgroup $\overline{M}S/\overline{M}$ of $G/\overline{M}$. By induction on $|G|$, we may therefore assume that $L/\overline{M}$ sbn $G/\overline{M}$, since $L/\overline{M} \cong H/\overline{M}$ is soluble. Thus L sbn G. Since H sbn L, we now have H sbn G by 6.3(ii).

Problem: Let p be a fixed prime. What can be said of those (soln subgroups H of G which intersect every Sylow p-subgroup of G in a Sylow p-subgroup of H?

(C) Theorem 11.3 (i) Let H sbn G, let P be a Sylow p-subgroup of H and let L be any subgroup of G. Then $\{P, L\}$ contains a Sylow p-subgroup of $\{H, L\}$.

(ii) Let $H_1, H_2, \ldots, H_n$ be subnormal subgroups of G and let P_i be a Sylow p-subgroup of H_i. Then $Q = \{P_1, P_2, \ldots, P_n\}$ contains a Sylow p-subgroup of $K = \{H_1, H_2, \ldots, H_n\}$.

(iii) The mapping

$$H \to H \cap P \qquad (H \text{ sbn } G),$$

where P is a fixed Sylow subgroup of G is a lattice homomorphism; in particular, if H_1 and H_2 are subnormal in G, then

$$\{H_1, H_2\} \cap P = \{H_1 \cap P, H_2 \cap P\}.$$

Proof: (i) is immediate if $H = G$ since then P is a Sylow p-subgp of G. If $H < G$, then $\overline{H} = \{H^\xi; \xi \in L\} < G$ and H^ξ sbn $\overline{H}$ for all $\xi \in L$ by 6.2. Also P^ξ is a Sylow p-subgroup of H^ξ. By induction on $|G|$, we may assume (ii) holds in $\overline{H}$ and so $\overline{P} = \{P^\xi; \xi \in L\}$ contains a Sylow p-subgroup of $\overline{H}$. But $\{H, L\} = \overline{H}L$; $\{P, L\} = \overline{P}L$; and by 3

$$|\overline{H}L : \overline{P}L| = |\overline{H} : \overline{P}| \cdot \frac{|L : \overline{H} \cap L|}{|L : \overline{P} \cap L|}$$

divides $|\overline{H} : \overline{P}|$ and is therefore prime to p. Thus (i) is proved.

To prove (ii), first suppose $n = 2$. Then we have

$|K:Q| = |K:\{P_1, H_2\}| \cdot |\{P_1, H_2\}:Q|$ and both these factors are prime to p by (i) since H_1 and H_2 are subnormal in G. Now let $n>2$. By induct on n, we may assume that $|K^*:Q^*|$ is prime to p, where $K^*=\{H_1,\cdots,H_{n-1}\}$ and $Q^*=\{P_1, P_2,\cdots,P_{n-1}\}$. But K^* sbn G by 11·1. Hence we have $|K:Q| = |\{K^*, H_n\}:\{Q^*, P_n\}|$ is prime to p by the case $n=2$, since Q^* contains a Sylow p-subgroup of K^*. Thus (ii) is proved.

(iii) $(H_1\cap P)\cap(H_2\cap P) = (H_1\cap H_2)\cap P$ so the mapping $H\to H\cap P$ is homomorphic with respect to intersections. If H_1 and H_2 are subnorma in G, then $H_1\cap P$ and $H_2\cap P$ are respectively Sylow p-subgroups of H_1 and H_2 and so $Q=\{H_1\cap P, H_2\cap P\}$ contains a Sylow p-subgroup of $K=\{H_1, H_2\}$ by (ii). But Q is a p-group. Hence Q is a Sylow p-subgroup of K. But K sbn G by 11·1 and so $K\cap P$ is also a Sylo p-subgroup of K. Since $Q\leq K\cap P$, it follows that $Q=K\cap P$ and s the mapping $H\to H\cap P$ (H sbn G) is also homomorphic with respect t joins.

(D). Let $M = \mathfrak{S}G$ be the semisimple radical of G and let H sbn G, so that

$$H = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G. \qquad (1)$$

Then $M_i = \mathfrak{S}H_i = H_i \cap M$ by 8·91 (ii) and M_i sbn G. Hence M_i is a direct factor of M by 8·91(i) and we may suppose that M_i is the direct product of M_{i-1} and N_i for each $i = 1, 2, \dots, r$. Since H normalizes both M_i and M_{i-1}, it must also normalize N_i. But $[H, N_i] \leq [H_{i-1}, H_i] \leq H_{i-1}$ and so $[H, N_i] \leq N_i \cap H_{i-1} = 1$. If $N = N_1 N_2 \cdots N_r$, we then have $[H, N] = 1$ and $M = \mathfrak{S}G$ is the direct product of $M_0 = \mathfrak{S}H$ and N. Since M_0 is semisimple, it is clear that $N = M \cap C_G(H)$.

Consider next the case in which $M = O_p G$ is the intersection of the Sylow p-subgroups of G. Then $M_i = M \cap H_i = O_p H_i$ by 8.92. Let $K = H^{O_p}$ be the subgroup generated by the p'-elements of H. Now $M = M_r$ and $[M_i, H] \leq M_{i-1}$ for each i, as in the semisimple case. Hence $[M, K] \leq M_r$. Suppose that for some $i > 0$, we have $[M, K] \leq M_i$ but $[M, K] \not\leq M_{i-1}$. Then we can choose $\alpha \in M$ so that $[\alpha, K] \not\leq M_{i-1}$. If $\xi, \eta \in K$, we have $[\xi\eta, \alpha] = [\xi, \alpha]^{\eta}[\eta, \alpha]$ by 7·1(i). Now $[\xi, \alpha] \in M_i$ by hypothesis, and so $[\xi, \alpha, \eta] \in M_{i-1}$. Hence the mapping $\xi \to [\xi, \alpha] M_{i-1}$ $(\xi \in K)$ is a homomorphism of K into the p-group M_i / M_{i-1}. But $K = H^{O_p}$ and so K has no quotient p-group other than K/K. Therefore the kernel of this homomorphism must be K and so $[K, \alpha] \leq M_{i-1}$, which is a contradiction. It follows that $[M, K] \leq M_0$.

Thus we have proved

Theorem 11·3. Let H be a subnormal subgroup of G. Then

(i) $\mathfrak{S}G$ is the direct product of $\mathfrak{S}H$ with $\mathfrak{S}G \cap C_G(H)$.

(ii) For every prime p, $[O_p G, H^{O_p}] \leq O_p H$.

(E) **Lemma 11.41** Let H, K, L, M be subgroups of a group G such that $[K,H] \leq L$ and $C_K(H) \leq M$. Then $|K| \leq |L|^{|H|} \cdot |M|$

Given $\alpha \in K$ consider the mapping $k(\alpha) : \xi \to [\xi, \alpha]$ $(\xi \in H)$. This is a mapping of H into L. If $\beta \in K$, we have $k(\alpha) = k(\beta)$ if and only if $\xi^\alpha = \xi^\beta$ for all $\xi \in H$, i.e. if $\alpha\beta^{-1} \in C_K(H)$. The number of distinct mappings $k(\alpha)$, $\alpha \in K$, is therefore $|K : C_K(H)|$. This cannot exceed $|L|^{|H|}$. Since $|C_K(H)| \leq |M|$, we obtain the result stated.

Theorem 11.42 Let H be a subnormal subgroup of G and let $C = \bigcap C_G(H^\alpha)$, where $H^\alpha = \mathfrak{G}_\infty H = \bigcap_p H^{\sigma_p}$ is the lower central limit of H. Then $|G|$ is bounded by a number depending only on $|H|$ and $|C|$.

Proof: Let $h = |H|$ and $c = |C|$. We can choose the classes $\mathfrak{X}_1, \mathfrak{X}_2, \dots, \mathfrak{X}_n$ where each $\mathfrak{X}_i$ is either $\mathfrak{A}$ or σ_p for some prime p so that we have

$$1 = L_0 < L_1 < \cdots < L_n = H$$

and $$L_i = \mathfrak{X}_i(H \bmod L_{i-1}) \qquad (i = 1, 2, \dots, n).$$

Here n is at most equal to the length of a chief series of H and so $n < h$, if we ignore the trivial case $H = 1$. If we define

$$1 = K_0 < K_1 < \cdots < K_n = K$$

by the equations $K_i = \mathfrak{X}_i(G \bmod K_{i-1})$, then by 8.92 we have $H_i = H \cap K_i$ for each $i = 1, 2, \dots, n$. If $N = H^\alpha$, we have $N \leq H^{\sigma_p} \leq H$ and so $[K_i, N] \leq K_{i-1} L_i$ for each i, by 11.3. Let $k_i = |K_i|$. Since N and L_i are subgroups of H, we obtain $k_i \leq (k_{i-1} h)^h c$, by 11.41; and so by induction on i, $k = k_n \leq f(h,c)$ owing to $n < h$. Hence $|G : C_G(K)| \leq h!$, since $K \lhd G$. But $N \leq H \leq K$ and so $|C_G(K)| \leq c$. Hence $|G| \leq c \cdot f(h,c)!$ and 11.42 is proved.

Now suppose that $\mathfrak{X}_i = \sigma_p$ so that K_i / K_{i-1} is a p-group; and let $M = K_i \cap C_G(H^{\sigma_p})$. Then $M \lhd HM$, since $K_i \lhd G$ and H normalizes $C_G(H^{\sigma_p})$. Hence if Q is a Sylow p-subgroup of HM containing a given Sylow p-subgroup P of H, then $R = Q \cap M$ is a Sylow p-subgroup of M and $R \lhd Q$. If $R \neq 1$, it follows that there is an

element $y \neq 1$ in $R \cap zQ$. Then y centralizes H^{σ_p}, since $y \in M$; and y also centralizes P since $y \in zQ$ and $P \leq Q$. But $H = PH^{\sigma_p}$, and so y centralizes H. We conclude that, if $C_G(H) = 1$, then M must be a p'-group and hence $M \leq K_{i-1}$. In this case, 11·3(ii) and 11·4 give the inequality $k_i \leq (k_{i-1}h)^h k_{i-1}$; and so by induction on i, we find $k \leq f(h)$, a bound depending only on h. Since $H \leq K$, we also have $C_G(K) = 1$ and hence $|G| \leq k!$ Thus we obtain

Theorem 11·43 Let H be subnormal in G and let $C_G(H) = 1$. Then $|G|$ is bounded by a number depending only on $|H|$.

(F). Let $H = H_1$ be a group with $zH = 1$. Then the mapping

$$\xi \to t(\xi) \qquad (\xi \in H)$$

of H onto its group of inner automorphisms is isomorphic. If we identify ξ with $t(\xi)$, we obtain $H_1 \lhd H_2 = \mathrm{Aut}\, H_1$. Since $[H_1, zH_2] = 1$, we have $zH_2 = 1$. Hence H_2 can be embedded canonically in $H_3 = \mathrm{Aut}\, H_2$ and so on. In this way we form the automorphism tower of H

$$H_1 \lhd H_2 \lhd H_3 \lhd H_4 \cdots$$

where $H_{i+1} = \mathrm{Aut}\, H_i$ and each $\xi \in H_i$ is identified with the corresponding inner automorphism $t(\xi) \in H_{i+1}$. And we have $zH_i = 1$ for all i.

For $i < j$, let $C_{ij} = C_{H_j}(H_i)$ and $N_{ij} = N_{H_j}(H_i)$. Then $C_{ij} \lhd N_{ij}$, $H_{i+1} \leq N_{ij}$ and $H_{i+1} \cap C_{ij} = 1$. Since $H_{i+1} \lhd H_{i+2}$, it follows that the product $H_{i+1} C_{i,i+2}$ is direct, and so $C_{i,i+2} \leq C_{i+1,i+2} = 1$. Every $\alpha \in N_{i,i+2}$ induces in H_i an automorphism $\beta \in H_{i+1}$ and so $\alpha\beta^{-1} \in C_{i,i+2}$. Since $C_{i,i+2} = 1$, it follows that $\alpha = \beta \in H_{i+1}$ and $N_{i,i+2} = H_{i+1}$. Suppose we have proved that $N_{i,i+j} = H_{i+1}$ and $C_{i,i+j} = 1$ for all $j = 1, 2, \cdots, k-1$ and all i. Then $H_{i+1} = N_{i,i+k} \cap H_{i+k-1} \lhd N_{i,i+k} \leq H_{i+k}$, since $H_{i+k-1} \lhd H_{i+k}$. Hence $N_{i,i+k} \leq N_{i+1,i+k} = H_{i+2}$ by hypothesis. So $N_{i,i+k} = N_{i,i+2} = H_{i+1}$, and [illegible] so $C_{i,i+k} = C_{i,i+1} = 1$. By induction on k, we have proved

Theorem 11·5 If $H = H_0 \lhd H_1 \lhd H_2 \lhd \cdots$ is the automorphism tower of a group H with $zH = 1$, then $N_{H_n}(H) = H_1$ and $C_{H_n}(H) = 1$ for all n. For some n, we must have $H_n = H_{n+1} = \cdots$.

