

Math 220A: Modern Algebra

Simon Rubinstein-Salzedo

January 31, 2004

0.1 Introduction

Professor: Adebisi Agboola.

Office Hours: Tuesday: 11:15-12:30, Wednesday: 11:15-12:30, Thursday: 11:15-12:30.

Textbooks: *Abstract Algebra* by Dummit and Foote and *Algebra* by Lang.

Chapter 1

Groups: Basic Concepts

Definition 1.1 A **group** (G, m) consists of a set G and a function $m : G \times G \rightarrow G$ such that

1. $\forall g_1, g_2 \in G, m(g_1, m(g_2, g_3)) = m(m(g_1, g_2), g_3)$. Let us now write g_1g_2 for $m(g_1, g_2)$. Thus $g_1(g_2g_3) = (g_1g_2)g_3$.
2. $\exists e \in G$ such that $\forall g \in G, ge = eg = g$. e is the identity or unit element.
3. $\forall g \in G, \exists g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$. g^{-1} is the inverse of g .

Proposition 1.2 If G is a group, the unit element is unique, and each $g \in G$ has a unique inverse.

Proof For the first part, let e and e' be unit elements. Then $e = ee' = e'$. For the second part, suppose that g^{-1} and \bar{g} are inverses of g . $g^{-1} = g^{-1}(g\bar{g}) = (g^{-1}g)\bar{g} = \bar{g}$.

Definition 1.3 A group G for which $g_1g_2 = g_2g_1 \forall g_1, g_2 \in G$ is called **abelian** or **commutative**. If G is abelian, we usually write $g_1 + g_2$ instead of g_1g_2 . Also we write $-g$ for g^{-1} and 0 for the unit element.

Example

1. $(\mathbb{Z}, +)$.
2. $(\mathbb{R} - \{0\}, \times)$.
3. $(\mathbb{Z}_n, +)$ if $n \geq 2$.
4. $(\mathbb{Z} - \{0\}, \times)$ is **not** a group since not all elements have inverses.

1.1 Permutations

Definition 1.4 Let X be any set. A **permutation** of X is a bijection of X with itself. The set of all permutations of X is denoted by S_X . Any permutation has an inverse, again a permutation. The product of two permutations (obtained by applying them in succession) is again a permutation. S_X forms a group with unit element equal to the identity permutation of X . Write S_n for S_X if $X = \{1, 2, \dots, n\}$.

Exercise S_n is nonabelian if $n \geq 3$.

Definition 1.5 An element $f \in S_n$ is called a **cycle** if \exists distinct integers $i_1, i_2, \dots, i_r \in \{1, 2, \dots, n\}$ such that $f(i_1) = i_2, f(i_2) = i_3, \dots, f(i_r) = i_1$, and $f(j) = j$ if $j \neq i_k$ for $1 \leq k \leq r$.

Example $1, 2, 3, 4 \rightarrow 2, 3, 1, 4$ is a cycle $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$, and 4 is fixed. $1, 2, 3, 4 \rightarrow 2, 1, 4, 3$ is **not** a cycle since $1 \rightarrow 2 \rightarrow 1$ and $3 \rightarrow 4 \rightarrow 3$.

Notation We write a cycle (i_1, i_2, \dots, i_r) . Observe that (i_1, i_2, \dots, i_r) is the same as $(i_2, i_3, \dots, i_r, i_1)$, etc.

Proposition 1.6 If (i_1, i_2, \dots, i_r) and (j_1, j_2, \dots, j_s) are disjoint cycles in S_n , then $(i_1, i_2, \dots, i_r)(j_1, j_2, \dots, j_s) = (j_1, j_2, \dots, j_s)(i_1, i_2, \dots, i_r)$.

Proof Take an integer $i \in \{1, 2, \dots, n\}$. If it is an i , say i_m , the LHS sends i_m to i_{m+1} , as does the RHS. The j case is symmetric. Thus the products are equal.

Example The above proposition is not true if the cycles are not disjoint. In S_3 , $(1, 2)(2, 3), 3 \rightarrow 1$, but $(2, 3)(1, 2), 3 \rightarrow 2$.

Theorem 1.7 Given $f \in S_n$, f can be written as a composite of disjoint cycles. Moreover, if we omit cycles of length 1, the result is unique except for the order in which the cycles occur.

Proof Define $i_1 = 1, i_2 = f(i_1), i_3 = f(i_2)$, etc. This defined a cycle provided that the first time we get $i_{r+1} = a$ predecessor, then $i_{r+1} = i_1$. Suppose $i_{r+1} = i_s$ with $1 < s \leq r$. Then $f(i_r) = i_{r+1} = i_s = f(i_{s-1})$, but a permutation is bijective, so we have a contradiction.

So we get a cycle which has the same effect on i_1, i_2, \dots, i_r as f . Now choose j to be the smallest integer not in $\{i_1, i_2, \dots, i_r\}$ to obtain another cycle $\{j_1, j_2, \dots, j_s\}$. Then $\{i_1, i_2, \dots, i_r\}$ and $\{j_1, j_2, \dots, j_s\}$ are disjoint, for if j_m is an i , then applying f enough times, we get $j_1 = \text{some } i$, which is a contradiction. Continue the same procedure until all integers $\in \{1, 2, \dots, n\}$ are accounted for. We get $f = (i_1, i_2, \dots, i_r)(j_1, j_2, \dots, j_s) \dots$ since both sides have the same effect on all integers $\leq n$.

As for uniqueness, suppose $f = \begin{cases} \alpha_1, \alpha_2, \dots, \alpha_r \\ \beta_1, \beta_2, \dots, \beta_s \end{cases}$, where the α_i, β_i are cycles of length ≥ 2 . Consider $\alpha_i = (i_1, i_2, \dots, i_t)$. Then $f(i_1) \neq i_1$, so i_1 occurs in some β . WLOG, we may suppose that $i_1 \in \beta_1$ and that $\beta_1 = (i_1, j_2, j_3, \dots, j_p)$. $j_2 = f(i_1) = i_2, i_3 = f(i_2) = i_3, \dots, f(j_p) = f(i_p) = i$. So $p = t$. We can continue in this way to show that every α is a β and vice versa.

Example S_6 : $1, 2, 3, 4, 5, 6 \rightarrow 5, 3, 2, 6, 4, 1$ is $(1, 5, 4, 6)(2, 3)$.

Definition 1.8 A permutation such as (a, b) is called a **transposition**. Every element of S_n is a product of transpositions. The parity of the number of transpositions that make up a cycle is invariant.

Definition 1.9 Given a permutation $t \in S_n$, the **signature** $\epsilon(f)$ of f is defined as follows: Let x_1, x_2, \dots, x_n be distinct. $\epsilon(f) = \prod_{1 \leq i < j \leq n} \frac{x_{f(i)} - x_{f(j)}}{x_i - x_j}$. $\epsilon(f) = \pm 1$. For each $i \neq j, \pm(x_i - x_j)$

occurs just once in the numerator and once in the denominator. We say that f is **even** if $\epsilon(f) = 1$ and **odd** if $\epsilon(f) = -1$.

Example Consider $\epsilon(a, b)$ with $a < b$. This permutation sends $1, \dots, a, \dots, b, \dots, n$ to $1, \dots, b, \dots, a, \dots, n$. (That is, we switch a and b and leave everything else fixed.) $\epsilon(a, b) = \frac{x_b - x_a}{x_a - x_b} \prod_{a < j < b} \frac{x_b - x_j}{x_a - x_j} \frac{x_a - x_j}{x_j - x_b}$. Other terms cancel. Thus $\epsilon(a, b) = -1$.

Proposition 1.10 Given $f, g \in S_n$, we have $\epsilon(fg) = \epsilon(f)\epsilon(g)$.

Proof $\epsilon(fg) = \prod_{i < j} \frac{x_{fg(i)} - x_{fg(j)}}{x_i - x_j} = \prod_{i < j} \frac{x_{f(i)} - x_{f(j)}}{x_i - x_j} \prod_{i < j} \frac{x_{fg(i)} - x_{fg(j)}}{x_{f(i)} - x_{f(j)}}$. We write $y_i = x_{f(i)}$ for all i . Then $x_{fg(i)} = y_{g(i)}$ by replacing i by $g(i)$. So $\prod_{i < j} \frac{x_{fg(i)} - x_{fg(j)}}{x_{f(i)} - x_{f(j)}} = \prod_{i < j} \frac{y_{g(i)} - y_{g(j)}}{y_i - y_j}$, which implies that $\epsilon(fg) = \epsilon(f)\epsilon(g)$, as claimed.

Corollary 1.11 If f is a composite of n transpositions, $\epsilon(f) = (-1)^n$.

Proposition 1.12 $\epsilon(i_1, i_2, \dots, i_r) = (-1)^{r-1}$.

Proof $(i_1, i_2, \dots, i_r) = (i_1, i_r)(i_1, i_{r-1}) \cdots (i_1, i_2)$.

Example $f = (1, 5, 4, 6)(2, 3)$, so $\epsilon(f) = (-1)^3(-1) = 1$, so f is even.

Notation If G is a finite group, then the number of elements in G is called the **order** of G and is denoted by $|G|$. Thus $|S_n| = n!$.

Definition 1.13 Let (G, m) be a group. A subset H of G is called a **subgroup** if $m(H \times H) \subset H$, and (H, m) is a group.