§12 Wreath Products, Burnside's Transfer Theorem, Z-groups, A-groups, Supersolv

(A) Let H and K be subgroups of $\Sigma(X)$ and $\Sigma(Y)$ respectively, and let $Z = X \times Y$ be the set of all ordered pairs (x, y) with $x \in X$, $y \in Y$. For $\xi \in H$, $y \in Y$ and $\eta \in K$ define the permutations ξ_y and $\overline{\eta}$ of Z by

$$(x, y)\xi_y = (x\xi, y) \; ; \quad (x, y_1)\xi_y = (x, y_1) \text{ if } y_1 \neq y \; ;$$
$$(x, y)\overline{\eta} = (x, y\eta) .$$

The group $H \wr K$ generated by all these permutations is called the wreath product of H with K. It is usual to identify $\overline{\eta}$ with η, so that K becomes a subgroup of $W = H \wr K$. For fixed $y \in Y$, the mapping $\xi \to \xi_y$ $(\xi \in H)$ is an isomorphism of H onto a subgroup H_y of W, and the product

$$\overline{H} = \prod_{y \in Y} H_y$$

is direct. $\overline{H}$ is called the base group of W. K is faithfully represented by automorphisms of $\overline{H}$ according to the law

$$\eta^{-1} \xi_y \eta = \xi_{y\eta} \qquad (\eta \in K, y \in Y, \xi \in H),$$

i.e. K permutes the $|Y|$ direct factors of $\overline{H}$. If this representation of K is f, then

$$H \wr K = \langle K, \overline{H} ; f \rangle$$

is the corresponding split extension. $W = \overline{H}K$; $\overline{H} \cap K = 1$; $\overline{H} \lhd K$. If $|X| = l$, $|Y| = m$, then W is a permutation group of degree lm and order $|H|^m \cdot |K|$.

If L is a subgroup of $\Sigma(V)$, where $|V| = n$ and if we make the natural identification $((x, y), v) = (x, (y, v)) = (x, y, v)$, then the two groups $(H \wr K) \wr L$ and $H \wr (K \wr L)$ coincide. This is the associative law for wreath products, and permits us to omit brackets in a repeated wreath product.

If H or K or both are not given explicitly as permutation groups, then $H \wr K$ is to be interpreted as being formed from the appropriate regular representation. We call this the regularity convention. For example we have

Lemma 12.1 If C is a cyclic group of order p, then the group

$$\wr^n C = \underbrace{C \wr C \wr \cdots \wr C}_{n}$$

is a Sylow p-subgroup of $\Sigma(C^n)$.

For $|C^n| = p^n$, C^n being the set of all ordered n-tuplets of elements of Hence $|\Sigma(C^n)|_p = (p^n!)_p = p^{1+p+p^2+\cdots+p^{n-1}} = |\wr^n C|$ by induction on n. This remark is due to Kalojnine.

Note that $H \wr K$ is determined to within isomorphism by the group H and the permutation group K, and does not depend as a group on the permutational representation chosen for H.

Lemma 12.2 (B) If H and K are given groups and $W = H \wr K$ (with the regularity convention), then every subgroup K_1 of W which is transversal to the base group $\overline{H}$ in W is conjugate to K in W.

Proof: Here we may identify $\xi \in H$ with $\xi_1 \in H_1$, so that $H = H_1$ and $H_\alpha = H^\alpha$, $\xi_\alpha = \alpha^{-1}\xi\alpha = \xi^\alpha$ for $\alpha \in K$. $\overline{H}$ is the direct prodn of the H^α, $\alpha \in K$. Every element $u \in \overline{H}$ is uniquely expressible as a product $\prod_{\alpha\in K} u_\alpha{}^\alpha$, with factors $u_\alpha \in H = H_1$. Since K_1 is transversal to $\overline{H}$ in W, the coset $\alpha\overline{H}$ contains exactly one element $\alpha u(\alpha)$ of K and since K_1 is a subgroup of W, we have $u(\alpha)^\beta u(\beta) = u(\alpha\beta)$ for all $\alpha, \beta \in K$. Factorising, this gives

$$u(\alpha\beta)_\eta = u(\alpha)_{\eta\beta^{-1}}\, u(\beta)_\eta \qquad (1)$$

for all $\alpha, \beta, \eta \in K$. Let $v \in \overline{H}$ have factors $v_\beta = u(\beta^{-1})_1$ so that $v = \prod_{\beta\in K} (u(\beta^{-1})_1)^\beta$. The β-factor of v^α is therefore $v_{\beta\alpha^{-1}}$ $= u(\beta\alpha^{-1})_1$. But the β-factor of $u(\alpha)v$ is $u(\alpha)_\beta\, u(\beta^{-1})_1 = u(\alpha\beta^{-1})_1$ by (1), and this is precisely the β-factor of v^{α}. Hence $v^\alpha = u(\alpha)v$ for all $\alpha \in K$, and so $\alpha u(\alpha) = v\alpha v^{-1}$. Thus $K = K_1^v$ is conjugate to K_1 in W as stated.

(C) Lemma 12·3 Let H be a subgroup of G and let S be any transversal to H in G, with elements $\sigma_1, \sigma_2, \dots, \sigma_m$ where $m = |G:H|$. For $\xi \in G$ and $1 \le i \le m$, define $i\xi$ by the condition $\sigma_i \xi \sigma_{i\xi}^{-1} \in H$, and let X be the set whose elements are the m cosets of H in G, so that $\tau_H(\xi)$ is the permutation $H\sigma_i \to H\sigma_i\xi = H\sigma_{i\xi}$ $(i = 1, \dots, m)$ of X. Define $m_H(\xi)$ to be the permutation

$$(\eta, H\sigma_i) \to (\eta\sigma_i\xi\sigma_{i\xi}^{-1}, H\sigma_{i\xi}) \qquad (\eta \in H,\ 1 \le i \le m)$$

of $H \times X$. Then m_H is an isomorphism mapping G into $H \wr \tau_H(G)$.

Here H is in its regular representation i.e. the regularity convention operates for H. Since $(i\xi)\xi_1 = i(\xi\xi_1)$ for $\xi, \xi_1 \in G$, we have $m_H(\xi\xi_1) = m_H(\xi)\, m_H(\xi_1)$. $m_H(\xi)$ is the identity on $H \times X$ only if $i\xi = i$ for all i and in addition $\sigma_i \xi \sigma_i^{-1} = 1$, which implies $\xi = 1$. Hence m_H is an isomorphic mapping of G into $\Sigma(H \times X)$. $W = H \wr \tau_H($ contains the permutation $(\eta, H\sigma_i) \to (\eta, H\sigma_{i\xi})$ which we identify with $\tau_H(\xi)$, and $m_H(\xi)\,\tau_H(\xi)^{-1}$ maps $(\eta, H\sigma_i)$ into $(\eta\sigma_i\xi\sigma_{i\xi}^{-1}, H\sigma_i)$. This shows that $m_H(\xi)\,\tau_H(\xi)^{-1}$ belongs to the base group $\overline{H}$ of W and so $m_H(\xi) \in W = \overline{H}\,\tau_H(G)$. This proves 12·3.

It is clear that the representation m_H of G depends not only on the subgroup H but also on the choice of the transversal S. However, preserving the notations of 12·3, we have

Lemma 12·4 Let f be a homomorphism of the subgroup H of G into an Abelian group A, which we write in additive notation. Then the mapping f^* of G into A defined by

$$f^*(\xi) = \sum_{i=1}^{m} f(\sigma_i \xi \sigma_{i\xi}^{-1})$$

is also homomorphic and is independent of the choice of the transversal S. Moreover

$$f^*(\xi) = \sum_{j \in J} f(\sigma_j \xi^{\tau_j} \sigma_j^{-1})$$

where the cosets $H\sigma_j$ are chosen one from each cycle of $\tau_H(\xi)$, and τ_j is the order of the cycle to which $H\sigma_j$ belongs, so that $\sum_{j \in J} \tau_j = |G:H| = m$.

Proof: Since f is homomorphic, we have for all i and all $\xi, \eta \in G$, $f(\sigma_i \xi \eta \sigma_{i\xi\eta}^{-1}) = f(\sigma_i \xi \sigma_{i\xi}^{-1}) + f(\sigma_{i\xi} \eta \sigma_{i\xi\eta}^{-1})$. Hence $f^*(\xi\eta) = f^*(\xi) + f^*(\eta)$ and f^* is homomorphic. If T is any other transversal to H in G, with elements $\tau_i = \eta_i \sigma_i$, $\eta_i \in H$, then $\tau_i \xi \tau_{i\xi}^{-1} = \eta_i (\sigma_i \xi \sigma_{i\xi}^{-1}) \eta_{i\xi}^{-1}$ and $f(\tau_i \xi \tau_{i\xi}^{-1}) = f(\eta_i) - f(\eta_{i\xi}) + f(\sigma_i \xi \sigma_{i\xi}^{-1})$. Summing for $i = 1, \cdots, m$, we obtain $\sum_i f(\tau_i \xi \tau_{i\xi}^{-1}) = \sum_i f(\sigma_i \xi \sigma_{i\xi}^{-1})$ since $\sum_i f(\eta_i) = \sum_i f(\eta_{i\xi})$. Thus f^* is independent of the choice of transversal.

The contribution to $f^*(\xi)$ of the cycle of $\tau_H(\xi)$ which contains $H\sigma_j$ is $\sum_{i=0}^{\tau_j - 1} f(\sigma_j \xi^i \xi \sigma_{j\xi^{i+1}}^{-1}) = f(\sigma_j \xi^{\tau_j} \sigma_j^{-1})$ since $j\xi^{\tau_j} = j$ and f is homomorphic. Thus 12.4 is proved

We call f^* the <u>transfer of f to G</u>. This is the terminology suggested by cohomology theory. However, if f is the natural homomorphism $\eta \to H'\eta$ $(\eta \in H)$ of H onto $A = H/H'$, then f^* is the <u>transfer of G into H</u>. It is a homomorphism of G into H/H' and, for $\xi \in G$, we have in this case

$$f^*(\xi) = H' \prod_{i=1}^{m} (\sigma_i \xi \sigma_{i\xi}^{-1}) = H' \prod_{j \in J} (\sigma_j \xi^{\tau_j} \sigma_j^{-1}). \qquad (1)$$

Note that $\sigma_j \xi^{\tau_j} \sigma_j^{-1}$ is the first positive power of $\sigma_j \xi \sigma_j^{-1}$ which lies in H

(D) <u>Theorem 12.5</u>. Let the group G have an Abelian Sylow p-subgroup. Let $N = N_G(H)$, $C = \zeta N \cap H$, $D = [H, N]$. Let i be the identity mapping of H, i^* the transfer of i to G and K the kernel of i^*. Then H is the direct product of C and D. Also $C = i^*(G) = i^*(H)$ and $D = G' \cap H = K \cap H$. G is the split extension of K by C and $G/K \cong C$ is the maximal p-quotient group of G.

Proof: Since $H' = 1$, we have $i^*(\xi) = \prod_{j \in J} \sigma_j \xi^{\tau_j} \sigma_j^{-1}$ by (1) above, for any $\xi \in G$. If $\xi \in H$, then the elements ξ^{τ_j} and $\sigma_j \xi^{\tau_j} \sigma_j^{-1}$ both lie in H and are conjugate in G. By 6.63, it follows that these two elements are conjugate in N, since $H = \zeta H$ is Abelian. Since $\sum_{j \in J} \tau_j = m = |G : H|$, we may therefore write $\sigma_j \xi^{\tau_j} \sigma_j^{-1} = \tau_j^{-1} \xi^{\tau_j} \tau_j$

with $\tau_j \in N$, and so

$$i^*(\xi) = \xi^m \prod_{j \in J} [\xi^{\tau_j}, \tau_j] \qquad (2)$$

for all $\xi \in H$, where of course J, τ_j and τ_j in general depend on ξ. If $\xi \in C$, then ξ^{τ_j} commutes with τ_j and so $i^*(\xi) = \xi^m$. But C is a p-group and $(m, p) = 1$. Hence $i^*(C) = C$.

If $\eta \in N$ and $\xi \in G$, then $\eta \sigma_i \xi (\eta \sigma_j)^{-1} \in H$ if and only if $\sigma_i \xi \sigma_j^{-1} \in H$. Hence ηS is also transversal to H in G, and replacing S by ηS does not affect $i^*(\xi)$ by 12.4. Hence $\eta\, i^*(\xi)\, \eta^{-1} = i^*(\xi)$ for all $\xi \in G$, $\eta \in H$. It follows that $i^*(G) = i^*(H) = i^*(C) = C$. Hence $KC = G$, $K \cap C = 1$ and G is a split extension of K by C. Since m is prime to $|H|$, every element of H has the form ξ^m with $\xi \in H$ and (2) now shows that $H = CD$. But $D = [H, N] \leq G' \leq K$ since $G/K \cong C$ is Abelian. Since $K \cap C = 1$, this shows that the product $H = CD$ is direct, and that $G' \cap H = K \cap H = D$.

Finally, let $K_1 \lhd G$ and let G/K_1 be a p-group. Then $K_1 H = G$ by 5.7 and so $G/K_1 \cong H/K_1 \cap H$ is Abelian. Hence K_1 contains G' and $|G : K_1| \leq |H : G' \cap H| = |C| = |G : K|$. Since $G/K \cap K_1$ is also a p-group, it follows that $K_1 \geq K$ and so G/K is the maximal p-quotient group of G.

Corollary 12.51 If the group G has a Sylow p-subgroup H which is contained in the centre of its normalizer in G, then G has a normal $S_{p'}$-subgroup.

For in this case $C = H$ and G is the split extension of K by H. Hence K is a normal $S_{p'}$-subgroup of G.

(E) A soluble group whose Sylow subgroups are all Abelian is called an A-group. The following result is due to D.R. Taunt.

Theorem 12.6 Let G be an A-group. Then

(i) $\zeta G \cap G' = 1$; (ii) if S is any systemizer of G, then G is the split extension of G' by S; (iii) more generally, if T is a relative systemizer of K in G, where $K \lhd G$, then $K'T = G$ and $T \cap K' = 1$; (iv) the length of the derived series of G cannot exceed the number of distinct primes which divide $|G|$.

Proof : (i) Suppose if possible that $\mathfrak{z}G \cap G'$ contains an element ξ of prime order p, let H be a Sylow p-subgroup of G containing ξ. Since H is Abelian, we can use the notation of 12·5. Then $\xi \in \mathfrak{z}N \cap H = C$ and $\xi \in G' \cap H = D$. But $C \cap D = 1$ so $\xi = 1$, a contradiction. Hence $\mathfrak{z}G \cap G' = 1$.

(ii) Let K/L be a chief factor of G with $K \leq G'$. Then G/L is an A-group by 5·6. Its derived group is G'/L. It follows from (i) that K/L is not a central factor of G. Hence $S \cap K \leq L$ by 10·4. Since this is true for all such K/L, we have $S \cap G' = 1$. By 10·4·2, SG' and this proves (ii).

(iii) Here K is an A-group by 5·6 and so $T \cap K' = 1$ by (ii); while by 10·8 (ii) and (v), $TK = G$. Since $K \leq TK'$ by 10·4·2, we have $TK' =$ and this proves (iii).

(iv) Suppose that $|G|$ has just n different prime factors. If $n = 1$, G is Abelian and $G' = 1$ by definition. Let $n > 1$ and let M be a minimal normal subgroup of G. If $|M| = p^m$, then every Sylow p-subg H contains M. Since H is Abelian, $H \leq C_G(M)$ and hence the automizer $G/C_G(M)$ is a p'-group. More generally, if K/L is any chief factor of G and if $|K:L| = p^l$, $C = C_G(K/L)$ is of index prime to p in G. Hence $|G/C|$ has at most $n-1$ different prime factors. By induction on n, we may assume that the $n-1$-st derived group of G/C is the unit subgroup. Since $(G/C)^{(n-1)} = CG^{(n-1)}/C$, this means that $G^{(n-1)} \leq C$. Then $G^{(n-1)}$ centralizes every chief factor of G. Hence $G^{(n-1)}$ has a central series and so is nilpotent. But $G^{(n-1)}$ is also an A-group and so it is the direct product of Abelian groups viz. its Sylow subgroups. Hence $G^{(n-1)}$ is itself Abelian and $G^{(n)} = 1$, as required.

(F) Note in passing the following (forgotten)

Lemma 12.7 (i) In any group G, the Fitting subgroup is the intersection of the centralizers of the chief factors of G.

(ii) In any soluble group G, the hypercentre is the intersection of the systemizers of G.

Proof: (i) Let $F = \mathfrak{N}G$, and let $C = \cap C_G(H/K)$ over all chief factors H/K of G. By 9.3 (i), we have $F \leq \mathfrak{N}(G \bmod K) \leq C_G(H/K)$ and so $F \leq C$. On the other hand, C has a central series viz. the part of any chief series of G from 1 to C. Hence C is nilpotent; and so $C \leq F$ by 7.61, since $C \lhd G$. Thus $C = F$.

(ii) Let $H = Z^\infty G$ and let K be the intersection of the systemizers of G. If L/M is any chief factor of G with $L \leq K$, then $L \leq MS$ for any systemizer S and so, by 10.4, L/M is a central factor of G. Hence $[L, G] \leq M$ and so $K \leq H$. Conversely, if L/M is any chief factor of G this time with $L \leq H$, then L/M is a central factor of G and so by 10.4 again $L \leq MS$. This is true for all such L/M and so $H \leq S$. This is true for all systemizers S of G and so $H \leq K$. Hence $H = K$.

(G) Let C_n denote a cyclic group of order n and let $\Phi_n = \operatorname{Aut} C_n$. If $C_n = \{\xi\}$ and $\alpha \in \Phi_n$, then $C_n = \{\xi^\alpha\}$ and so $\xi^\alpha = \xi^a$ where $(a, n) = 1$, by 2.5. Conversely, if $(a, n) = 1$, then $\xi^s \to \xi^{as}$ $(s = 0, 1, \ldots, n-1)$ is an automorphism of C_n. If $\beta \in \Phi_n$ and $\xi^\beta = \xi^b$, then $\xi^{\alpha\beta} = \xi^{ab} = \xi^{\beta\alpha}$. Hence Φ_n is Abelian. The integer a is determined by the automorphism α only modulo n. Thus Φ_n is isomorphic with the multiplicative group of prime residue classes mod n, i.e. of all those residue classes (a) mod n for which $(a, n) = 1$.

The number $\varphi(n) = |\Phi_n|$ is called Euler's function. If $(m, n) = 1$, then Φ_{mn} is the direct product of subgroups isomorphic with Φ_m and Φ_n respectively by 8.2. Thus, if $(m, n) = 1$,

$$\Phi_{mn} \simeq \Phi_m \times \Phi_n \quad \text{and} \quad \varphi(mn) = \varphi(m)\varphi(n)$$

Here we merely need to record

Lemma 12.8 (i) The group of automorphisms of a cyclic group of order n is an Abelian group of order $\varphi(n)$.

(ii) If p is a prime, $\varphi(p^m) = p^{m-1}(p-1)$.

(iii) Let H be a Sylow p-subgroup of G, where p is the smallest prime dividing $|G|$. If H is cyclic, then G has a normal $S_{p'}$-subgroup.

Proof: (i) has already been shown and (ii) is clear since $C_{p^m} = \{1\}$ has only one maximal subgroup viz. $\{1\}^p$ of order p^{m-1}.

(iii) Since H is Abelian, we have $H \leq C_G(H) \leq N_G(H) = N$ and so the automizer $A_G(H) \cong N_G(H)/C_G(H)$ has order prime to p. Any prime q which divides $|A_G(H)|$ is therefore greater than p, by definition of p. But $q \leq 1$ by (ii)., so no such prime exists. Hence $H \leq ZN$ and the result follows from 12.51.

(H) A group G is called a Z-group if all its Sylow subgroups are cyclic. A group G is called supersoluble if all its chief factors are cyclic.

Theorem 12.9. (i) Z-groups are supersoluble.

(ii) If G is supersoluble, then G' is nilpotent; every maximal subgroup of G has index a prime; and if ϖ consists of all primes $\geq p$, then G has a normal S_ϖ-subgroup. Here p is any prime.

(iii) If G is a Z-group, then G' is cyclic and so are the systemizers S of G; moreover $|G'|$ and $|S|$ are coprime and G is the split extension of G' by S. Further, for each divisor d of $|G|$, G contains one and only one class of conjugate subgroups of order d.

Proof: (i) Let G be a Z-group. By 12.8, G has a normal $S_{p'}$-subgroup G_1 where p is the smallest prime dividing $|G|$. By induction on $|G|$, we may assume G_1 soluble. G/G_1 is a p-group and therefore soluble. Hence G is soluble. By 5.6 all sections of Z-groups are Z-groups. In particular, a chief factor of G must be cyclic of prime order, since it is an elementary Abelian prime-power group by the solubility

of G.

(ii) Let G be supersoluble. By 12·7 (i), $F = \mathfrak{N}G = \cap C_G(H/K)$ over all chief factors H/K of G. By definition, each H/K is cyclic and so, by 12·8 (i), $G/C_G(H/K)$ is Abelian. All these centralizers contain G' by 7 Hence $G' \leq F$ and so G' is nilpotent.

By 9·2, if M is any maximal subgroup of a soluble group G, then $|G:M| = |H:K|$ for some chief factor H/K of G. If G is supersoluble, $|H:K|$ is a prime and so every maximal subgroup of G is of index a prime

Let $G = G_0 > G_1 > \cdots > G_n = 1$ be a chief series of G. Since G is supersoluble, each $|G_{i-1}:G_i| = p_i$ is a prime. Choose a chief series for which $\sum_{i=1}^{n} i p_i = s$ is a maximum and suppose if possible that $p_i > p_{i+1}$ for some i. A Sylow p_i-subgroup G_i^*/G_{i+1} of G_{i-1}/G_{i+1} is normal in G_{i-1}/G_{i+1} by 5·4 (iv). G_i^*/G_{i+1} is therefore characteristic in G_{i-1}/G_{i+1}, he $G_i^* \lhd G$ and we may obtain a new chief series with larger s by replaci G_i by G_i^*. This contradicts our choice of chief series. Hence $p_i \leq p_{i+1}$ for all $i = 1, 2, \cdots, n-1$ and one of the terms G_i will be an S_ϖ-subg of G with the given set of primes ϖ.

(iii) Let G be a Z-group. By (i) and (ii), G' is nilpotent. G' is al a Z-group, hence G' is cyclic by 8·2 (i) and (iii). Since G is an A-gr we have $G = G'S$, $G' \cap S = 1$, by 12·6 (ii); and so $S \cong G/G'$ is Abel Since S is also a Z-group, S is cyclic by 8·2 again.

Let q be the greatest prime dividing $|G|$. By (i) and (ii) the Sylow q-subgroup of G is normal in G. It is also cyclic. Hence G ha one and only one subgroup Q of order q. If q divides d, every subgro H of G of order d must contain Q. By induction on $|G|$, we may assume that the Z-group G/Q has one and only one class of conjugate subgroups of order d/q. The result for G now follows.

If q does not divide d, and if H is any subgroup of G of order d then $Q \cap H = 1$ and QH/Q is a subgroup of order d of G/Q, and so H is an $S_{q'}$-subgroup of QH. By induction, we may assume that

subgroups G/Q has a single class of conjugate subgroups K/Q of order d_3. By 9.5, each such K has a single class of conjugate subgroups H of order d and $K = HQ$. Hence in this case also the corresponding result follows for G.

This completes the proof of 12.9. Perhaps we should add

Lemma 12.91 Let A be a maximal normal Abelian subgroup of the supersoluble group G. Then $A = C_G(A)$.

Proof: Let $C = C_G(A)$. Since A is Abelian, we have $A \leq C$. Since $A \lhd G$ we have $C \lhd G$. Hence if $A < C$, there is a chief factor B/A of G such that $B \leq C$. Since G is supersoluble, B/A is cyclic of order a prime. Since $B \leq C_G(A)$, we have $A \leq zB$, and so B/zB is cyclic. Hence $B = zB$ is Abelian by 7.2(iii), contrary to the definition of A. This contradiction shows that $A = C$.

Note that nilpotent groups are supersoluble. Hence 12.91 applies when G is a p-group.

Corollary 12.92 Let H be a Sylow p-subgroup of any group G and let A be a maximal normal Abelian subgroup of H. Then A is a Sylow p-subgroup of $C = C_G(A)$.

Proof: Since $A \lhd H$, we have $H \leq N = N_G(A)$. H is therefore a Sylow p-subgroup of N. Since $C \lhd N$, it follows that $H \cap C$ is a Sylow p-subgroup of C by 5.6. But $H \cap C = A$ by 12.91.

§13. p'-Automorphisms of p-groups.

(A) Let $V = X \oplus Y$ be an additive Abelian p-group and let Γ be a p'-group operating on V and leaving the direct summand X invariant: so $v(\xi\eta) = (v\xi)\eta$ for $v \in V$, ξ and η in Γ; $(u+v)\xi = u\xi + v\xi$ for $u, v \in V$, ξ in Γ; and $X\Gamma = X$.

Every $v \in V$ is uniquely expressible in the form $x+y$ with $x \in X$, $y \in Y$. For $y \in Y$, $\xi \in \Gamma$ we can therefore define $y^\xi \in Y$ and $y_\xi \in X$ by the equation

$$y\xi = y^\xi + y_\xi .$$

Expressing that $y(\xi\eta) = (y\xi)\eta$, we then obtain

$$y^{\xi\eta} = (y^\xi)^\eta \quad \text{and} \quad y_{\xi\eta} = y^\xi{}_\eta + y_\xi\eta \tag{1}$$

for all $\xi, \eta \in \Gamma$.

Let $|\Gamma| = g$. Since $(g,p) = 1$, we can choose an integer h such that $gh \equiv 1 \mod |V|$ and so $gh v = v$ for all $v \in V$. Define

$$w(y) = h \sum_{\eta \in \Gamma} y^\eta{}_{\eta^{-1}}, \tag{2}$$

so that $y \to w(y)$ is a mapping of Y into X. Then for $\xi \in \Gamma$,

$$w(y^\xi) = h \sum_\eta y^{\xi\eta}{}_{\eta^{-1}} = h \sum_\eta y^\eta{}_{\eta^{-1}\xi}$$

by the first equation of (1) and so, by the second equation of (1), we h

$$w(y^\xi) = h \sum_\eta (y_\xi - y_\eta \eta^{-1}\xi) = y_\xi - \Big(h \sum_\eta y_\eta \eta^{-1}\Big)\xi .$$

But $y1 = y$ and so $y_1 = 0$ if 1 is the unit element of Γ. So (1) fu $y_\eta \eta^{-1} = -y^\eta{}_{\eta^{-1}}$ and we obtain

$$w(y^\xi) = y_\xi + w(y)\xi \tag{3}$$

For y_1, y_2 in Y we have $(y_1 + y_2)\xi = y_1\xi + y_2\xi$ and hence $(y_1+y_2)^\xi = y_1^\xi + y_2^\xi$, $(y_1+y_2)_\xi = (y_1)_\xi + (y_2)_\xi$ and so

$$w(y_1 + y_2) = w(y_1) + w(y_2) \tag{4}.$$

So $y \to w(y)$ is a homomorphism of Y into X and the set T of all

$$t(y) = y + w(y) \qquad (y \in Y)$$

is therefore a subgroup of V complementary to X, i.e. $V = X \oplus T$.