Example

1. $H = G$ and $H = \{e\}$ are always subgroups. Other subgroups are called **proper subgroups**.
2. $G = (\mathbb{Z}, +)$, $H =$ even integers.

Proposition 1.14 Let G be a group. A subset H of G is a subgroup if

1. $H \neq \emptyset$
2. Given $h_1, h_2 \in H$, then $h_1 h_2^{-1} \in H$.

Proof First show that \exists a unit element. To do so, take $h \in H$. Then by (2), $hh^{-1} = e \in H$. Next if $h \in H$, then since also $e \in H$, then since also $e \in H$, we have (2) by $eh^{-1} = h^{-1} \in H$.

Clearly multiplication is associative, and finally $m(H \times H) \subset H$. Since, given $h_1 h_2 \in H$, then $h_2 \in H$, $h_1(h_2^{-1}) = h_1 h_2 \in H$.

Example

1. $G = (\mathbb{Q}, +)$, $H = \mathbb{Z}$. Then $H \neq \emptyset$, and $n_1 - n_2 \in \mathbb{Z}$ whenever $n_1, n_2 \in \mathbb{Z}$. Thus \mathbb{Z} is a subgroup.
2. Take $G = S_n$. The set of even permutations in S_n forms a subgroup A_n , called the alternating group.

Proposition 1.15 Let G be a group.

1. If H is a subgroup of G , and J is a subgroup of H , then J is a subgroup of G .
2. If H, J are both subgroups of G , then so is $H \cap J$.

Proof

1. Trivial from the definitions.
2. $H \cap J \neq \emptyset$ since $e \in H \cap J$. Furthermore, if $g, h \in H \cap J$, then $gh^{-1} \in H$ and $gh^{-1} \in J$, so $gh^{-1} \in H \cap J$.

Remark Unions don't work: Let $G = \{\mathbb{C}, +\}$, $H = \{x + iy | y = 0\}$, $J = \{x + iy | x = 0\}$. Then $H \cup J$ is not closed under addition.

Let G be a group and $X \subset G$ a subset.

Definition 1.16 The subgroup of G generated by X , $\langle X \rangle$, is defined to be the intersection of all subgroups of G containing X . (i.e. $\langle X \rangle = \{g \in G | g \in \text{every subgroup containing } X\}$).

Proposition 1.17 $\langle X \rangle$ is a subgroup and is the "smallest" subgroup containing X in the sense that if H is a subgroup of G and $X \subset H$, then $\langle X \rangle \leq H$.

Proof $\langle X \rangle$ is a subgroup because it is the intersection of subgroups. The second part is modified from Definition 1.16.

Proposition 1.18 $\langle X \rangle$ consists of e , together with all elements of the form $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, where $x_1, x_2, \dots, x_n \in X$ (not necessarily distinct), and $a_1, a_2, \dots, a_n \in \mathbb{Z}$ ($n \geq 1$).

Proof The collection H of such elements **does** form a subgroup by Proposition 1.14. Clearly $H \supset X$, and so $H \geq \langle X \rangle$. But any subgroup containing X must also contain all such elements, so $\langle X \rangle$ contains all such elements, i.e. $\langle X \rangle \geq H$, and so $\langle X \rangle = H$.

Example

1. Take G to be any group, and $X = \emptyset$. Then $\langle \emptyset \rangle = e$.
2. Take $G = (\mathbb{Z}, +)$, $H = \langle 2 \rangle$, i.e. the even integers.
3. $G = (\mathbb{R}, +)$, $H = \langle 1 \rangle = \mathbb{Z}$.

Definition 1.19 Let g be an element of a group G . Then the subgroup $\langle g \rangle$ is called the **cyclic subgroup generated by g** . If $\exists g \in G$ such that $\langle g \rangle = G$ then G is a **cyclic group**.

Definition 1.20 The order of an element g in G is $|\langle g \rangle|$ if this quantity is finite. If \exists a finite set $X \subset G$ such that $G = \langle X \rangle$, then G is **finitely generated**.

Example Consider the group S_n . We know that every permutation can be expressed as a product of transpositions. We claim that S_n is generated by $(1, 2), (1, 3), \dots, (1, n)$. To show this, we only have to express a general transposition in terms of those of the form (i, j) . If $i, j \neq 1$, this is done by the formula $(i, j) = (1, i)(i, j)(1, j)$ combined with the relation $(1, i) = (i, 1)$. This establishes the

result. We now claim that A_n is generated by $(1, 2, 3), (1, 2, 4), \dots, (1, 2, n)$. First observe that A_n is generated by the set of all 3-cycles. This is because we have the formula $(i, j)(k, l) = (k, i, l)(i, j, k)$ and $(i, k)(i, j) = (i, j, k)$. Now use the following formulae to express any 3-cycles in terms of the cycles $(1, 2, i)$:

$$\begin{aligned}(i, j, k) &= (1, 2, i)(2, j, k)(1, 2, i)^{-1} \\ (2, j, k) &= (1, 2, j)(1, 2, k)(1, 2, j)^{-1} \\ (1, j, k) &= (1, 2, k)^{-1}(1, 2, j)(1, 2, k)\end{aligned}$$

Theorem 1.21 Let $G = \langle g \rangle$ be a cyclic group. Then G is abelian. If $|G| = n$ (i.e. G is finite), then the elements of G are $e, g, g^2, \dots, g^{n-1}$, and $g^n = e$. Indeed, $g^m = e$ iff $n \mid m$. If $|G|$ is not finite, then $g^n = g^m$ iff $n = m$.

Proof This is left as an exercise to the reader.

Definition 1.22 Given groups G, H , a function $\theta : G \rightarrow H$ is a **homomorphism** if $\forall g_1, g_2 \in G$, $\theta(g_1g_2) = \theta(g_1)\theta(g_2)$.

Proposition 1.23 Suppose that $\theta : G \rightarrow H$ is a homomorphism. Then

1. If $e \in G$ is the unit element, then $\theta(e) \in H$ is the unit element in H .
2. $\forall g \in G$, $\theta(g^{-1}) = \theta(g)^{-1}$.

Proof

1. Suppose $f \in H$ is the unit element. Then $f = hh^{-1}$. For any $h \in H$, $f = \theta(g)\theta(g)^{-1}$, and if $g \in G$, $\theta(eg)\theta(g)^{-1} = \theta(e)\theta(g)\theta(g)^{-1} = \theta(e)$.
2. $\theta(g^{-1})\theta(g) = \theta(gg^{-1}) = \theta(e) = f$. Similarly $\theta(g)\theta(g^{-1}) = f$. Thus $\theta(g^{-1}) = \theta(g)^{-1}$.

Example G = the group of positive reals under multiplication, $H = (\mathbb{R}, +)$. Then $\theta : G \rightarrow H; \theta(x) = \log(x)$ is a homomorphism.

Definition 1.24 If $\theta : G \rightarrow H$ is bijective, it is called an **isomorphism**. In this case, we say G and H are **isomorphic**, and we write $G \simeq H$.

Definition 1.25 An isomorphism $\theta : G \rightarrow G$ is called an **automorphism**. A homomorphism $\theta : G \rightarrow G$ is called an **endomorphism**.

Definition 1.26 If $\theta : G \rightarrow H$ is a homomorphism, the **image** $\theta(G) \subset H$ is defined as for sets and functions. The set $\{g \in G \mid \theta(g) = f, \text{ the unit element of } H\}$ is called the **kernel** of θ and is written $\ker(\theta)$.

1.2 Homomorphisms

Proposition 1.27 Suppose that $\theta : G \rightarrow H$ is a homomorphism. Then $\theta(G)$ is a subgroup of H , and $\ker(\theta)$ is a subgroup of G . Moreover, θ is 1-1 iff $\ker(\theta) = \{e\}$. Thus θ is an isomorphism iff $\ker(\theta) = \{e\}$ and $\theta(G) = H$.

Proof Use Proposition 1.14: $\theta(e) \in \theta(G)$, and so $\theta(G) \neq \emptyset$. Suppose $h_1, h_2 \in \theta(G)$. Then $\exists g_1, g_2 \in G$ such that $\theta(g_1) = h_1$ and $\theta(g_2) = h_2$. So $h_1 h_2^{-1} = \theta(g_1) \theta(g_2)^{-1} = \theta(g_1 g_2^{-1}) \in \theta(G)$.

Set $f =$ the identity element of H . We have $e \in \ker(\theta)$. So $\ker(\theta) \neq \emptyset$. If $g_1, g_2 \in \ker(\theta)$, then $\theta(g_1 g_2^{-1}) = \theta(g_1) \theta(g_2)^{-1} = f$. (i.e. $g_1 g_2^{-1} \in \ker(\theta)$). If θ is 1-1, and $g \in \ker(\theta)$, then $\theta(g) = f = \theta(e)$ implies $g = e$. Conversely, if $\ker(\theta) = \{e\}$, and $\theta(g_1) = \theta(g_2)$. Then $\theta(g_1 g_2^{-1}) = \theta(g_1) \theta(g_2^{-1}) = \theta(g_1) \theta(g_2)^{-1} = f$. Thus $g_1 g_2^{-1} \in \ker(\theta)$, and so $g_1 g_2^{-1} = e$, i.e. $g_1 = g_2$. So θ is 1-1.

Examples

1. $G = H = (\mathbb{R}, +)$. $\theta : G \rightarrow H$; $\theta(x) = 2x$.
2. $G = \mathbb{Z}_2$, $H = (\pm 1, \times)$. $\theta : G \rightarrow H$ by $\theta(0) = 1, \theta(1) = -1$.