Since $t(y)^\sigma = y^\sigma + w(y)^\sigma = y^\sigma + y_\sigma + w(y)^\sigma = y^\sigma + w(y^\sigma) = t(y^\sigma)$ by (3), we see that T is Γ-invariant. This gives

Theorem 13.1 Let the p'-group Γ be represented by automorphisms of the additive Abelian p-group V. If Γ leaves invariant a direct summand X of V, then there is a Γ-invariant subgroup T such that $V = X \oplus T$.

Note that the number of subgroups Y of V such that $V = X \oplus Y$ is equal to $|\mathrm{Hom}(V/X, X)|$, which is a power of p. Hence 13.1 is immediate in the case $|\Gamma| = q^m$, q prime.

V is called Γ-indecomposable if it cannot be expressed as the direct sum of two proper Γ-invariant subgroups. Obviously, we can always express V as a direct sum $V_1 \oplus V_2 \oplus \cdots \oplus V_r$ $(r \geq 0)$ of Γ-invariant subgroups $V_i \neq 0$ each of which is Γ-indecomposable. The V_i are Γ-indecomposable components of V.

An Abelian p-group is called homocyclic if all its invariants are equa

Corollary 13.11. The Γ-indecomposable components of V are all homocyclic

Proof: We may assume that V is Γ-indecomposable. Suppose if possible that V is not homocyclic and let l be the largest invariant of V. Then $l > 1$ and if $W = \Omega_1 V$ and $X = W \cap \mathfrak{V}_{l-1} V$, we have $0 < X < W$. Since W is elementary, X is a direct summand of W. Since X and W are characteristic in V, they are Γ-invariant. Hence there is a Γ-invaria subgroup T_1 such that $W = X \oplus T_1$ by 13.1. Since $X \cap T_1 = 0$, the largest invariant of $V_1 = V/T_1$ is still l. If V_1 is not homocyclic, we can proceed similarly to the existence of a Γ-invariant subgroup $T_2 > T_1$ such that $T_2 \cap X + T_1 = T_1$ and so $T_2 \cap X = 0$, and the largest invariant of $V_2 = V/T_2$ is therefore still l. Continuing in this way, we eventually find a Γ-invariant subgroup T of V such that $X \cap T = 0$ and V/T is homocyclic. If $|X| = p^r$, this implies that V/T is of type $(l, l, \ldots, l)$ (r times). Here r is the multiplicity of l as an invariant of V, and V contains subgroups $U \cong V/T$. For any such U, $\Omega_1(U) = \mathfrak{V}_{l-1}(U) = X$ and so $V = T \oplus$

It follows from 13·1 that U may be chosen to be Γ-invariant. This contradicts the Γ-indecomposability of V and we conclude that V must in fact be homocyclic.

(B) Theorem 13·2 Let the p'-group Γ be represented by automorphisms of the p-group G, let $H = [G, \Gamma]$ and let $C = C_G(\Gamma)$. Then (i) $G = HC$; (ii) $[H, \Gamma] = H$ and (iii) if $H \leq \varphi(G)$, then $H = 1$.

Here C is the subgroup of all $\xi \in G$ which are left invariant by every $\gamma \in \Gamma$. We can form the split extension $G\Gamma$ of G by Γ determined by the given representation of Γ. By 7·1 (iii), $H \lhd G\Gamma$.

Proof: (iii). Let $\Phi = \varphi(G)$. By 5·2 (vi), G/Φ is an elementary Abelian p-group. Let $|G : \Phi| = p^r$ and let $\Phi\xi_1, \cdots, \Phi\xi_r$ be a basis of G/Φ. By 9·1 (i), $G = \{\xi_1, \cdots, \xi_r\}$. Let A_1 be the group of all automorphisms $\alpha \in \operatorname{Aut} G$ such that $[G, \alpha] \leq \Phi$. Then $A_1 \lhd A = \operatorname{Aut} G$ and A/A_1 is isomorphic with a subgroup of $\operatorname{Aut} G/\Phi$, which has order $(p^r - 1)(p^r - p) \cdots (p^r - p^{r-1})$ by 8·81. If $\alpha \in A_1$, then $[\xi_i, \alpha] \in \Phi$ for each i; and since the ξ_i generate G, α is uniquely determined by the r elements $[\xi_i, \alpha]$. More generally, if $\xi_i \eta_i^{-1} \in \Phi$ for each i, then $G = \{\eta_1, \cdots, \eta_r\}$ and so no element $\alpha \neq 1$ in A_1 leaves any such ordered set $(\eta_1, \cdots, \eta_r)$ invariant. The total number of such ordered sets is $|\Phi|^r$. Hence $|A_1|$ divides $|\Phi|^r$ and thus A_1 is a p-group. If $H \leq \Phi$, the automorphisms of G which represent Γ all belong to A_1 and since Γ is by hypothesis a p'-group, it follows that $H = 1$ and $C = G$. Thus (iii) is proved.

The principle used here may be worth stating as

Lemma 13·21 Let G be any group and K any ~~normal~~ characteristic subgroup of G contained in $\varphi(G)$. Let $A = \operatorname{Aut} G$ and let A_1 consist of all $\alpha \in A$ such that $[G, \alpha] \leq K$, so that $A_1 \lhd A$ and A/A_1 is isomorphic with the subgroup of $\operatorname{Aut} G/K$ induced by elements of A. Then $|A_1|$ divides $|K|^r$ where r is the minimum number of generators of G.

Note that r is also the minimum number of generators of G/K and equally of $G/\varphi(G)$.

(i) Suppose first that $H \leq \zeta G$. Then the mapping $\xi \to [\xi, \gamma]$, $(\xi \in G)$, is homomorphic by 7.1 (i) for each $\gamma \in \Gamma$. Since $[G, \gamma] \leq H$, which is Abelian, the kernel of this homomorphism contains G', by 7.1(vii). This is true for each $\gamma \in \Gamma$. Hence $G' \leq C$. G/G' is a normal Abelian Sylow p-subgp of $G\Gamma/G'$ and so, by 12.5, it is the direct product of $\overline{C}/G'$ and $\overline{H}/G'$ where $\overline{H} = HG'$ and $\overline{C}$ consists of all $\xi \in G$ such that $[\xi, \Gamma] \leq G'$. Hence $C \leq \overline{C}$. If $\overline{H} = G'$, we have $H = 1$ by (iii) and $C = G$ and the result follows. If $\overline{H} > G'$, then $\overline{C} < G$ and we may assume by induction on $|G|$ that $\overline{C} = [\overline{C}, \Gamma]C$. But $[\overline{C}, \Gamma] \leq \overline{C} \cap \overline{H} = G' \leq C$ and so $\overline{C} = C$. Since $H \lhd G$, CH is a subgroup of G and we have $CHG' = \overline{C}\overline{H} = G$. Hence $CH = G$ should be G' by 9.1 (i) and 5.2 (vi).

If $H \not\leq \zeta G$, let $K = H \cap \zeta G$. Then $1 < K \lhd G\Gamma$. Let C_1 consist of all $\xi \in G$ such that $[\xi, \Gamma] \leq K$. Then $C \leq C_1$ and by induction we may assume that $HC_1 = G$. Since $H \not\leq \zeta G$, we have $C_1 < G$. By induction again we may assume that $[C_1, \Gamma]C = C_1$. This gives $HC = H[C_1, \Gamma]C = HC_1$ since $[C_1, \Gamma] \leq H$. Thus (i) is proved.

(ii) Let $H_1 = [H, \Gamma]$. By (i), $H \leq H_1C$ and so $G = H_1C$. ~~Every element of G has the form $\eta_1\xi$ with $\eta_1 \in H_1$ and $\xi \in C$. By (iii), Γ normalizes~~ Hence $G = CH_1$ and every element of G has the form $\xi\eta_1$ with $\xi \in C$, $\eta_1 \in H_1$. Therefore H is generated by the elements $[\xi\eta_1, \gamma] = [\eta_1, \gamma]$, with $\eta_1 \in H_1$ and $\gamma \in \Gamma$. But H and H_1 are normalized by Γ, so $[\eta_1, \gamma] \in H_1$ and $H_1 \leq H$. Hence $H_1 = H$.

(C) Lemma 13.3 Let G be a p-soluble group, let M be a minimal normal subgroup of G and suppose that $|M| = p^m$ with $m > 1$, but that every chief p-factor of G/M has order p. Then G is the split extension of M by a maximal subgroup H of index p^m in G.

Proof: If $K \lhd G$ and $K \cap M = 1$, then G/K satisfies the conditions prescribed for G. If H/K is a subgroup transversal to KM/K in G/K, then $H \cap M = 1$ and $HM = G$. By induction on $|G|$, we may therefore assume that M is the only minimal normal subgroup of G.

Let L/M be a chief factor of G, and suppose first that L/M is a p'-group. By 9.4, L has a single class of conjugate $S_{p'}$-subgroups H and these are intravariant in L. If $N = N_G(H)$, it follows that $NL = G$ by 10.8 (iii). Since $HM = L$, we have $NM = G$. Since M is Abelian and normal in G, $N \cap M$ is normal in $NM = G$. Since M is a minimal normal subgroup of G, either $N \cap M = 1$ or $M \leq N$. In the second case, $H \lhd L$ and, as a normal $S_{p'}$-subgroup of L, H is even characteristic in L. This would imply $H \lhd G$ contrary to the assumption that M is the only minimal normal subgroup of G. Hence $N \cap M = 1$ and the theorem follows.

Since G is p-soluble, L/M if not a p'-group must be a p-group and therefore, by the assumption about G, we have $|L : M| = p$. Then L is a p-group and $\mathfrak{z}L \cap M \neq 1$ by 5.2 (i). Since $\mathfrak{z}L \cap M \lhd G$ it follows that $M \leq \mathfrak{z}L$. But L/M is cyclic and hence $L = \mathfrak{z}L$ is Abelian by 7.2 (iii). Since M is elementary of order p^m, L must be elementary of order p^{m+1}; for the only alternative is for L to be of type $(l^{m-1}2)$ and since $m > 1$ this would imply $M = \Omega_1(L) > \mathfrak{V}_1(L) > 1$, $\mathfrak{V}_1(L) \lhd G$, contrary to the hypothesis that M is a minimal normal subgroup of G.

Now let $C = C_G(L)$. Then $C < G$. Let D/C be a chief factor of G.

Suppose first that D/C is a p-group. Then $|D:C| = p$ by hypothesis and $C_M(D) \neq 1$ by 5.1. Since $C_M(D) \lhd G$, it follows that $[M, D] = 1$. Let $D = \{C, \xi\}$ and $L = \{M, \eta\}$. Since $[L, C] = 1$, $[L, D]$ is generated by $\gamma = [\xi, \eta]$ and its conjugates in D. But $[L, D] \leq M$ by 5.1 and so $[\gamma, D] = 1$. Hence $[L, D] = \{\gamma\}$ is cyclic. Since $[L, D] \lhd G$, this contradicts the hypothesis that M is a minimal normal subgroup of G.

We conclude that D/C must be a p'-group Γ. This is represented by automorphisms of the elementary Abelian p-group L. By 13.1, we have L as the direct product $L_0 L_1 \cdots L_r$ of a certain number of minimal normal subgroups L_i of D, where we may assume that $M = L_1 L_2 \cdots L_r$, so that $|L_0| = p$. Joining together those L_i which are Γ-isomorphic to a given one, we obtain L as the direct product $W_0 W_1 \cdots W_s$, where each W_j is a Wedderburn component of L with respect to Γ. Let W_0 contain L_0. Then $W_1 W_2 \cdots W_s \leq M$. Since $D \lhd G$, the mapping $W_i \to W_i^x$ is a permutation of $W_0, \ldots, W_s$, as in theorem 8.9. Since $M \lhd G$, it follows that $W_0 \lhd G$ and since M is minimal normal, we must have $W_0 \cap M =$ and so $W_0 = L_0$. This contradicts the hypothesis that M is the only minimal normal subgroup of G. So this case also is impossible and we conclude that L/M has to be a p'-group.

This concludes the proof of 13.3.

<u>Theorem 13.4</u> Let M be a maximal subgroup of G.

(i) If $|G:M|$ is either a prime or the square of a prime for all M, then G is soluble.

(ii) If $|G:M|$ is a prime for all M, then G is supersoluble.

Note that (ii) is the converse of part of 12.9 (ii). It allows us to characterize supersoluble groups as those groups in which every maximal subgroup is of prime index. This result is due to B. Huppert.

Proof: (i). Let p be the largest prime divisor of $|G|$, let P be a Sylow p-subgroup of G. If $P \lhd G$, we may assume that G/P is soluble

by induction on $|G|$. Hence G is soluble, since P is a p-group and therefore certainly soluble. If $N = N_G(P) < G$, let M be a maximal subgroup of G containing N. Then $|G:M| = q$ or q^2 for some prime $q < p$, by hypothesis But $|G:M| \equiv 1 \bmod p$ by 5.43. Since $(p, q-1) = 1$, we must have $|G:M|$ and p divides $q+1$. Hence $p = 3$, $q = 2$ and G is soluble by 9.8, corollary.