1.3 Group Actions and Coset Decompositions

Let X be a set, and let G be any group. A group action of G on X or a G -**action** on X is a mapping $\mu : G \times X \rightarrow X$ such that

1. $\mu(gh, x) = \mu(g, \mu(h, x)) \forall x \in X, \forall g, h \in G$.
2. $\mu(e, x) = x \forall x \in X$.

We say that G **acts on** X , and X is called a G -**set**.

We write gx rather than $\mu(g, x)$. Given a G -action on X , each $g \in G$ defines a mapping $\varphi_g : x \rightarrow x$ by $\varphi_g(x) = gx$. Hence the mapping $g \mapsto \varphi_g$ is a mapping $G \rightarrow \{\text{mappings of } X \text{ to itself}\}$. Now (1) implies that $\varphi_g \varphi_{g^{-1}} = \varphi_e = 1x$. Hence each map φ_g is a permutation of X . It now follows from (1) that the map $g \mapsto \varphi_g$ is a homomorphism $G \rightarrow S_X$. The action is said to be **faithful** if this homomorphism is injective. Conversely, suppose we are given any set X together with a homomorphism $g \mapsto \varphi_g$ from G to S_X . Then we can define a G -action on X by setting $gx = \varphi_g(x)$.

Let X be a set. Then any group action on X may be used to define an equivalence relation on X . Put $X \sim Y$ iff $y = gx$ for some $g \in G$.

1. \sim is reflexive since $1x = x \forall x \in X$.
2. \sim is symmetric since $y = gx$ implies $x = g^{-1}y$.
3. \sim is transitive since $y = gx$ and $z = hy$ implies $z = h(gx) = (hg)x$.

The equivalence classes are called the **orbits** of the action. We write Gx for the orbit containing x . If X consists of a single orbit, then G is said to act **transitively** on X .

Example

1. If X is any set, the symmetric group S_X acts on X in a natural way. We can pass from any element of X to any other by a suitable permutation. Hence S_X acts transitively.
2. If X is any set and G any group, we can define a G -action by putting $gx = x \forall x \in X, g \in G$. This is called the **trivial** G -action, and its orbits are the one-element subsets of X .
3. Let G be any group. We can let G act on itself via left multiplication (i.e. for each $g \in G$, we define a map $G \rightarrow G$ by $\lambda g : x \mapsto gx$). This is called the **regular representation** of G . Here G acts transitively on itself.
4. Consider a mapping $\alpha_g : x \mapsto gxg^{-1}$. Then $\alpha_g \alpha_h(x) = \alpha_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \alpha_{gh}(x)$. Plainly $\alpha_e = \text{identity map}$. So we have a group action called **conjugation**. This action is never transitive unless G is trivial. Since each α_g leaves e fixed, this is the trivial action precisely when G is abelian.
5. Given a group G and a subgroup H , consider the natural H -action on G obtained by left multiplication. If H is a proper subgroup, this action is not transitive: the orbits are of the form $Hx(x \in G)$. These are called the **right cosets** of H in G .

Note $H = H_e$ is itself a right coset. Recall that orbits are equivalence classes. Thus right cosets are classes of an equivalence relation (namely $x \sim y$ iff $x = hy$ for some $h \in H$). Therefore we obtain a partition of G in the form $G = \bigcup Hx$, which is the disjoint union of equivalence classes. This is called a **right coset decomposition**.

Suppose now that G is *finite*. Then the number of right cosets of H in G is finite. It is called the **index** of H in G , and it is written $|G : H|$. Now for each $x \in G$, \exists a bijection between H and Hx given by $h \mapsto hx$. Hence each right coset has $|H|$ elements. This from the right coset decomposition, we obtain $|G| = |G : H||H|$.

Theorem 1.28 (Lagrange's Theorem) Let G be a finite group. Then the order of any subgroup divides the order of G .

1.4 Isomorphism Theorems

Let X be a subset of a group G . An element $c \in G$ is said to **normalize** X if $c^{-1}Xc = X$. A subset C of G is said to **normalize** X if each $c \in C$ normalizes X . The set $\{c \in G | c \text{ normalizes } X\}$ is called the **normalizer** of X . If G is the normalizer of X , then we say that X is **normal** in G .

Now suppose G, H are groups and that $f : G \rightarrow H$ is a homomorphism.

Proposition 1.29 $\ker(f)$ is normal in G .

Proof Suppose that $a \in \ker(f)$ and $c \in G$. Then $f^{-1}(c^{-1}f(a)f(c)) = f^{-1}(c^{-1}e c) = f^{-1}(e) = a$.

Proposition 1.30 Every normal subgroup occurs as the kernel of some homomorphism.

Proof Let N be a normal subgroup of G , i.e. $N \triangleleft G$. We have $c^{-1}Nc = N \forall c \in G$, so $cN = Nc \forall c \in G$.

Write G/N for the collection of all cosets of N in G . Define a multiplication of cosets as follows: Put $(aN)(bN) = abN$. This is well-defined (i.e. independent of a and b). With this multiplication, G/N is a group: the unit element is N , and the inverse of aN is $a^{-1}N$. G/N is called a **quotient group**.

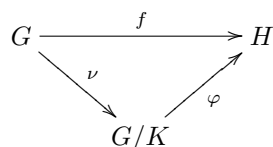
Proposition 1.31 Suppose that $N \triangleleft G$. Then the function $\nu : G \rightarrow G/N$ given by $\nu(a) = aN$ is a surjective homomorphism, and $\ker(\nu) = N$.

Proof Exercise.

Theorem 1.32 (First Isomorphism Theorem) Let $f : G \rightarrow H$ be a homomorphism with kernel K . Then $K \triangleleft G$, and $G/K \simeq \text{Im}(f)$.

Proof We've already shown that $K \triangleleft G$. Define $\varphi : G/K \rightarrow H$ by $\varphi(aK) = f(a)$. First we must prove that φ is well-defined. Suppose $aK = bK$, i.e. $a^{-1}b \in K$, and write e_H for the unit element in H . Then $f(a^{-1}b) = f(a)^{-1}f(b) = e_H$. Thus $f(a) = f(b)$, and so φ is well-defined. Now we must show that φ is a homomorphism. $\varphi(aK \cdot bK) = \varphi(abK) = f(ab) = f(a)f(b) = \varphi(aK)\varphi(bK)$. Finally we must show that φ is injective. Suppose that $\varphi(aK) = \varphi(bK)$. Then $f(a) = f(b)$. So $f(ab^{-1}) = e_H$. Hence $ab^{-1} \in K$, and so $aK = bK$.

Diagram



Definition 1.33 Suppose that H, K are any subgroups of G .

1. The subset HK of G is defined by $HK = \{hk|h \in H, k \in K\}$.
2. Write $H \vee K$ for the subgroup of G generated by $H \cup K$. So $H \vee K$ consists of all products of the form $a_1 a_2 \cdots a_n$, with $a_i \in H \cup K$, $n \geq 1$. $H \vee K$ is the smallest subgroup of G containing both H and K , and it is called the **join** of H and K . Plainly

$$HK \leq H \vee K. \tag{*}$$

Equality need not hold, e.g. take $G = S_4$, $H = \langle (1, 2) \rangle$, $K = \langle (1, 2, 3, 4) \rangle$. Then $H \vee K$ is S_4 since S_4 is generated by $(1, 2)$ and $(1, 2, 3, 4)$ (Show this!). However, $|H| = 2$; $|K| = 4$, and so $|HK| \leq 8$, while $|S_4| = 24$.

Now HK always contains H and K . Hence equality holds in (*) precisely when HK is a subgroup of G .

Lemma 1.34 HK is a subgroup of G iff $HK = KH$.

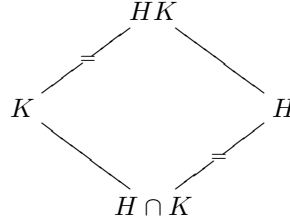
Proof Suppose that $HK = KH$. Then $HKHK = HHKK = HK$. $(HK)^{-1} = KH = HK$. Hence HK is a subgroup. Suppose conversely that HK is a subgroup. Then $HK = (HK)^{-1} =$

$$K^{-1}H^{-1} = KH.$$

Next we note that $HK = KH$ if one of H, K is normal in G .

Theorem 1.35 (Second Isomorphism Theorem) Let G be a group and H and K subgroups of G , with $K \triangleleft G$. Then $H \cap K \triangleleft H$, and there is an isomorphism $H/H \cap K \simeq HK/K$.

Diagram



Proof Consider the natural homomorphism $\nu : G \rightarrow G/K$, and let $\nu_1 = \nu|_H$. $\ker(\nu_1)$ consists of all elements of H mapped to 1 under ν i.e. $\ker(\nu_1) = H \cap K$. $\text{Im}(\nu_1)$ consists of the union of the cosets of K having a representative in H , i.e. HK . Hence, by the First Isomorphism Theorem, $H/H \cap K \simeq HK/K$.

Example Suppose that $H \leq S_n$. Either $H \leq A_n$, in which case H consists entirely of even permutations, or H contains an odd permutation. In the latter case, $HA_n = S_n$, and so $H/H \cap A_n \simeq S_n/A_n$, which is of order 2. Hence if H contains any odd permutations at all, then the even permutations in H form a normal subgroup of index 2.