(ii) By (i), G is soluble. Let $G = G_0 > G_1 > \cdots > G_m = 1$ be a chief series of G. If G is not supersoluble, let i be the least integer for which $|G_{i-1} : G_i|$ is not a prime. Then G_{i-1}/G_i is an elementary Abelian p group of order p^m, $m > 1$, for some prime p; and the group G/G_i satisfies the hypotheses of 13.3 with $G_{i-1}/G_i = M$. Hence there is a maximal subgroup H of G such that $H \cap G_{i-1} = G_i$ and $HG_{i-1} = G$. Then $|G:H| = p^m$, contrary to the assumption that all maximal subgroups of G are of prime index. We conclude that G is supersoluble.

(D) Theorem 13.5 If every maximal subgroup of G is nilpotent, then G is soluble.

This theorem is due to Otto Schmidt and was found later independently by Iwasawa.

Proof: Suppose there are two distinct maximal subgroups M_1 and M_2 of G such that $D = M_1 \cap M_2 \neq 1$. Choose M_1 and M_2 so that D is as large as possible, and let $N = N_G(D)$. By 6.8 (iii), $D < M_1 \cap N = N_{M_1}(D)$ and similarly $D < M_2 \cap N$. If $N < G$, let M be a maximal subgroup of G containing N. By the maximality of D, we should then have $M_1 = M = M_2$ contrary to $M_1 \neq M_2$. Hence $N = G$ and $D \lhd G$. By induction on $|G|$ we may assume that G/D is soluble. Since D is nilpotent, it follows that G is soluble.

We may now assume that $M_1 \cap M_2 = 1$ for every pair of maximal subgroups M_1 and M_2 of G. If $M_1 \lhd G$, we obtain the solubility of G by induction on $|G|$, since $M_1 = 1$ implies that G is cyclic of order a prime and in any case M_1 is supposed to be nilpotent. We may therefore suppose

that no maximal subgroup M_1 of G is normal in G. Let $|M_1| = m_1$ and $|G:M_1| = n_1$. Then M_1 has n_1 conjugates in G and together these contain exactly $1 + n_1(m_1-1)$ elements of G. This number is less than $|G| = n_1 m_1$ and so G must have a maximal subgroup M_2, of order m_2 and index n_2 in G, which is not conjugate to M_1 in G. Since M_2 and its conjugates contain besides the unit element exactly $n_2(m_2-1)$ further elements of G, we obtain $|G| = n_2 m_2 \geq 1 + n_1(m_1-1) + n_2(m_2-1)$ and so $n_2 - 1 \geq n_1(m_1-1) \geq n_1$. Similarly, $n_1 - 1 \geq n_2$, which is a contradiction. Thus 13.5 is proved

(E). Suppose that G is not nilpotent but that all proper subgroups of G are nilpotent. By 13.5, G is soluble. Hence G has a maximal normal subgroup M of index a prime p and so $G = \{M, \xi\}$ where ξ is of order p^r for some r and $\xi^p \in M$. Since M is nilpotent but not G, we have $M = \mathfrak{N}G$ the Fitting subgroup of G. For some $q \neq p$, the Sylow q-subgroup Q of M must contain an element η which does not commute with ξ; for otherwise G would be nilpotent. Then $G = \{\xi, \eta\}$ since $\{\xi, \eta\}$ is not nilpotent; and so $Q = \{\eta^G\}$ and M is the direct product of Q with $\{\xi^p\}$. Thus G is the split extension of Q by the cyclic p-group $\{\xi\}$. Moreover every proper subgroup Q_1 of Q which is normalized by ξ must be centralized by ξ; for otherwise $\{Q_1, \xi\} = G_1$ would be a proper subgroup of G but not nilpotent.

We consider a slightly more general situation in

Theorem 13.6 Let the q'-group Γ be represented by automorphisms of the q-group Q and suppose that there is an element $\gamma \in \Gamma$ which centralizes every proper Γ subgroup of Q which is normal in the split extension $Q\Gamma$ but which does not centralize Q. Then $Q' \leq \zeta Q$ and Q/Q' is a chief factor of $Q\Gamma$. Either Q is elementary; or Q is of class 2 with Q/Q' and Q' both elementary and $Q' = \zeta Q$.

Proof. Since $Q' \leq \varphi(Q)$ and γ has order prime to q and does not centralize Q, it follows from 13.21 that γ does not centralize Q/Q'.

Hence Q/Q' is Γ-indecomposable; for otherwise there would be a Γ-invariant subgroup Q_1 containing Q' and such that $[Q_1, \gamma] \neq Q'$, contrary to hypothesis. By 12.5, Q/Q' is the direct product of $C_{Q/Q'}(\gamma)$ with another group. Since γ does not centralize Q/Q', it follows that γ does not centralize $\Omega_1(Q/Q')$ either. But $\Omega_1(Q/Q') = Q_2/Q'$ with Q_2 characteristic in Q. Hence $Q = Q_2$ and Q/Q' is elementary. Since it is Γ-indecomposable, it is therefore a chief factor of $Q\Gamma$.

Let $\Gamma_0 = \{\gamma^\Gamma\}$. Then $\Gamma_0 \lhd \Gamma$; and Γ_0 centralizes Q' because γ does so. A $[Q, \Gamma_0] \lhd Q\Gamma$ and $[Q, \Gamma_0]$ is not contained in Q' since γ does not centralize Q/Q'. Since the latter is a chief factor of $Q\Gamma$, it follows that $Q'[Q, \Gamma_0] = Q$ and hence $[Q, \Gamma_0] = Q$ by 9.1.(i). Since $[Q', \Gamma_0] = 1$, both $[Q', Q, \Gamma_0]$ and $[\Gamma_0, Q', Q]$ are equal to 1. Hence $[Q, Q'] = [Q, \Gamma_0, Q'] =$ by 7.7 (ii). Thus $Q' \leq \mathfrak{z}Q$.

If Q is not elementary, we have $Q' \neq 1$ and so $Q' \leq \mathfrak{z}Q < Q$. But $\mathfrak{z}Q \lhd Q\Gamma$ and Q/Q' is a chief factor of $Q\Gamma$; so in this case $Q' = \mathfrak{z}Q$. Let ξ, η be in Q and let $\zeta = [\xi, \eta]$. Then $\zeta \in \mathfrak{z}Q$ and $\xi\eta^{-1}\xi\eta = \xi\zeta$ and so $\eta^{-q}\xi\eta^q = \xi\zeta^q$. But $\eta^q \in Q' = \mathfrak{z}Q$ and so η^q commutes with ξ. Hence $\zeta^q = 1$. The Abelian group Q' is generated by elements ζ of order q. Thus Q' is elementary and 13.6 is proved.

Lemma 13.52 Let Q be a q-group such that $Q' = \mathfrak{z}Q$ is of order q a prime. Then Q is the central product of a certain number r of non-Abelian groups of order q^3. For each prime q and each integer $r = 1, 2, \ldots$ there are exactly two non-isomorphic groups Q of this kind and Q/Q' is elementary of order q^{2r}.

Proof: Let ξ, η be in Q and let $[\xi, \eta] = \zeta$. By hypothesis $\zeta^q = 1$. As we have just seen, $\eta^q\xi\eta^q = \xi\zeta^q$ since $\zeta \in \mathfrak{z}Q$. Hence η^q commutes with ξ. This is true for all ξ, η in Q. Hence $\eta^q \in Q' = \mathfrak{z}Q$ and Q/Q' is elementary.

Let $|Q : Q'| = q^s$. Then $s > 1$, since $Q/\mathfrak{z}Q$ cannot be cyclic. Since $Q' \neq 1$, we can choose ξ_1, η_1 in Q such that $\zeta = [\xi_1, \eta_1] \neq 1$.

(F) Let Γ be any group, let X be a cyclic group of order p and let $G = X \wr \Gamma$. If $|\Gamma| = n$, the base group V of G is elementary Abelian of order p^n, with a basis x_α ($\alpha \in \Gamma$) such that $x_\alpha{}^\beta = x_{\alpha\beta}$ for all $\alpha, \beta \in \Gamma$. Thus Γ is represented faithfully by automorphisms of V and this is called the <u>regular representation of Γ mod p</u>.

Let $1 = V_0 < V_1 < \cdots < V_r = V$ be part of a chief series of V. Then Γ is represented, with kernel Γ_i say, by automorphisms of V_i/V_{i-1}. If $\Delta = \bigcap_{i=1}^{r} \Gamma_i$, we have $[V_i, \Delta] \leq V_{i-1}$ for all i and so Δ is a p-group by 7·9 (i).

A group Γ is called <u>monolithic</u> if it has only one minimal normal subgroup M. This implies $\Gamma \neq 1$.

<u>Theorem 13·7</u> (i) Let Γ be a monolithic group such that $O_p \Gamma = 1$. Then Γ has a faithful irreducible representation of mod p.

(ii) If $p_1, p_2, \cdots, p_n$ are primes such that $p_{i-1} \neq p_i$ $(i = 2, \cdots, n)$, then there exist groups G with one and only one chief series

$$G = G_0 > G_1 > \cdots > G_n = 1$$

and such that G_{i-1}/G_i is an elementary Abelian p_i-group for each $i = 1, \cdots, n$.

Proof: (i) Since $O_p \Gamma = 1$, we have $\Delta = 1$; and this implies that $\Gamma_i = 1$ for some i, since Γ is monolithic. Hence Γ is represented faithfully and irreducibly by automorphisms of V_i/V_{i-1}.

(ii) When $n = 1$, we can take G to be cyclic of order p_1. Let $n > 1$. By induction we may assume the existence of a group Γ with only one chief series $\Gamma = \Gamma_0 > \Gamma_1 > \cdots > \Gamma_{n-1} \neq 1$ and such that Γ_{i-1}/Γ_i is a p_i-group for $i = 1, \cdots, n-1$. Then Γ is monolithic. Its unique minimal normal subgroup Γ_{n-2} is a p_{n-1}-group. Since $p_{n-1} \neq p_n$, we have $O_{p_n} \Gamma = 1$. By (i), Γ has a faithful irreducible representation f by automorphisms of an elementary Abelian p_n-group G_{n-1}. Let $G = \langle \Gamma, G_{n-1}; f \rangle$ be the corresponding split extension. Since f is irreducible, G_{n-1} is a minimal normal subgroup of G; it is the only one by 6·9, since f is faithful. Hence G is monolithic. Since $G/G_{n-1} \cong \Gamma$, G has only one chief series, with terms $G_n = 1$, $G_{n-k} = G_{n-1}\Gamma_{n-k}$ $(k = 1, 2, \cdots, n)$ and

§ 14 Some Special p-Groups

(A) **Lemma 14.1** Let f be a representation of the group H by automorphisms of the group K and let $\overline{G} = \langle H, K ; f \rangle$. Let θ be an isomorphic mapping of a normal subgroup M of H into K such that for all $\mu \in M$, $\eta \in H$ and $\xi \in K$ we have

$$\mu^{\theta f(\eta)} = \mu^{\eta\theta} \quad \text{and} \quad \xi^{f(\mu)} = \xi^{\mu\theta}. \tag{1}$$

Then the set of all pairs (μ^{-1}, μ^θ) with $\mu \in M$ forms a normal subgroup $\overline{M}$ of $\overline{G}$ such that $\overline{H} \cap \overline{M} = \overline{K} \cap \overline{M} = 1$ and $\overline{M} \cong M$.

Here ~~we identify~~ $\overline{H}$ is the subgroup of G with the set of all pairs $(\eta, 1)$, $\eta \in H$; and similarly for $\overline{K}$.

Proof: Let μ_1, μ_2 be in M. Then $\mu_1^{\theta f(\mu_2^{-1})} \mu_2^\theta = \mu_1^{\mu_2^{-1}\theta} \mu_2^\theta = (\mu_2 \mu_1)^\theta$ and so $(\mu_1^{-1}, \mu_1^\theta)(\mu_2^{-1}, \mu_2^\theta) = (\mu_1^{-1}\mu_2^{-1}, \mu_1^{\theta f(\mu_2^{-1})} \mu_2^\theta) = (\mu_1^{-1}\mu_2^{-1}, (\mu_2\mu_1)^\theta) \in \overline{M}$. Thus $\overline{M}$ is a subgroup of $\overline{G}$. The transform of (μ^{-1}, μ^θ) by $(\eta, 1)$ is $(\eta^{-1}\mu^{-1}\eta, \mu^{\theta f(\eta)}) = ((\mu^\eta)^{-1}, \mu^{\eta\theta})$ which is in $\overline{M}$. The transform of (μ^{-1}, μ^θ) by $(1, \xi)$ is $(\mu^{-1}, \xi^{-f(\mu^{-1})} \mu^\theta \xi)$ ~~$= (\mu^{-1}, \mu^\theta)$~~, $= (\mu^{-1}, (\mu^\theta)^{\theta} \xi^{-1} (\mu^\theta)^{-1} \mu^\theta \xi) = (\mu^{-1}, \mu^\theta)$ which is also in $\overline{M}$. Thus $\overline{M} \lhd \overline{G} = HK$. It is clear that $H \cap \overline{M} = K \cap \overline{M} = 1$ since θ is an isomorphism. The mapping $(\mu^{-1}, \mu^\theta) \to \mu^{-1}$ is an isomorphism of $\overline{M}$ onto M. Thus 14.1 is proved.

Clearly, $G = \overline{G}/\overline{M} = H_1 K_1$, where $H_1 = \overline{M}\overline{H}/\overline{M} \cong H$ and $K_1 = \overline{M}\overline{K}/\overline{M} \cong K$. Moreover $K_1 \lhd G$ and $H_1 \cap K_1 = M_1 \cong M$.

Conversely, let $G = HK$ with $K \lhd G$ and let $M = H \cap K$. Let $f(\eta)$, $\eta \in H$, be the automorphism of K induced by transforming with η. Then f is a representation of K. Since $(\eta_1, \xi_1)(\eta_2, \xi_2) = \eta_3 \xi_3$ where $\eta_3 = \eta_1 \eta_2$ and $\xi_3 = \xi_1^{f(\eta_2)} \xi_2$ for all $\eta_i \in H$, $\xi_i \in K$, the mapping $(\eta, \xi) \to \eta\xi$ of $\overline{G} = \langle H, K ; f \rangle$ onto G is a homomorphism, with kernel $\overline{M}$ such that $\overline{H} \cap \overline{M} = \overline{K} \cap \overline{M} = 1$. Moreover $\overline{M}$ consists of all pairs (μ, μ^{-1}) with $\mu \in M$. If θ is the identity mapping of M considered as a subgroup of H onto itself considered as a subgroup of K, the relations $\mu^{\theta f(\eta)} = \mu^{\eta\theta}$ and $\xi^{f(\mu)} = \xi^{\mu\theta}$ hold for all $\xi \in K$,

$\eta \in H$ and $\mu \in M$. Hence $\overline{M}$ is one of the normal subgroups of $\overline{G}$ described in 14·1. Hence we have

Lemma 14·12. If $G = HK$ with $K \lhd G$, then $G \cong \overline{G}/\overline{M}$ where $\overline{G} = \langle H, K ; f \rangle$, f is the representation of H by the automorphisms of K induced by transforming in G and $\overline{M}$ consists of all pairs (μ, μ^{-1}) with $\mu \in M = H \cap K$.

The conditions (1) of 14·1 are therefore necessary and sufficient for the existence of a semi-normal product $G = HK$ obtained with a given representation f of H by automorphisms of K and a given identification θ of a subgroup M of H with a subgroup M^θ of K, and such that $M = H \cap K$.

The simplest particular case is that of cyclic extensions. Here we have

Lemma 14·13 Let α be an automorphism of the group K which leaves invariant a certain element ξ of K and suppose that α^n is the inner automorphism $t(\xi)$ of K. Then there is a group $G = \{K, \eta\}$ such that $\eta^n = \xi$, $\eta^{-1}\beta\eta = \beta^\alpha$ for all $\beta \in K$ and $|G : K| = n$.

If ξ is of order m, we take $H = \{\eta\}$ to be of order mn, $M = \{\eta^n\}$ and $(\eta^n)^\theta = \xi$. The conditions (1) of 14·1 are then fulfilled.

Since the composition factors of a soluble group are all cyclic of prime order, 14·13 gives by repeated application a method of constructing all soluble groups, at least in principle. In simple enough cases, this method is usable and we shall illustrate it by discussing some special types of p-groups.

(B) The exponent of a group G is the least integer $n > 0$ such that $\theta^n = 1$ for all $\theta \in G$. Obviously n divides $|G|$ and is the l.c.m. of the orders of the elements of G. A nilpotent group of exponent n actually has elements of order n.

Lemma 14·21 A group G of exponent 2 is Abelian.

For, $\xi = \xi^{-1}$ for all $\xi \in G$ and so $\eta\xi = (\eta\xi)^{-1} = \xi^{-1}\eta^{-1} = \xi\eta$ for all ξ and $\eta \in G$.

Theorem 14·2 (i) In a group G of exponent 3, every element commutes with all its conjugates in G, and so $\{\xi^G\}$ is Abelian for all $\xi \in G$.

(ii) If $\{\xi^G\}$ is Abelian for all $\xi \in G$, then G is nilpotent of class at most 3 and $\gamma_3 G$ is of exponent 3.

Proof (i). We have $(\xi\eta)^3 = 1$ for all ξ, η in G and so $\xi^{-1}\eta^{-1}\xi^{-1} = \eta\xi\eta$. Hence $[\eta, \xi, \xi] = \xi^{-1}\eta^{-1}\xi\eta \cdot \xi^{-1} \cdot \eta^{-1}\xi\eta\xi \cdot \xi = \xi^{-1}\eta^{-1}\xi\eta \cdot \eta\xi\eta \cdot \eta\xi \cdot \xi = \xi^{-1}(\eta^{-1}\xi)^3\xi$ since $\eta^2 = \eta^{-1}$ and so $[\eta, \xi, \xi] = 1$. Hence ξ commutes with $\xi^\eta = \xi[\xi, \eta] = \xi[\eta, \xi]^{-1}$ for all $\eta \in G$.

(ii) We now merely assume $[\eta, \xi, \xi] = 1$ for all ξ, η in G, so that every element of G commutes with all its conjugates in G. Then we have ① $1 = [\xi\xi^{-1}, \eta] = [\xi, \eta]^{\xi^{-1}}[\xi^{-1}, \eta]$ and so $[\xi^{-1}, \eta] = [\xi, \eta]^{-1}$ since ξ^{-1} commutes with $[\xi, \eta]$. Here and repeatedly we shall use 7·1 (i) and (ii). If ζ is a third element of G, we have $1 = [\xi, \eta\zeta, \eta\zeta] = [[\xi, \zeta][\xi, \eta]^\zeta, \eta\zeta]$ $= [\xi, \zeta, \eta\zeta]\,[[\xi, \eta]^\zeta, \eta\zeta]$ since $[\xi, \eta]^\zeta$ and $[\xi, \zeta]$ both lie in $X = \{\xi^G\}$ and therefore commute. $[\xi, \zeta, \eta\zeta] = [\xi, \zeta, \eta]$ since $[\xi, \zeta, \zeta] = 1$ and ζ commutes with the element $[\xi, \zeta, \eta] \in Z = \{\zeta^G\}$. Similarly η commutes with the element $[\xi, \eta]^\zeta \in Y = \{\eta^G\}$ and so $[[\xi, \eta]^\zeta, \eta\zeta] = [[\xi, \eta]^\zeta, \zeta] = [\xi, \eta, \zeta]$. Thus we obtain ② $[\xi, \zeta, \eta] = [\xi, \eta, \zeta]^{-1}$. Since $[\eta, \xi^{-1}] = [\xi^{-1}, \eta]^{-1} = [\xi, \eta]$ by ①, we have $[\xi, \eta^{-1}, \zeta]^\eta = [\xi, \eta^{-1}, \zeta] = [\eta, \xi, \zeta]$ and 7·7 (i) gives the relation ③ $[\eta, \xi, \zeta][\zeta, \eta, \xi][\xi, \zeta, \eta] = 1$.

① and ② together show that $[\xi, \zeta, \eta]$ changes into its inverse when any two of ξ, η, ζ are interchanged. Hence it is unaltered by a cyclic permutation of ξ, η, ζ and this gives ④ $[\xi, \zeta, \eta]^3 = 1$ from ③

Finally, if τ is yet another element of G, we obtain
$\theta = [\xi, \eta, \zeta, \tau] = [\zeta, \tau, [\xi, \eta]]$ by cyclic permutation, $= [\xi, \eta, [\zeta, \tau]]^{-1}$
But by ① and ②, θ changes to its inverse for any odd permutation of its four arguments. Hence $\theta = [\zeta, \tau, \xi, \eta] = [\xi, \eta, [\zeta, \tau]] = \theta^{-1}$. So we have $\theta^2 = 1$. By ④, $\theta^3 = 1$. Hence $\theta = 1$. This is true for all ξ, η, ζ, τ of G and so $\gamma_4 G = 1$ by 7·5(i). Thus G is nilpotent of class at most 3. By 7·5(i) again, the Abelian group $\gamma_3 G$ is generated by elements $[\xi, \eta, \zeta]$ of order 1 or 3, so $\gamma_3 G$ is of exponent 3.

Corollary 14·23 If $p \neq 3$, any p-group G in which $\{\xi^G\}$ is Abelian for all $\xi \in G$ is of class at most 2.

Note that in 14·2, the assumption that G is finite is irrelevant. It is clear that in any nilpotent group G of class 2, every element ξ commutes with all its conjugates. For $G' \leq \zeta G$ and $\{\xi, G'\} \lhd G$.

Lemma 14·24 Let G be a p-group of class 2 and let p be odd. Then the elements $\theta \in G$ such that $\theta^{p^n} = 1$ form a subgroup $\mathfrak{N}_n G$, just as in an Abelian p-group.

Proof: let $\xi, \eta \in G$ and let $\zeta = [\xi, \eta]$. Then $\zeta \in G' \leq \zeta G$ and so $\eta^{-\tau} \xi \eta^{\tau} = \xi \zeta^{\tau}$ for all $\tau = 1, 2, \ldots$ by induction on τ. Now in any group we have the identity

$$(\eta \xi)^{\tau} = \eta^{\tau} \xi^{\eta^{\tau-1}} \xi^{\eta^{\tau-2}} \cdots \xi^{\eta} \xi .$$

In our case, this gives $(\eta\xi)^{\tau} = \eta^{\tau} \xi^{\tau} \zeta^{\binom{\tau}{2}}$ since ξ commutes with ζ. Suppose that $\xi^{p^n} = \eta^{p^n} = 1$ and take $\tau = p^n$. Then $\zeta^{p^n} = [\xi, \eta^{p^n}] = 1$; and if $p \neq 2$, $\frac{1}{2} p^n (p^n - 1)$ is a multiple of p^n. Hence $(\eta\xi)^{p^n} = \eta^{p^n} \xi^{p^n} \zeta^{\frac{1}{2} p^n (p^n - 1)} = 1$.

As a corollary of this we have

Lemma 14·25 If p is odd, a p-group G with only one subgroup of order p must be cyclic.

(C) We shall now consider the structure of a non-Abelian p-group G which has a cyclic subgroup of index p. By 7·2 (iv), $|G| = p^n$ with $n > 2$.

Lemma 14·31 Let $C = \{\xi\}$ be a cyclic group of order p^n, $n \geq 2$.

(i) If $p = 2$, $n = 2$, then $A = \mathrm{Aut}\, C$ is of order 2 and is generated by the automorphism $\beta : \xi \to \xi^{-1}$.

(ii) If $p = 2$, $n > 2$, then A is an Abelian 2-group of type $(n-2, 1)$ with a basis α, β defined by

$$\alpha : \xi \to \xi^5 \quad \text{and} \quad \beta : \xi \to \xi^{-1}.$$

(iii) If p is odd, the Sylow p-subgroup of the Abelian group A is generated by the automorphism $\alpha : \xi \to \xi^{1+p}$ and has order p^{n-1}.

Proof: (i) is clear.

(ii) $5^{2^m} \equiv 1 \bmod 2^{m+2}$ but $\not\equiv 1 \bmod 2^{m+3}$. Hence α has order 2^{n-2}. Obviously $\beta \notin \{\alpha\}$. Hence $A = \{\alpha, \beta\}$ with basis α, β, since $|A| = \varphi(2^n) = 2^{n-1}$.

(iii) Here $|A| = \varphi(p^n) = p^{n-1}(p-1)$ and $(1+p)^{p^m} \equiv 1 \bmod p^{m+1}$ but $\not\equiv 1 \bmod p^{m+2}$. Hence α generates the Sylow p-subgroup of A.

Corollary 14·32 If $C = \{\xi\}$ has order 2^n, $n > 2$, then C has exactly three involutory automorphisms viz.

$$\alpha^{2^{n-3}} : \xi \to \xi^{1+2^{n-1}} \; ; \quad \beta : \xi \to \xi^{-1} \; ; \text{ and } \alpha\beta : \xi \to \xi^{-1+2^{n-1}}.$$

We can now prove

Theorem 14·3 Let G be a group of order p^n with a cyclic subgroup $H = \{\xi\}$ of index p. Suppose that $n > 2$ and that G is not Abelian.

(i) If p is odd, G is determined to within isomorphism and $G = \{H, \eta\}$ where $\eta^p = 1$ and $\eta^{-1}\xi\eta = \xi^{1+p^{n-2}}$. G is of class 2 and $\Omega_1 G = \{\xi^{p^{n-2}}, \eta\}$ is of order p^2.

(ii) If $p = 2$ and $n = 3$, there are to within isomorphism two distinct types of group $G = \{H, \eta\}$: the octic group O is determined by the equations $\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{-1}$; the quaternion group Q by $\eta^2 = \xi^2$, $\eta^{-1}\xi\eta = \xi^{-1}$. H is a characteristic subgroup of O and the remaining two subgroups of order 4 in O are elementary. In Q, every element $\notin$ not in $Q' = \zeta Q$ has

orders 4.

(iii) $\mathrm{Aut}\, O \cong O$; $\mathrm{Aut}\, Q \cong \Sigma_4$. The automorphisms

$$\alpha : \xi \to \eta \to \xi\eta \quad \text{and} \quad \beta : \xi \leftrightarrow \eta^{-1}$$

of Q generate a group isomorphic with Σ_3. The split extension $\{Q, \alpha, \beta\}$ of order 48 is called the binary-octahedral group ; $\{Q, \alpha\}$ of order 24 is the binary-tetrahedral group.