Theorem 1.36 (Third Isomorphism Theorem) Suppose that $K \leq H \leq G$, and $K \triangleleft G$ and $H \triangleleft G$. Then H/K is a normal subgroup of G/K , and $(G/K)/(H/K) \simeq G/H$.

Proof Define $f : G/K \rightarrow G/H$ by $f(aK) = aH$. Then f is well-defined and surjective, and $\ker(f) = H/K$.

Theorem 1.37 (The Correspondence Theorem) Let G, H be groups, and let $\varphi : G \rightarrow H$ be a surjective homomorphism with kernel N . So $H \simeq G/N$. So there is a bijective correspondence, given by φ , between the set of subgroups of G that contain N and the set of subgroups of H . If K is a subgroup of G containing N , then this correspondence sends K to $\varphi(K)$.

If L is a subgroup of H , then the subgroup under this correspondence is $\varphi^{-1}(L) = \{x \in G | \varphi(x) \in L\}$. Moreover, if K_1, K_2 are subgroups of G containing N , then

1. $K_2 \leq K_1$ iff $\varphi(K_2) \leq \varphi(K_1)$. In this case, we have $|K_1 : K_2| = |\varphi(K_1) : \varphi(K_2)|$.
2. $K_2 \triangleleft K_1$ iff $\varphi(K_2) \triangleleft \varphi(K_1)$. In this case, the map $K_1/K_2 \rightarrow \varphi(K_1)/\varphi(K_2) \times K_2 \mapsto \varphi(x)\varphi(K_2)$ is an isomorphism.

Proof Exercise.

Suppose that G is a group and $H \leq G$. (H is not necessarily normal.) Write G/H for the collection of all the left cosets H in G .

Theorem 1.38 Suppose that $H \leq G$ and that $|G : H| = n$. Then \exists a homomorphism $\rho : G \rightarrow S_n$ with $\ker(\rho) \leq H$.

Proof Suppose that $g \in G$. Define a **function** $\rho_g : G/H \rightarrow G/H$ by $xH \mapsto g \times H \forall x \in G$. Then each ρ_g is a permutation since the inverse of ρ_g is $\rho_{g^{-1}}$, and $g \mapsto \rho_g$ is a homomorphism $G \rightarrow S_{G/H} \simeq S_n$. Suppose that $g \in \ker(\rho)$. Then $g \times H = xH \forall x \in G$, and so $g \in H$. So $\ker(\rho) \leq H$. (ρ is called the representation of G on the cosets of H .)

Corollary 1.39 (Cayley's Theorem) Every group G can be embedded as a subgroup of S_G . In particular, if $|G| = n$, then G can be embedded in S_n .

Proof Take $H = \{e\}$ in Theorem 1.38.

A group G is **simple** if it has no proper normal subgroups.

Corollary 1.40 Suppose that G is an infinite simple group. Then G has no proper subgroups of finite index.

Proof Suppose $H \leq G$ with $1 < |G : H| < \infty$. Then Theorem 1.38 gives a homomorphism $\rho : G \rightarrow S_{G/H}$ with $\ker(\rho) \leq H$. Since $\ker(\rho) \triangleleft G$, we must have $\ker(\rho) = \{e\}$, which is a contradiction since G is infinite.

Suppose that X, Y are G -sets. A function $\varphi : X \rightarrow Y$ is called a **G -set homomorphism** if it commutes with the actions of G , i.e. $\varphi(gx) = g\varphi(x) \forall g \in G, x \in X$. If φ is bijective, then φ is called a **G -set isomorphism**. We write $X \simeq Y$ in this case. We want to classify all G -sets up to isomorphism. Let X be a G -set, and let $x \in X$.

Recall that the orbit of x is $\{gx | g \in G\} = Gx$.

The stabilizer of x , written G_x , is defined by $G_x = \{g \in G | gx = x\}$. This is plainly a group, sometimes called the isotropy group of x .

A subset of X is a G -set under the action induced from X iff it is a union of orbits.

Lemma 1.41 If X is a G -set, then $G_{gx} = gG_xg^{-1}$ for any $g \in G$ and $x \in X$.

Proof $u \in G$ stabilizes gx iff $g^{-1}ug$ stabilizes x iff $u \in gG_xg^{-1}$. Now a subset of X is a transitive G -set under the action induced from X iff it consists of a single orbit. Furthermore, X is a disjoint union of orbits. So, to describe all G -sets it suffices to describe all transitive G -sets.

Proposition 1.42 If X is a transitive G -set, then $X \simeq G/G_x$ are G -sets for any $x \in X$.

Proof Let $x \in X$, and define $\varphi : G \rightarrow G/G_x \rightarrow X$ by $\varphi(gG_x) = gx$.

First we must prove that φ is well-defined. Suppose that $gG_x = g'G_x$ for $g, g' \in G$. Then $g^{-1}g' \in G_x$, and so $g'x = gx$.

A similar argument shows that φ is injective.

Next, we observe that if $u \in G$ and $gG_x \in G/G_x$, $u\varphi(gG_x) = ugx = (ug)x = \varphi(ugG_x) = \varphi(u(gG_x))$, and so φ is a G -set homomorphism.

Suppose that $y \in X$. Then by transitivity, $\exists g \in G$ such that $y = gx = \varphi(gG_x)$, and so φ is surjective. Therefore φ is a G -set isomorphism.

Corollary 1.43 (The Orbit-Stabilizer Theorem) Let X be a G -set. Then $Gx \simeq G/G_x$ as G -sets for any $x \in X$. In particular, if G is finite, then $|Gx| = |G : G_x|$.

Proof The proof follows from Proposition 1.42 since Gx is a transitive G -set.

When are two transitive G -sets isomorphic?

Lemma 1.44 Let $\varphi : X \rightarrow Y$ be a homomorphism of G -sets, and let $x \in X$. Then $G_x \leq G_{\varphi(x)}$. Furthermore, if φ is an isomorphism, then $G_x = G_{\varphi(x)}$.

Proof If $g \in G_x$, then $\varphi(x) = \varphi(gx) = g\varphi(x)$. Hence $G_x \leq G_{\varphi(x)}$. If φ is an isomorphism, then look at the G -set homomorphism $\varphi^{-1} : Y \rightarrow X$. We have $G_{\varphi(x)} \leq G_{\varphi^{-1}(\varphi(x))} \leq G_x$, and so $G_x = G_{\varphi(x)}$.

Proposition 1.45 If H and K are subgroups of G , then the G -sets G/H and G/K are isomorphic iff H and K are conjugate.

Proof G/H and G/K are transitive G -sets. Hence Lemma 1.41 implies that the set of stabilizers of the G -set G/H is precisely the set of conjugates of H . Similarly, the set of stabilizers of the G -set G/K is the set of conjugates of K . Now if $G/H \simeq G/K$ as G -sets, then Lemma 1.44 implies that these sets of stabilizers are equal. So, in particular, H and K are conjugates. Conversely, suppose that $H = gKg^{-1}$ for some $g \in G$. Then H is the stabilizer of $gK \in G/K$. Hence $G/K \simeq G/H$ as G -sets.

Example Let X be a G -set. We say that X is **2-transitive** (and we say that G acts 2-transitively on X) if the following is true: (x_1, x_2) and (y_1, y_2) are elements of $X \times X$, with $x_1 \neq x_2$ and $y_1 \neq y_2$. \exists such $g \in G$ such that $gx_1 = y_1$ and $gx_2 = y_2$. e.g. The natural action of S_n on $\{1, 2, \dots, n\}$ for $n \geq 2$ is transitive. Any 2-transitive set is clearly transitive.

A proper subgroup H of G is said to be **maximal** if there is no proper subgroup of G that properly contains H . e.g. Any subgroup of prime index is maximal.

Claim Let G be a group, and let X be a 2-transitive G -set, and let $x \in X$. Then G_x is a maximal subgroup of G .

Proof Since X is 2-transitive and hence transitive, we have $X \simeq G/G_x$ as G -sets. Suppose that $G_x < K < G$ for some subgroup K . Then $\exists g \in G$ and $k \in K$ such that $g \notin K$ and $k \notin G_x$. Since X is 2-transitive, $\exists u \in Gx$ such that $u(G_x) = Gx$, $u(kG_x) = gGx$. Therefore $u \in Gx$, and hence $uk \in K$. Next, observe that we have $g^{-1}ukG_x = Gx$, and so $g^{-1}uk \in Gx$. Hence $g^{-1} \in K$. This is a contradiction, so G_x is maximal.

Definition 1.46 Let G be any group. For $x \in G$, we define the **centralizer** of x in G to be the set $C_G(x) = \{g \in G \mid gx = xg\}$. Plainly $C_G(x) \leq G$ for any $x \in G$.

If $S \leq G$, then $C_G(S) = \{g \in G \mid gx = xg \forall x \in S\} = \bigcap_{x \in S} C_G(x)$ is the centralizer of S in G .

$Z(G) = C_G(G)$ is called the **center** of G .

The **conjugacy class** of $x \in G$ is the set $\{gxg^{-1} \mid g \in G\}$ of all conjugates of x by elements of G .

Proposition 1.47 The conjugacy classes of G form a partition of G . If G is finite, then an element $x \in G$ has $|G : C_G(x)|$ conjugates in G .

Proof Let G act on itself by conjugation (so $g \in G$ sends $x \in G$ to gxg^{-1}). The orbit of $x \in G$ under this action is $\{gxg^{-1} \mid g \in G\}$. This implies the first assertion. The stabilizer G_x of $x \in G$ is $\{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x)$. The second assertion now follows from the Orbit–Stabilizer Theorem (Corollary 1.43).

Theorem 1.48 (The Class Equation) Let G be a finite group, and let g_1, g_2, \dots, g_n be representatives of the distinct conjugacy classes of G not contained in $Z(G)$. Then $|G| = |Z(G)| + \sum_{i=1}^n |G : C_G(g_i)|$.

Proof First note that $\{x\}$ is a conjugacy class of size 1 iff $x \in Z(G)$ since then $g^{-1}xg = x \forall g \in G$. Let $Z(G) = \{1, 2, \dots, Z_m\}$. Let K_1, K_2, \dots, K_n be the conjugacy classes of G not contained in $Z(G)$, and let g_i be a representation of K_i for each i . The full set of conjugacy classes of G is $\{1\}, \{Z_1\}, \{Z_2\}, \dots, \{Z_m\}, K_1, K_2, \dots, K_n$. Since these partition G , we have $|G| = \sum_{i=1}^m |Z_i| + \sum_{i=1}^n |K_i| = |Z(G)| + \sum_{i=1}^n |G : C_G(g_i)|$.

Remark All the summands on the right side of the class equation are divisors of $|G|$. This restricts their possible values.

For $H \leq G$, recall that the normalizer $N_G(H)$ is defined by $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. Then $N_G(H) \leq G$, and $H \triangleleft N_G(H)$. (In fact, $N_G(H)$ is the largest subgroup of G in which H is normal.) $N_G(H) = G$ iff $H \triangleleft G$.

Proposition 1.49 A subgroup H of a finite group G has exactly $|G : N_G(H)|$ conjugates in G . In particular, the number of conjugates of H in G divides $|G : H|$ and is equal to 1 iff $H \triangleleft G$.

Proof Let $\wp(G)$ be the set of all subsets of G . Let $g \in G$ act on $\wp(G)$ by sending $S \in \wp(G)$ to gSg^{-1} . This defines an action of G on $\wp(G)$.

The orbit of H under this action is the set of conjugates of H in G . The stabilizer of H is $N_G(H)$. The result now follows from the Orbit–Stabilizer Theorem.

How many orbits are there in a G -set?

Theorem 1.50 Let G be a finite group acting on a finite G -set X . For each $g \in G$, let C_g be the number of points fixed by g . Then the number of orbits is $t = \frac{1}{|G|} \sum_{g \in G} C_g$. So t is the “average” number of points fixed by a permutation.

Proof Count the number of pairs $(g, x) \in G \times X$ such that $gx = x$ in two ways:

1. For each $g \in G$, the number of pairs containing g is C_g . Thus the total number of pairs is $\sum_{g \in G} C_g$.
2. For each orbit of k points, say, each point is fixed by the elements of its stabilizer. This stabilizer has $|G|/k$ elements by the Orbit-Stabilizer Theorem. Hence each orbit contributes $|G|$ pairs.

Hence the number of pairs is $t|G|$, so $t|G| = \sum_{g \in G} C_g$, or $t = \frac{1}{|G|} \sum_{g \in G} C_g$.

Chapter 2

Local Structure

Definition 2.1 Let G be a group and p a prime divisor of $|G|$. Say that $g \in G$ is a p -**element** if its order is a power of p . Say that G is a p -**group** if $|G|$ is a power of p . Say that $H \leq G$ is a p -**subgroup** of G if $|H|$ is a power of p .

Definition 2.2 Suppose that G is a group of order $n = p^\alpha n'$, where $p \nmid n'$. Any subgroup of G of order p^α is called a **Sylow p -subgroup** of G . A subgroup of G is said to be a **Sylow subgroup** of G if it is a Sylow p -subgroup for some prime divisor p of n .

Lagrange's Theorem provides a necessary condition on the order of a subgroup of a finite group. This condition is not sufficient, e.g. $|A_4| = 12$, but A_4 has no subgroup of order 6.

Theorem 2.3 (Sylow, 1872) If n divides $|G|$, then G has a subgroup of order n provided that n is a prime power.

Remark Let G be a p -group acting on a finite set X . Let X_0 denote the set of points fixed by G , i.e. the collection of 1-point orbits. The Orbit-Stabilizer Theorem implies that the number of points in any orbit is a power of p and hence is either 1 or is divisible by p . So, modulo p , we can ignore orbits with more than one point, and so we have $|X_0| \equiv |X| \pmod{p}$.

Theorem 2.4 (Sylow) Let G be a finite group and p and prime.

1. G has Sylow p -subgroups, and every p -subgroup of G is contained in a Sylow p -subgroup.
2. All Sylow p -subgroups of G are conjugate. Hence, if S denotes one of them, their number is a divisor of $|G : S|$.
3. The number of Sylow p -subgroups is congruent to 1 (mod p).

Proof

1. Write $|G| = n = p^\alpha n'$, where $p \nmid n'$. Let M be the collection $\{x_1, x_2, \dots, x_k\}$ of all subsets of G of size p^α . Let G act on M by left multiplication. At least one orbit has order prime to p . The stabilizer S of every element in the orbit is a Sylow p -subgroup of G . Now let S be the Sylow p -subgroup just found, and let H be any p -subgroup of G . Let H act on the set of left cosets of S in G via left multiplication: $xS \mapsto axS$ ($a \in H$). The total number of

cosets is $|G : S| = n'$, which is prime to p . Since H is a p -subgroup, the remark implies that H fixes some coset, i.e. $HxS = xS$ for some $x \in G$. Hence $Hx \subset xS$, or $H \subset xSx^{-1}$. Since $|xSx^{-1}| = |S| = p^\alpha$, xSx^{-1} is a Sylow p -subgroup of G .

2. Suppose that H above is itself a Sylow p -subgroup. Then $H = xSx^{-1}$. Hence all Sylow p -subgroups are conjugate. Let N be the normalizer of S in G . Then $S \leq N$, and the number of conjugates of S in G is $|G : N|$. This is a factor of $|G : S| = |G : N||N : S|$.
3. Let $\Sigma = \{S_1, S_2, \dots, S_r\}$ be the set of all Sylow p -subgroups of G , and let S_1 act on Σ by conjugation. We claim that the only fixed point under this action is S_1 . If not, then $a^{-1}S_i a = S_i$ for some $i \neq 1$ and $\forall a \in S_1$. This implies that $S_1 S_i = S_i S_1$. Hence $S_1 S_i$ is a subgroup of G , and $S_i \triangleleft S_1 S_i$. But S_1 and S_i are both Sylow p -subgroups of $S_1 S_i$, and hence S_1 is conjugate to S_i in $S_1 S_i$. This is impossible since S_1 is normal in $S_1 S_i$ but different from S_i . Hence Σ has just one fixed point under the action of S_1 , and the remark shows that $|\Sigma| \equiv 1 \pmod{p}$.

Corollary 2.5 (Cauchy's Theorem) Suppose that $p \mid |G|$. Then G has an element of order p .

Proof G has a non-trivial Sylow p -subgroup, and hence G has a non-trivial p -element, some power of which is of order p .

Example There is no simple group G of order 36.

Proof $36 = 4 \cdot 9$. Suppose that G is simple, and let P be a Sylow 3-subgroup of G . Then P has 4 conjugates in G (or else P has 1 conjugate, but we assume that doesn't happen by hypothesis). Now $|G : P| = 4$. Consider the action of G on the left cosets of P in G via multiplication. This gives us a homomorphism $\psi : G \rightarrow S_4$ with $\ker \psi \leq P$. Since G is simple, ψ is injective, which is a contradiction since $36 > 24$.

Theorem 2.6 (Frattini's Argument) Suppose that G is a finite group and that $K \triangleleft G$. Suppose that P is a Sylow p -subgroup of K . Then $G = KN_G(P)$.

Proof If $g \in G$, then $gPg^{-1} \leq gKg^{-1} = K$, since $K \triangleleft G$. Hence gPg^{-1} is a Sylow p -subgroup of K , and so $\exists k \in K$ with $kPk^{-1} = gPg^{-1}$. Hence $P = (k^{-1}g)P(k^{-1}g)^{-1}$, and so $k^{-1}g \in N_G(P)$. The result now follows since $g = k(k^{-1}g)$.

Proposition 2.7 Suppose that G is a finite group and that $H, K \leq G$. Then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof Let $X = G/K$, and consider X as an H -set under left multiplication. Then the orbit of $x \in G/K$ under the action of H is just $\{hk|h \in H\} = HK$. Hence $|HK| = |K| \times$ the number of cosets of K which lie in this orbit. The stabilizer H_K of K is $H \cap K$. Thus by the Orbit-Stabilizer Theorem, the orbit in question consists of $|H : H \cap K|$ cosets of K .

Question What is the relationship between the Sylow p -subgroups of a group and those of its normal subgroups and quotient groups?

Proposition 2.8 Let $N \triangleleft G$, and let P be a Sylow p -subgroup of G . Then PN/N is a Sylow p -subgroup of G/N , and $P \cap N$ is a Sylow p -subgroup of N .