(iv) If $p = 2$ and $n > 3$, then G is of class either 2 or $n-1$. In the former case, $G = \{\xi, \eta\}$ is determined to within isomorphism by the relations $\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{1+2^{n-2}}$. G has exactly three involutions, forming with 1 the characteristic subgroup $\{\xi^{2^{n-2}}, \eta\}$.

(v) If $p = 2$, $n > 3$ and G has class $n-1$, then there are three distinct types of group G to within isomorphism, which will be denoted by O_{2^n}, P_{2^n} and Q_{2^n}. We have $G = \{\xi, \eta\}$ where

$\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{-1}$ in the dihedral group O_{2^n}

$\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{-1+2^{n-2}}$ in the intermediate group P_{2^n}

$\eta^2 = \xi^{2^{n-1}}$, $\eta^{-1}\xi\eta = \xi^{-1}$ in the generalized quaternion group Q_{2^n}

Note that $O = O_8$, $Q = Q_8$. Besides the cyclic subgroup $H = \{\xi\}$, G has two other subgroups of index 2. In O_{2^n}, these are both of type $O_{2^{n-1}}$. In P_{2^n}, one is of type $O_{2^{n-1}}$ and the other of type $Q_{2^{n-1}}$. In Q_{2^n}, both are of type $Q_{2^{n-1}}$. G has centre $\{\xi^{2^{n-2}}\} = Z$ of order 2 and in all three groups, G/Z is of type $O_{2^{n-1}}$.

Note that $H \lhd G$ by 5.2(v). Since $G' \neq 1$, the automizer $A_0 = A_G(H)$ is of order p.

Proof: (i) By 14.31 (iii), there is only one choice for A_0 viz. $A_0 = \{\alpha^{p^{n-3}}\}$. Here $\gamma = \alpha^{p^{n-3}}$ is $\xi \to \xi^{1+p^{n-2}} = \xi\zeta$. So $zG = \{\xi^p\}$ is of index p^2 and $G' = \{\zeta\}$ is of order p and G is of class 2. Also $G = \{\xi, \eta_1\}$ where $\eta_1^{-1}\xi\eta_1 = \xi\zeta$. Then $\eta_1^p = \xi^{rp}$ for some r, since η_1^p commutes with η_1. Since $[\xi^{-r}, \eta_1] = \zeta^{-r}$ and $\zeta^p = 1$, we have $(\eta_1\xi^{-r})^p = 1$ because p is odd. Then $G = \{\xi, \eta\}$ with $\eta^{-1}\xi\eta = \xi^{1+p^{n-2}}$, $\eta^p = 1$. $K = \{\eta, \zeta\}$ is normal in G and elementary; $G = \{K, \xi\}$ so G/K is cyclic. No element outside of K can have order p, so $K = \Omega_1 G$.

(ii) By 14.31 (i), the choice of A_1 is again unique and $G = \{\xi, \eta\}$ with $\eta^{-1}\xi\eta = \xi^{-1}$. Here $G' = zG = \{\xi^2\}$ is of order 2 and there are only two possibilities for η^2 viz. $\eta^2 = 1$ giving O; or $\eta^2 = \xi^2$ giving Q. Since $(\eta\xi^r)^2 = \eta^2 \cdot \eta^{-1}\xi^r\eta \cdot \xi^r = \eta^2$, and $\eta\xi^r$ transforms ξ into its inverse for all choices of r, these two cases are distinct. In O, $H = \{\xi\}$ as the only cyclic subgroup of order 4 is characteristic; $|\mathrm{Aut}\, O| = 8$ because each of the mappings $\xi \to \xi^{\pm 1}$, $\eta \to \eta\xi^r$ $(r = 0, 1, 2, 3)$ defines an automorphism of O. If η^* is $\xi \to \xi^{-1}$, $\eta \to \eta$ and ξ^* is $\xi \to \xi$, $\eta \to \eta\xi$, then $\mathrm{Aut}\, O = \{\xi^*, \eta^*\}$ where ξ^* is of order 4, η^* of order 2 and η^* transforms ξ^* into its inverse. Thus $\mathrm{Aut}\, O \cong O$.

(iii) In the case of Q, all three subgroups of index 2 are cyclic. Hence if ξ_1, η_1 are any two non-commuting elements of Q, we have $Q = \{\xi_1, \eta_1\}$ and $\xi \to \xi_1$, $\eta \to \eta_1$ is an automorphism. Hence $|\mathrm{Aut}\, Q| = (8-2)(8-4) = 24$. If α is $\xi \to \eta \to \xi\eta$ and β is $\xi \leftrightarrow \eta^{-1}$, then $\alpha^3 = \beta^2 = 1$ and $\beta^{-1}\alpha\beta = \alpha^{-1}$ so $S = \{\alpha, \beta\} \cong \Sigma_3$. S permutes the three subgroups of index 2 in Q faithfully. These subgroups are normal in Q and so $\mathrm{Aut}\, Q = ST$, where $S \cap T = 1$ and T is the group of inner automorphisms of Q. $T \cong Q/Q'$ is elementary of order 4, so $|\mathrm{Aut}\, T| = 6$. But $C_S(T) = 1$. Hence $\mathrm{Aut}\, Q$ is isomorphic with the holomorph of T. The same applies to Σ_4. So $\mathrm{Aut}\, Q \cong \Sigma_4$.

(iv). Here we have three possible choices for A_0 by 14.32, and $G = \{\xi, \eta\}$ where $\eta^{-1}\xi\eta$ is either $\xi^{1+2^{n-2}}$, ξ^{-1} or $\xi^{-1+2^{n-2}}$. Let $\zeta = \xi^{2^{n-2}}$. In the first case, as in (i) for p odd, we have $G' = \{\zeta\} \leq \mathfrak{z}G = \{\xi^2\}$ and G is of class 2, and again the maximal subgroups of G are all Abelian. If $\{\eta, \xi^2\}$ is cyclic, we may suppose $\eta^2 = \xi^2$ and obtain $(\eta\xi^{-1})^2 = 1$. If $\{\eta, \xi^2\}$ is not cyclic, it is of type $(n-2, 1)$. In any case we may choose $\eta = 1$. Thus G is determined to within isomorphism; and in fact just two of the three subgroups of index 2 are cyclic. The third is a characteristic Abelian subgroup of type $(n-2, 1)$. Hence $\Omega_1 L$ contains all the involutions of G and is an elementary group of order 4, characteristic in G.

(v) In the remaining two cases, η transforms ξ^2 into its inverse and $\mathfrak{z}G = \{\zeta\}$ is of order 2. $[\eta, \xi] = \xi^2$ or $\xi^2\zeta$ and successive commutations with η give ξ^{-4}, ξ^8, ξ^{-16}, ... Hence G is of class $n-1$ and $\mathfrak{z}_{k+1}G = \{\xi^{2^k}\}$. For η^2 only two values are available, 1 and ζ. However, when $\eta^{-1}\xi\eta = \xi^{-1}\zeta$ we have $(\eta\xi)^2 = \eta^2\zeta$ and the two choices for η^2 lead to the same group P_{2^n}, of intermediate type. Taking $\eta^2 = 1$, $\{\xi^2, \eta\}$ is then of type $O_{2^{n-1}}$ and $\{\xi^2, \eta\xi\}$ of type $Q_{2^{n-1}}$. When $\eta^{-1}\xi\eta = \xi^{-1}$, we have $(\eta\xi^r)^2 = \eta^2$ for all r. When $\eta^2 = 1$, we have the group O_{2^n} in which every element outside $\{\xi\}$ is of order 2. When $\eta^2 = \zeta$, we have Q_{2^n} in which every element outside $\{\xi\}$ is of order 4. The remaining statements of (v) are clear.

Corollary 14.33 If the p-group G has no elementary subgroups of order p^3, then either G is cyclic, or else $p = 2$ and $G = Q_{2^n}$ is the generalized quaternion for some $n \geq 3$. (Including the case $Q = Q_8$, $n = 3$, the ordinary quaternion group.)

Proof: Suppose G is not cyclic. Then it contains a non-cyclic subgroup G_1 with a cyclic subgroup of index p. G_1 cannot be Abelian, for then $\Omega_1 G_1$ would be elementary of order p^2. By 14.3 (i), it follows that $p = 2$. By 14.3 (ii), (iv), (v), G_1 must be of type Q_{2^n} for some n. By induction on n, we may assume $|G : G_1| = 2$. We may assume that

$G_1 = \{\xi, \eta\}$ with $\{\xi\}$ of order 2^{n-1} and normal in $G = \{G_1, \tau\}$; for $\{\xi\}$ char G_1 if $n > 3$ and if $n = 3$, G_1 has three cyclic subgroups of order 4. In Aut $\{\xi\}$, the automorphism $\xi \to \xi^{-1}$ induced by η is not a square. Hence $\tau^2 \in \{\xi\}$, and $G/\{\xi\}$ is elementary of order 4. Since the automorphism $\xi \to \xi^{1+2^{n-2}}$ cannot be induced in G, 14.32 shows that G has an Abelian subgroup H of index 2 viz. $H = C_G(\xi)$. Then H must be cyclic and so G is of type $Q_{2^{n+1}}$

(D). Theorem 14.34 Let G be a group of order 2^n, $n > 3$. Then the following conditions are equivalent.

(i) $|G : G'| = 4$.

(ii) G is of class $n-1$.

(iii) G is one of the groups O_{2^n}, P_{2^n}, Q_{2^n}.

Proof: (ii) $\Rightarrow$ (i) is clear. For a nilpotent group G with cyclic G/G' must itself be cyclic, by 9.1 (i) and 6.8 (v). [This should have been made explicit in § 9 (A) somewhere]. Hence $|G : G'| \geq 4$. But $|G : G'| > 4$ implies $\gamma_{n-1} G = 1$, so that the class of G would be less than $n-1$.

(i) $\Rightarrow$ (iii). By 14.21 and 14.3 (ii), O and Q are the only non-Abelian groups of order 8. Let $Z \lhd G$, $|Z| = 2$, $Z \leq G'$. Such a subgroup Z exists by 5.2 (i), and by induction we may assume that G/Z has a cyclic subgroup H/Z of index 2. Let $Z = \{\zeta\}$ and $H = \{\xi, \zeta\}$. If $H = \{\xi\}$, the result follows from 14.3 (iv) and (v). If H is not cyclic, it is Abelian of type $(n-2, 1)$ and if $\eta = \xi^{2^{n-3}}$, then $Y = \{\eta\}$ is a characteristic subgroup of H. So $Y \lhd G$. Also $Y \leq G'$ since G/G' is elementary. By induction, G/Y also has a cyclic subgroup L/Y of index 2. But H/Y is Abelian of type $(n-3, 1)$. Hence $H \neq L$ and $G = HL$ and $H \cap L = \zeta G$ is of index 4. Hence G is of class 2 and $G' = \{[\alpha, \beta]\}$ where $G = \{\alpha, \beta\}$. Here $\gamma = [\alpha, \beta]$ is of order 2 since $\alpha^2 \in \zeta G$. Then $|G'| = 2$, contradicting $n > 3$.

(iii) $\Rightarrow$ (ii) is contained in 14.3 (iv), (v).

(E) We consider now the non-Abelian groups of order p^3.
If $p=2$, then 14·21 and 14·3 (ii) show that the octic and quaternion groups are the only possible types. For odd p there are also exactly two distinct types of groups.

For let $|G| = p^3$, $G' \neq 1$, p odd. If G has an element ξ of order p^2, then $G = \{\xi, \eta\}$ with $\eta^p = 1$, $\eta^{-1}\xi\eta = \xi^{1+p}$ by 14·3 (i). On the other hand, if G is of exponent p, then $G = \{\xi, \eta\}$ with $\xi^p = \eta^p = \zeta^p = 1$ and $\zeta = [\xi, \eta]$. Here $\{\zeta\} = {}_1G = G'$, and G is the split extension of the elementary group $\{\xi, \zeta\}$ by $\{\eta\}$, with $\eta^{-1}\xi\eta = \xi\zeta$ and of course $\eta^{-1}\zeta\eta = \zeta$. We shall denote these two groups by

$$P^*_{p^3} \quad \text{and} \quad P_{p^3},$$

respectively. We state

Lemma 14·35 For given p, there are exactly two types of non-Abelian groups G of order p^3. For both of them, $G' = {}_1G$ is of order p and G/G' is elementary. When $p=2$, they are the octic and quaternion groups. When p is odd, they are the groups $P^*_{p^3} = P^*$ and $P_{p^3} = P$. In P, $p+1$ subgroups of index p are all elementary, while in P^* there is a characteristic elementary subgroup $\Omega_1 P$ of order p^2 and the remaining p subgroups of index p are all cyclic.