Proof The Correspondence Theorem immediately implies that $|G/N : PN/N| = |G : PN|$. Now $|G : PN|$ divides $|G : P| = |G : PN||PN : P|$, and $p \nmid |G : P|$. Hence $p \nmid |G/N : PN/N|$. Since $PN/N \simeq P/P \cap N$, it follows that PN/N must be a p -group. Hence PN/N is a Sylow p -subgroup of G/N . Now Proposition 2.7 implies that $|N : P \cap N| = |PN : P|$. Since PN is a subgroup of G (since $N \triangleleft G$), and P is a Sylow p -subgroup of G , we must have $p \nmid |PN : P|$. Hence $P \cap N$ is a p -subgroup of N which index in N is coprime to p , as required.

Exercise on Direct Products Suppose that G is a group having subgroups H_1, H_2, \dots, H_n such that the following conditions hold:

1. $H_i \triangleleft G$ for each $1 \leq i \leq n$.
2. Every $g \in G$ has a unique expression $g = h_1 h_2 \cdots h_n$, where $h_i \in H_i$ for each i .

Then conditions (1) and (2) imply the following:

3. $G = H_1 H_2 \cdots H_n$.
4. $H_i \cap (H_1 H_2 \cdots H_i \cdots H_n) = 1$ for each i .
5. If $i \neq j$, then the elements of H_i commute with those of H_j .
6. If $g = h_1 h_2 \cdots h_n$ and $g' = h'_1 h'_2 \cdots h'_n$ (where $h_i h'_i \in H_i$ for each i), then $gg' = (h_1 h'_1)(h_2 h'_2) \cdots (h_n h'_n)$.
Under these circumstances, $G \simeq H_1 \times H_2 \times \cdots \times H_n$.

Remark If (1) holds, then (2) holds iff **both** (3) and (4) hold.

2.1 Finite p -groups

Here is the most basic property of finite p -groups

Theorem 2.9 If P is a nontrivial finite p -group, then $Z(P)$ is also nontrivial. Moreover, if $1 \neq N \triangleleft P$, then $N \cap Z(P) \neq 1$.

Proof Let K_1, K_2, \dots, K_r be the conjugacy classes of P not lying in $Z(P)$. Then $p \mid |K_i|$, $i = 1, 2, \dots, r$, and the class equation gives $|P| = |Z(P)| + \sum_{i=1}^r |K_i|$. Since $p \mid |P|$, it follows that $p \mid |Z(P)|$ also. Hence $Z(P)$ is a nontrivial group.

Now suppose that $N \triangleleft P$, with $N \neq 1$. N is a disjoint union of conjugacy classes of P . If $N \cap Z(P) = \{1\}$, then this would imply that $N = \{1\} \cup K_{i_1} \cup K_{i_2} \cup \cdots \cup K_{i_s}$. Hence $|N| \equiv 1 \pmod{p}$, which is a contradiction since N is a p -group. Thus $N \cap Z(P) \neq 1$.

Corollary 2.10 The only finite simple p -groups are the groups of prime order.

On the other hand, the center of a non-abelian finite p -group cannot be too large either.

Lemma 2.11 If G is **any** non-abelian group, then $G/Z(G)$ cannot be cyclic. In particular, if P is a finite, non-abelian p -group, then $|P : Z(P)| \neq p$.

Proof Suppose that $G/Z(G) = \langle xZ(G) \rangle$ for some $x \in G$. Then $G = \langle x, Z(G) \rangle$, and this group is clearly abelian.

Recall that a proper subgroup H of a group G is said to be **maximal** if there is no proper subgroup of G that properly contains H . Maximal subgroups of finite p -groups are well-behaved.

Proposition 2.12 If P is a finite p -group, then every maximal subgroup of P is normal in P .

Proof We use induction on $|P|$. If $|P| = 1$, then P has no maximal subgroups. If $|P| = p$, then P is cyclic of order p , and the result clearly holds. Assume that $|P| > p$ and that the result holds \forall p -groups of order less than $|P|$. Let M be a maximal subgroup of P , and let $Z = Z(P)$. Now $Z \triangleleft P$, and so MZ is a subgroup of P which contains M . Since M is maximal, we have either $MZ = M$ or $MZ = P$.

If $MZ = P$, then, as M and Z are both contained in $N_P(M)$, we have $N_P(M) = P$, and so $M \triangleleft P$.

Now suppose that $MZ = M$. Then $Z \triangleleft M$, and the Correspondence Theorem implies that M/Z is a maximal subgroup of the p -group P/Z . Since $Z \neq 1$ (by Theorem 2.9), we have $|P/Z| < |P|$. So, by induction, $M/Z \triangleleft P/Z$. This gives $M \triangleleft P$ by the Correspondence Theorem.

Corollary 2.13 Any maximal subgroup of a finite p -group is of index p .

Proof Let P be a finite p -group, and let M be a maximal subgroup of P . Then $M \triangleleft P$. Since P/M is a nontrivial p -group, it follows via Cauchy's Theorem that P/M has a subgroup of order p . This subgroup must have the form L/M for some $M \triangleleft L \leq P$. But since M is maximal, we must have $L = P$, and so $|P : M| = p$.

We shall now classify all finite abelian p -groups.

Lemma 2.14 Let P be a cyclic p -group, and suppose that $y \in P$ does not generate P . Then y is a p th power in P .

Proof Suppose that $p = \langle x \rangle$. Then P contains a unique subgroup of index p , namely $\langle x^p \rangle$, and this is the unique maximal subgroup of P . Since y does not generate p , $\langle y \rangle$ is contained in a maximal subgroup of P , so $\langle y \rangle \leq \langle x^p \rangle$. Hence $y = x^{pr} = (x^r)^p$ for some r , so y is a p th power.

Theorem 2.15 A finite abelian p -group is a direct product of cyclic p -groups.

Proof Let P be a finite abelian p -group. Then proof proceeds by induction on $|P|$. Assume that $|P| > p$ and that the result is true for abelian p -groups of order $< |P|$. Let Q be a maximal subgroup of P ; then $|P/Q| = p$ by Corollary 2.13. By induction, we have $Q = Q_1 \times Q_2 \times \cdots \times Q_s$, where Q_i is cyclic of order a_i , $i = 1, 2, \dots, s$. Without loss of generality, assume that $a_1 \geq a_2 \geq \cdots \geq a_s \geq 1$.

Suppose that $x \in P - Q$. Since $|P/Q| = p$, we have $x^p \in Q$. Hence $x^p = y_1 y_2 \cdots y_s$, with $y_i \in Q_i$ for each i .

Observation Suppose that for some i and some $x_i \in Q_i$, we have $y_i = x_i^p$. Then $(x x_i^{-1})^p = x^p x_i^{-p} = x^p y_i^{-1} = y_1 y_2 \cdots y_{i-1} y_{i+1} \cdots y_s \in Q$. However, $x x_i^{-1} \notin Q$ since $x \in Q$.

Hence $\exists x \in P - Q$ such that $x^p = y_1 y_2 \cdots y_s$, where each y_i is either a generator of Q_i or is the identity. (See Lemma 2.14.)

If $x^p = 1$, then $p = \langle x \rangle \times Q$, and so P is a direct product of cyclic p -groups.

So we may now assume that $x^p \neq 1$. Then $y_i \neq 1$ for some i . Let $i \leq j \leq s$ be maximal such that $y_j \neq 1$. Then $x^p = y_j y_{j+1} \cdots y_s$ ($y_j \neq 1$). Since P is abelian, the order of $x^p = \text{lcm}$ of the orders of $y_j, y_{j+1}, \dots, y_s = b^{a_j}$. Thus $|\langle x \rangle| = p^{a_j+1}$. Let $\bar{Q} = Q_1 \times Q_2 \times \cdots \times Q_j \times \cdots \times Q_s \leq Q$. Then $|\bar{Q}| = \frac{|Q|}{|Q_j|} = \frac{|Q|}{p^{a_j}}$. Now if $\langle x \rangle \cap \bar{Q} = 1$, then $\langle x \rangle \bar{Q}$ is a direct product of order p^{a_j+1} . $\frac{|Q|}{p^{a_j}} = p|Q| = |P|$, and this would imply that P is a direct product of cyclic p -groups.

Suppose that $x^t \in \langle x \rangle$, $1 \leq t < p^{a_j+1}$. Since $x^p \in Q$ and $x^n \notin Q$ for $1 \leq n < p$, we have that $x^t \in Q$ only if $p \mid t$. So now suppose that $x^t \in Q$ with $t = mp$, with $1 \leq m < p^{a_j}$.

Then $x^t = (x^p)^m = y_j^m y_{j+1}^m \cdots y_s^m$. Now $y_j^m \neq 1$ since $m < p^{a_j} = |\langle y_j \rangle|$. Hence the unique decomposition of x^t in $Q = Q_1 \times Q_2 \times \cdots \times Q_s$ has a non-identity element in the coordinate associated to Q_j .

But \bar{Q} consists precisely of those elements of Q whose unique decomposition in Q has the identity in the Q_j -coordinate. Hence $\langle x \rangle \cap \bar{Q} = 1$.

Proposition 2.16 Suppose that a finite group G is the direct product of its subgroups H_1, H_2, \dots, H_n , where the orders of the H_i s are pairwise coprime. Then any subgroup L of G is the direct product of $L \cap H_1, L \cap H_2, \dots, L \cap H_n$.

Proof Consider the case $n = 2$. (The general case follows by induction.) Set $H = H_1, K = H_2$. So $G = H \times K$, and $(|H|, |K|) = 1$. Suppose that $L \leq G$. Then $L \cap H \triangleleft L, L \cap K \triangleleft L$ since $H \triangleleft G, K \triangleleft G$. Also $(L \cap H) \cap (L \cap K) = 1$, since $H \cap K = 1$. So inside L , we can construct the direct product $(L \cap H) \times (L \cap K)$. Suppose that $g \in L$. Then $g = hk$ for some $h \in H$ and $k \in K$.

To show that $L = (L \cap H) \times (L \cap K)$, it suffices to show that $h, k \in L$. Now h and k are commuting elements of coprime order, and so order of $hk = (\text{order of } h) \times (\text{order of } k)$. So $\langle h \rangle \times \langle k \rangle = \langle hk \rangle$. Since $\langle g \rangle = \langle hk \rangle \leq \langle h \rangle \times \langle k \rangle$, we have $h, k \in \langle g \rangle \leq L$.

Theorem 2.17 The following statements about a finite group G are equivalent:

1. Every Sylow subgroup of G is normal in G .
2. G is the direct product of its Sylow subgroups.
3. Every maximal subgroup of G is normal in G .

Remark A finite group satisfying these equivalent conditions is said to be **nilpotent**. Plainly, all finite abelian groups and all finite p -groups are nilpotent. We'll see an equivalent definition of

nilpotence which extends to infinite groups later.

Proof We shall first show that (1) implies (2). Let p_1, p_2, \dots, p_n be the distinct prime divisors of $|G|$, and let P_i be the Sylow p_i -subgroup of G . By hypothesis, each $P_i \triangleleft G$. It follows easily by induction that $P_1 P_2 \cdots P_i$ is a normal subgroup of G of order $|P_1| |P_2| \cdots |P_i|$ for every i by Proposition 2.7. Hence we have $G = P_1 P_2 \cdots P_n$. Similarly, we have that $|P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_n| = |P_1| |P_2| \cdots |P_{i-1}| |P_{i+1}| \cdots |P_n|$, and so $P_i \cap P_1 P_2 \cdots P_{i-1} P_{i+1} \cdots P_n = \{1\}$ for every i . Hence $G = P_1 \times P_2 \times \cdots \times P_n$.

We shall now show that (2) implies (3). Suppose that (2) holds. Let M be a maximal subgroup of G , and let P_1, P_2, \dots, P_n be the Sylow subgroups of G . (The P_i s are unique by hypothesis.) Proposition 2.16 implies that M is the direct product of the $M \cap P_i$. Since M is maximal in G , it follows that there is exactly one j for which $M \cap P_j$ is maximal in P_j and that $M \cap P_i = P_i$ for all other i . Proposition 2.12 implies that $M \cap P_j \triangleleft P_j$. It follows that $M \triangleleft G$, as required.

Finally, we shall show that (3) implies (1). Suppose that (3) holds. Let P be a Sylow subgroup of G , and suppose that P is not normal in G . Then $P \leq N_G(P) < G$, and so \exists a maximal subgroup M of G such that $P \leq N_G(P) \leq M$. Since P is a Sylow subgroup of M , and $M \triangleleft G$, the Frattini Argument (Theorem 2.6) now gives $G = N_G(P)M \leq M$, which is a contradiction. Thus (3) implies (1).

Corollary 2.18 (The Basis Theorem for Finite Abelian Groups) A finite abelian group is a direct product of cyclic p -groups.

Proof Theorem 2.17 implies that any finite abelian group is a finite product of its Sylow subgroups. By Theorem 2.15, each of these Sylow subgroups is a direct product of cyclic p -groups.

A finite p -group has **normal** subgroups of all possible orders.

Theorem 2.19 Let P be a finite p -group of order p^m . Then P has normal subgroups P_0, P_1, \dots, P_m such that $1 = P_0 \leq P_1 \leq \cdots \leq P_{m-1} \leq P_m = P$, and $|P_i| = p^i$, $0 \leq i \leq m$.

Proof The proof proceeds by induction on m . The result is trivial if $m \leq 1$. So suppose that $m > 1$ and that the result is true \forall p -groups of order $\leq p^{m-1}$. Since P is a p -group, we have $Z(P) \neq 1$ by Theorem 2.9. Choose $z \in Z(P)$ with $z \neq 1$, and suppose that z is of order p^n , $n \geq 0$. Set $P_1 = \langle z^{p^{n-1}} \rangle \leq Z(P)$. Then $|P_1| = p$, and $P_1 \triangleleft P$. Let $\bar{P} = P/P_1$. Then $|\bar{P}| = p^{m-1}$, and so by induction, \bar{P} has normal subgroups \bar{P}_i , $0 < i \leq m-1$ with $1 = \bar{P}_0 \leq \bar{P}_1 \leq \cdots \leq \bar{P}_{m-1} = \bar{P}$, and $|\bar{P}_i| = p^i$ for each i . Now the Correspondence Theorem implies that each \bar{P}_i is of the form P_{i+1}/P_1 , where $P_i \leq P_{i+1} \triangleleft P$. Also, we have $P_1 \leq P_2 \leq \cdots \leq P_m = P$, and for even i , $|P_{i+1}| = |\bar{P}_i| |P_1| = p^{i+1}$. Now (with $P_0 = 1$) the subgroups P_0, P_1, \dots, P_m satisfy the equivalent conditions.

Corollary 2.20 Let G be a finite group, and let p^m be any prime power divisor of the order of G . Then G has a subgroup of order p^m .

Proof Let H be a Sylow p -subgroup of G , with $|H| = p^l$. Then $m \leq l$, and so by Theorem 2.19, H has a subgroup of order p^m .

Chapter 3

Normal Structure

The main theme of this chapter is the examination of a group G through the study of descending series of subgroups of G , in which each term is either normal in G or normal in the preceding term.

Definition 3.1 A **factor** of a group G is a quotient H/K where $H, K \leq G$ and $K \triangleleft H$.

Idea Given a group G , take a chain of subgroups

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}. \quad (\dagger)$$

If $G_i \triangleleft G_{i-1}$ for $i = 1, 2, \dots, r$, the chain is said to be **normal**. In this case, we can look at the factors G_{i-1}/G_i and obtain information about G . Any chain obtained from (\dagger) by inserting further terms is called a **refinement** of (\dagger) . We allow (\dagger) as a refinement of itself, as well as **proper** refinements, where new subgroups are actually inserted.

Assume that (\dagger) is a normal chain. A second normal chain

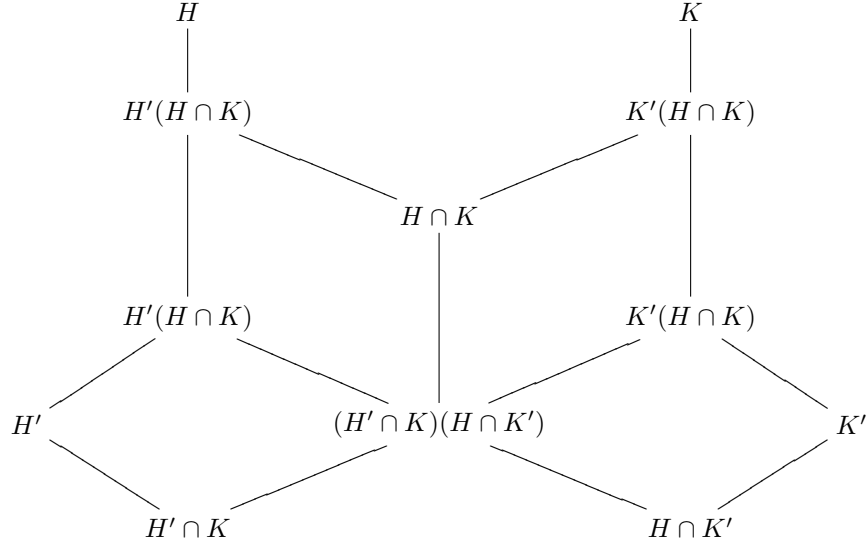
$$G = H_0 \geq H_1 \geq \cdots \geq H_s = \{1\} \quad (\ddagger)$$

is said to be **isomorphic** to (\dagger) if $s = r$ and there is a permutation $i \mapsto i'$ such that $G_{i-1}/G_i \simeq H'_{i-1}/H'_i$. How do we compare different chains in G ? First look at the question of comparing different factors.

Lemma 3.2 (The Zassenhaus Butterfly Lemma) Suppose given a group G and subgroups H, H', K, K' with $H' \triangleleft H$ and $K' \triangleleft K$. Then $K'(H' \cap K) \triangleleft K'(H \cap K)$ and $H'(H \cap K') \triangleleft H'(H \cap K)$, and there are isomorphisms

$$\frac{K'(H \cap K)}{K'(H' \cap K)} \simeq \frac{H \cap K}{(H \cap K')(H' \cap K)} \simeq \frac{H'(H \cap K)}{H'(H \cap K')}.$$

Diagram



Proof Apply the second isomorphism theorem to the subgroups $K', H \cap K$ of K . Since $K' \triangleleft K$ and $K' \cap H \cap K = H \cap K'$, we obtain

$$\frac{K'(H \cap K)}{K'} \simeq \frac{H \cap K}{H \cap K'}.$$

It follows that $H \cap K' \triangleleft H \cap K$. By symmetry, $H' \cap K \triangleleft H \cap K$, and so $(H \cap K')(H' \cap K) \triangleleft H \cap K$.