It is easy to see that

$$|\mathrm{Aut}\, P| = (p^3-p)(p^3-p^2) \quad \text{and} \quad |\mathrm{Aut}\, P^*| = p(p^3-p^2).$$

(F) To form a central product of two groups H and K, we have to establish an isomorphism identifying a subgroup Z of the centre of H with a subgroup of the centre of K. If $G = HK$ is the central product determined in this way, then $|G| = |H|\cdot|K|/|Z|$. The choice $Z = 1$ is always possible and then G is simply the direct product of H and K. However in speaking of a central product it will always be tacitly assumed that the amalgamated subgroup Z is $\neq 1$. If ${}_1H$ and ${}_1K$ are of order p a prime, this leaves only one possible choice $Z = {}_1H = {}_1K$. But $|\mathrm{Aut}\, Z| = p-1$ so that there are $p-1$ possible choices for the identifying

isomorphism
~~automorphism~~). Nevertheless, if ~~the~~ the automizer of $Z = \zeta H$ in Aut H is the full group Aut Z, then the central product $G = HZ$ will be determined to within isomorphism. For by definition $G = \overline{G}/Z_\theta$, where $\overline{G} = H \times K$ is the Cartesian product and Z_θ consists of all pairs (ζ, ζ^θ) with $\zeta \in Z$, and where θ is an isomorphism of $Z = \zeta H$ onto ζK. Under the assumption mentioned, the $p-1$ subgroups Z_θ of $\overline{G}$ are all conjugate under Aut $\overline{G}$.

When H is one of the non-Abelian groups of order p^3, then this assumption is in fact correct, as is easy to see. Hence there is no ambiguity in the definition of the central product of any number of such groups.

Theorem 14.4 (i) Let G be a p-group such that $G' = \zeta G$ is of order p. Then $|G| = p^{2r+1}$ for some $r = 1, 2, \cdots$; G/G' is elementary; and G is expressible (in many ways if $r > 1$) as the central product $G_1 G_2 \cdots G_r$ of r non-Abelian groups of order p^3.

(ii) When $p = 2$, we have the central product isomorphisms

$$Q^r \cong O^2 Q^{r-2} \cong O^4 Q^{r-4} \cong \cdots$$

and $$O Q^{r-1} \cong O^3 Q^{r-3} \cong \cdots$$

but Q^r and $O Q^{r-1}$ are not isomorphic.

(iii) When p is odd, we have the central product isomorphisms

$$P^* P^{r-1} \cong (P^*)^2 P^{r-2} \cong \cdots \cong (P^*)^r$$

but $P^* P^{r-1}$ and P^r are not isomorphic. Here $P = P_{p,2}$ and $P^* = P^*_{p^2}$.

Proof: From 7.1 (i), and $G' = \zeta G$ of order p, it follows that G/G' is elementary viz. $\xi^p \in \zeta G$ for all $\xi \in G$. In fact, in a group of class 2, the mapping $\xi \to [\xi, \alpha]$ is homomorphic for any fixed α.

Since G is not Abelian, we can choose ξ_1, η_1 so that $[\xi_1, \eta_1] \neq 1$. Then $G_1 = \{\xi_1, \eta_1\}$ is non-Abelian of order p^3. Let $\overline{G}_1 = C_G(G_1)$. Then $\overline{G}_1 = X_1 \cap Y_1$ where $X_1 = C_G(\xi_1)$ and $Y_1 = C_G(\eta_1)$. But ξ_1 and η_1 have each exactly p conjugates in G. Hence $|G : X_1| = |G : Y_1| = p$. Since ξ_1 and η_1 do not commute, $X_1 \neq Y_1$ and so $|G : \overline{G}_1| = p^2$. Also $G_1 \cap \overline{G}_1 = \zeta G_1 = G'$ and so the elementary group G/G' is the direct product of G_1/G' and $\overline{G}_1/G'$. Hence $G = G_1 \overline{G}_1$ is a central product of G_1 and $\overline{G}_1$. Since $\zeta G = G'$, we

have $z\overline{G}_1 = G'$ also. Hence $z\overline{G}_1 = \overline{G}_1'$ is of order p and (i) follows by induction on $|G|$.

(ii) It will be sufficient to prove $Q^2 \cong O^2$. Let $G = Q^2$. Then $G = \{\xi_1, \eta_1, \xi_2, \eta_2\}$ and $G' = \{S\}$, where $S^2 = 1$ and $\xi_i^2 = \eta_i^2 = [\xi_i, \eta_i] = S$ $(i = 1, 2)$, while $[\xi_1, \xi_2] = [\xi_1, \eta_2] = [\xi_2, \eta_1] = [\eta_1, \eta_2] = 1$. Here $G = G_1 G_2$ where $G_1 = \{\xi_1, \eta_1\}$ and $G_2 = \{\xi_2, \eta_2\}$ are two quaternion groups and $[G_1, G_2] = 1$. Let $G_1^* = \{\xi_1, \eta_1\eta_2\}$ and $G_2^* = \{\xi_1\xi_2, \eta_2\}$. Then $G = G_1^* G_2^*$ and $[G_1^*, G_2^*] = 1$ and here G_1^*, G_2^* are octic groups.

The group Q^2 contains 6 cyclic subgroups of order 4, three in G_1 and three in G_2, while OQ contains 10. More generally, Q^r contains $3r + 3^3\binom{r}{3} + 3^5\binom{r}{5} + \cdots = \frac{1}{2}\{(1+3)^r - (1-3)^r\} = 2^{r-1}\{2^r - (-1)^r\}$ cyclic subgroups of order 4; while OQ^{r-1} contains $2^{2r-2} + 2^{r-1}\{2^{r-1} + (-1)^r\} = 2^{r-1}\{2^r + (-1)^r\}$ cyclic subgroups of order 4. So Q^r and OQ^{r-1} cannot be isomorphic.

(iii) Let p be odd. If G is of exponent p, then all the central factors G_i must be of type $P = P_{p^3}$ and so $G = P^r$. It is sufficient to prove $(P^*)^2 \cong P^*P$. Let $G = G_1 G_2$ where $G_i = \{\xi_i, \eta_i\}$ and $[G_1, G_2] = 1$ and $\xi_i^p = [\xi_i, \eta_i]$ generates G_i', while $\eta_i^p = 1$, $i = 1, 2$. So G is of type $(P^*)^2$. We may assume that $\xi_1^p = \xi_2^{-p}$, so that $\xi_1\xi_2$ is of order p. Then $G_1^* = \{\xi_1\xi_2, \eta_2\}$ is of type I and if G_2^* is its centralizer, G is the central product $G_1^* G_2^*$. Here G_2^* is necessarily of type P^*, for otherwise G would be of exponent p, by 14.24.

If $G = G_1 G_2 \cdots G_r$ is of type P^*P^{r-1} with $G_2, \ldots, G_r$ of type P and $G_1 = \{\xi_1, \eta_1\}$ of type P^*, where $\eta_1^p = 1$, then $\Omega_1 G = \{\eta_1, G_2, \ldots, G_r\}$ is of index p. It is the direct product of $\{\eta_1\}$ with the group $G_2 \cdots G_r$ of type P^{r-1}.

Lemma 14.41 If G is a p-group such that $G' = zG$ is of order p, then every automorphism of G which transforms G/G' identically is an inner automorphism.

Proof: Let $|G : G'| = p^{2r}$. Since $|G'| = p$, the number of automorphisms of G transforming G/G' identically is at most p^{2r}. This is also equal to $|G : zG|$, the number of inner automorphisms of G and the latter all

If $C = H$, it is an easy consequence of Theorem 14.3 that $p = 2$. Then Theorem 14.3 implies that G is one of O_{2^n}, P_{2^n}, Q_{2^n}.

Suppose $C \supset H$ and p is odd. Since G/C is cyclic, Theorem 14.3 implies that $C = G$. Let $G_1 = \Omega_1(G).H$. By Lemma 14.41, $G = G_1 C(G_1)$ and so $G = G_1$. By Lemma 14.4, we have $G = P^r H$, and we are done.

Finally, suppose $C \supset H$ and $p = 2$. If $|H| = 2$, the theorem follows from Theorem 14.1, so suppose $|H| > 2$. Since C' is of order 2, it follows that $\Omega_1(C) = O_8^s Q_8^{s'} Z_1$, where $Z_1 = \Omega_2(H)$. Thus, C is the central product of $O_8^s Q_8^{s'}$ and H. If $C = G$, the proof is complete. Otherwise, we get $G = \Omega_1(C).C(\Omega_1(C))$ by Lemma 14.41. Furthermore, H is a maximal normal abelian subgroup of $C(\Omega_1(C))$. It follows that $C(\Omega_1(C))$ is one of P_{2^k}, Q_{2^k}, O_{2^k}. The various isomorphisms follow easily from Theorem 14.4.

(G) Let H be a p-group with ζH of order p and let Z be cyclic of order p^m, $Z = \{\zeta\}$. Then the central product HZ is defined to within isomorphism, because the identified subgroup can only be $Z_1 = \Omega_1 \zeta H$ with $Z_1 = \{\zeta^{p^{m-1}}\}$ and the automizer of Z_1 in $\mathrm{Aut}\, Z$ is $\mathrm{Aut}\, Z_1$.

Theorem 14.5 Let G be a non-Abelian p-group such that every characteristic Abelian subgroup of G is cyclic and let $Z = \{\zeta\} = \zeta G$ be of order p^m. Then

(i) for odd p, G is the central product ZP^r for some $r = 1, 2, \ldots$ where $P = P_{p3}$ and the factor Z may be suppressed if $m = 1$. $|G| = p^{m+2r}$.

(ii) If $p = 2$ and $m = 1$, G is a central product of one of the forms Q^r, DQ^{r-1} $(r > 0)$ or $D_{2^k} Q^r$, $P_{2^k} Q^r$, $Q_{2^k} Q^r$ $(k > 3, r \geq 0)$ and no two of these are isomorphic. We have the central product isomorphisms

$$D_{2^k} Q^r \cong Q_{2^k} DQ^{r-1} \cong D_{2^k} D^2 Q^{r-2} \cong Q_{2^k} D^3 Q^{r-3} \cong \ldots$$

$$P_{2^k} Q^r \cong P_{2^k} DQ^{r-1} \cong P_{2^k} D^2 Q^{r-2} \cong \ldots$$

$$Q_{2^k} Q^r \cong D_{2^k} DQ^{r-1} \cong Q_{2^k} D^2 Q^{r-2} \cong D_{2^k} D^3 Q^{r-3} \cong \ldots .$$

(iii) If $p = 2$ and $m > 1$, G is the central product ZQ^r for some $r > 0$ and we have the central product isomorphisms $ZQ^r \cong ZDQ^{r-1} \cong ZD^2 Q^{r-2} \cong \ldots$

We need first

Lemma 14.51 Let G be a p-group such that $\zeta G'$ is cyclic. Then G' is cyclic.

Proof: Let $Z = \zeta G'$. Since $Z \lhd G$, $Z \leq G'$, we can choose a normal cyclic subgroup H of G which is maximal subject to $Z \leq H \leq G'$. If G' is not cyclic, then $H < G'$ and by 5.2 (i), there is a normal subgroup K of G such that $H < K \leq G'$ and $|K : H| = p$. Then K is not cyclic. If K is Abelian, it is of type $(m, 1)$ where $|H| = p^m$, and $\Omega_1 K$ is of order p^2. If K is not Abelian, $\Omega_1 K$ is still of order p^2 for odd p, by 14.3 (i); and also for $p = 2$ provided K is of class 2, by 14.3 (iv). The only alternative is for K to be one of the groups $D_{2^{m+1}}$, $P_{2^{m+1}}$, $Q_{2^{m+1}}$ by 14.3 (iv) and (v). But K contains a subgroup L of order p^2 and normal in G. Hence $L \leq \zeta^2 G$ and so $[L, G'] = 1$ by 7.8 (ii). Hence $L \leq \zeta K$. But the

groups O_{2m+1}, ... have centre of order 2, so K cannot be one of these. We conclude that K has a characteristic subgroup $M = \Omega_1 K$ of order p^2. Then $M \lhd G$ and so, as we have just seen, $[M, G'] = 1$. This contradicts the assumption that $\mathfrak{z} G'$ is cyclic.

Proof of 14.5. Since $\mathfrak{z} G'$ is a characteristic Abelian subgroup of G, it is cyclic, by hypothesis. Hence G' is cyclic by 14.51, and ZG' is a characteristic Abelian subgroup of G. So ZG' is cyclic too. Let H be a maximal characteristic cyclic subgroup of G containing ZG'. Then $H < G$, and if $C = C_G(H)$, then $\mathfrak{z} C$ is a characteristic Abelian subgroup of G containing H; hence $\mathfrak{z} C$ is cyclic, and so $\mathfrak{z} C = H$. Also $C' \leq G' \leq H = \mathfrak{z} C$. If $C > H$, then C is of class 2 and $[\xi^r, \eta^s] = [\xi, \eta]^{rs}$ for all ξ, η in C, by 7.1 (i), (ii). Let the Abelian group C/H be of type $(\tau_1, \tau_2, \dots)$, where $\tau_1 \geq \tau_2 \geq \cdots$, and let $H\xi_1, H\xi_2, \dots$ be a basis of C/H. Then we have $[\xi_1^{p^{\tau_2}}, \xi_i] = [\xi_1, \xi_i^{p^{\tau_2}}] = 1$ for $i = 2, 3, \dots$ and hence $\xi_1^{p^{\tau_2}} \in H = \mathfrak{z} C$. Hence $\tau_1 = \tau_2$. If $\tau_1 > 1$, we have $[\xi_i^{p^{\tau_1 - 1}}, \xi_j^{p^{\tau_1 - 1}}] = [\xi_i^{p^{2\tau_1 - 2}}, \xi_j] = 1$ for all i, j. If $L/H = \mho_{\tau_1 - 1}(C/H)$, it would follow that L char G, $L' = 1$, $L > H$, hence L cyclic, contrary to the choice of H. Hence $\tau_1 = 1$ and C/H is elementary, and so C' is of order p.