Now define $f : K'(H \cap K) \rightarrow H \cap K / (H \cap K')(H' \cap K)$ as follows: Suppose $x = k'd \in K'(H \cap K)$ with $k' \in K', d \in H \cap K$. Set $f(x) = d(H \cap K')(H' \cap K)$. We must now show that f is well-defined. Suppose that $x = k'_1 d_1 = k'_2 d_2$ with $k'_1, k'_2 \in K', d_1, d_2 \in H \cap K$. Then $d_1 d_2^{-1} = k'_1 k'^{-1}_2 \in (H \cap K) \cap K' = H \cap K' \leq (H \cap K')(H' \cap K)$. f is plainly surjective. Furthermore $\ker f = K^{-1}(H \cap K^{-1})(H' \cap K) = K(H' \cap K)$. It therefore follows that f induces an isomorphism

$$\frac{K'(H \cap K)}{K'(H' \cap K)} \simeq \frac{H \cap K}{(H \cap K')(H' \cap K)}.$$

By symmetry, we have

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{H \cap K}{(H \cap K')(H' \cap K)}.$$

Remark Given two factors H/H' and K/K' of a group G , the factor $K'(H \cap K)/K'(H' \cap K)$ is sometimes referred to as the projection of H/H' on K/K' . So Lemma 3.2 asserts that the projection of one factor on a second is isomorphic to the projection of the second factor on the first.

Theorem 3.3 (Schreier Refinement Theorem) Any two normal chains in a group G have isomorphic refinements.

Proof The idea is to take two normal chains in G and project their factors onto each other. Suppose we have normal chains

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = 1 \quad (1)$$

$$G = H_0 \geq H_1 \geq \cdots \geq H_s = 1. \quad (2)$$

Set $G_{i,j} = G_i(H_j \cap G_{i-1})$, $i = 1, 2, \dots, r$, $j = 1, 2, \dots, s$. Then $G_{i-1} = G_{i,0} \geq G_{i,1} \geq \cdots \geq G_{i,s} = G_i$ is a normal chain from G_{i-1} to G_i . Putting these pieces together, we get a refinement of (1). Thus

$$G = G_{0,0} \geq G_{0,1} \geq \cdots \geq G_{0,s} = G_{1,0} \geq \cdots \geq G_{r-1,s} = G_{r,0} \geq \cdots \geq G_{r,s} = 1. \quad (3)$$

Similarly the groups $H_{j,i} = H_j(G_i \cap H_{j-1})$, $i = 1, 2, \dots, r$, $j = 1, 2, \dots, s$. Provide a refinement of (2):

$$G = H_{0,0} \geq H_{0,1} \geq \cdots \geq H_{0,r} = H_{1,0} \geq \cdots \geq H_{s-1,r} = H_{s,0} \geq \cdots \geq H_{s,r} = 1. \quad (4)$$

This shows that the chains (3) and (4) are isomorphic.

Definition 3.4 A normal chain in G which has no proper refinements is called a **composition series** of G . Its factors are necessarily simple groups and are called the **composition factors** of G .

Definition 3.5 We say that N is a **maximal normal subgroup** of a group G if $N \triangleleft G$ and there is no proper normal subgroup of G that properly contains N .

Any nontrivial finite group has maximal normal subgroups. The Correspondence Theorem implies that N is a maximal normal subgroup iff G/N is simple.

Note A maximal normal subgroup of G need not be a maximal subgroup of G , e.g. $A_5 \times \mathbb{Z}_2$ has $1 \times \mathbb{Z}_2$ as a maximal normal subgroup that is not maximal.

Proposition 3.6 Finite groups have composition series.

Proof Let G be a finite group. We use induction on $|G|$. If G is simple, then $G \geq 1$ is a composition series of G . Otherwise G has some maximal normal subgroup G_1 , which has a composition series $G_1 \geq G_2 \geq \cdots \geq G_r = 1$, by induction. Since G/G_1 is simple, it follows that $G \geq G_1 \geq \cdots \geq G_r = 1$ is a composition series for G .

Example Infinite groups need not have composition series. For instance, every nontrivial subgroup of the infinite cyclic group \mathbb{Z} is isomorphic to \mathbb{Z} . Since \mathbb{Z} is not simple, it follows that \mathbb{Z} has no simple subgroups. Hence we cannot construct a composition series of \mathbb{Z} since the last nontrivial term of such a series would have to be a simple subgroup of \mathbb{Z} .

Since composition factors are simple groups, in studying arbitrary finite groups, we need a detailed knowledge of finite simple groups.

Theorem 3.7 (Jordan–Hölder Theorem) If a group has a composition series, then any normal chain without repetitions can be refined to a composition series, and any two composition series are isomorphic.

Proof Let G be any group with a composition series. First observe that any refinement of this series reduces to the series itself once we omit repetitions. Now take any normal chain in G_1 and

construct the isomorphic refinements of this chain and this given composition series, which exists by Theorem 3.3. These refinements must be composition series (possibly with repetition).

The Jordan–Hölder Theorem asserts that, up to equivalence, a group has at most one composition series. Hence a group having a composition series has a well–defined collection of composition factors, and understanding these factors provides a framework for understanding the structure of the group.

Example Consider $G = \mathbb{Z}_m$, the additive group of integers (mod m). This is a finite abelian group, and so it has a composition series. Let $m = p_1 p_2 \cdots p_t$, where the p_i s are not necessarily distinct primes, and suppose that $G = \langle x \rangle$. Then $G = \langle x \rangle \geq \langle x^{p_1} \rangle \geq \langle x^{p_1 p_2} \rangle \geq \cdots \geq \langle x^{p_1 p_2 \cdots p_{t-1}} \rangle \geq \langle x^{p_1 p_2 \cdots p_t} \rangle = 1$ is a normal series. The factor groups have prime orders p_1, p_2, \dots, p_t , and so this is a composition series. It follows from the Jordan–Hölder Theorem that the numbers p_1, p_2, \dots, p_t depend only upon m . This gives another proof of the Fundamental Theorem of Arithmetic.

3.1 Soluble Groups

Definition 3.8 A **soluble series** of a group G is a normal series all of whose factor groups are abelian. A group G is **soluble** if it has a soluble series.

Theorem 3.9 Every subgroup H of a soluble group G is soluble.

Proof Let $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$ be a soluble series for G . Consider the series

$$H = H \cap G_1 \geq H \cap G_2 \geq \cdots \geq H \cap G_n = 1. \quad (*)$$

Now $G_{i+1} \triangleleft G_i$, and so $H \cap G_{i+1} = (H \cap G_i) \cap G_{i+1} \triangleleft H \cap G_i$. Also we have $G_i/G_{i+1} \geq G_{i+1}(H \cap G_i)/G_{i+1} \simeq H \cap G_i/H \cap G_i \cap G_{i+1} = H \cap G_i/H \cap G_{i+1}$. Since G_i/G_{i+1} is abelian, it follows that $(H \cap G_i)/(H \cap G_{i+1})$ is also abelian, and hence $(*)$ is a soluble series for H .

Theorem 3.10 Every quotient of a soluble group is soluble.

Proof We shall show that if G is a soluble group, and $f : G \rightarrow H$ is a surjective homomorphism, then H is soluble. Suppose that $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$ is a soluble series of G . Consider the series

$$H = f(G_0) \geq f(G_1) \geq \cdots \geq f(G_n) = 1. \quad (**)$$

Suppose that $f(x_i) \in f(G_i)$. Then $f(x_i)f(G_{i+1})f(x_i)^{-1} = f(x_i G_{i+1} x_i^{-1}) \leq f(G_{i+1})$, since $G_{i+1} \triangleleft G_i$. So $f(G_{i+1}) \triangleleft f(G_i)$ for all i , and so $(**)$ is a normal series for H . Next observe that the map $\varphi : G_i \rightarrow f(G_i)/f(G_{i+1})$ is plainly surjective. Since $G_{i+1} \in \ker \varphi$, φ induces a surjection $G_i/G_{i+1} \rightarrow f(G_i)/f(G_{i+1})$, and so $f(G_i)/f(G_{i+1})$ is a quotient of the abelian group G_i/G_{i+1} and is therefore abelian. Hence $(**)$ is a soluble series for H , and so H is soluble.

Theorem 3.11 If $H \triangleleft G$, and if both H and G/H are soluble, then G is soluble.

Proof Suppose that

$$G/H \geq \overline{K}_1 \geq \overline{K}_2 \geq \cdots \geq \overline{K}_n = 1 \quad (*)$$

is a soluble series for G/H . The Correspondence Theorem tells us that each group \overline{K}_i corresponds to a subgroup K_i of G such that

1. $H \triangleleft K_i$ and $\overline{K}_i \simeq K_i/H$.
2. $K_{i+1} \triangleleft K_i$.
3. $K_i/K_{i+1} \simeq \overline{K}_i/\overline{K}_{i+1}$, and so K_i/K_{i+1} is abelian.

Since H is soluble, it has a soluble series

$$H \geq L_1 \geq L_2 \geq \cdots \geq L_m = 1. \quad (**)$$

Hence the series

$$G \geq K_1 \geq K_2 \geq \cdots \geq K_n = H \geq L_1 \geq L_2 \geq \cdots \geq L_m \geq 1 \quad (***)$$

is a soluble series for G , and so G is soluble.

Corollary 3.12 Suppose that H, K are soluble groups. Then so is $H \times K$.

Proof Set $G = H \times K$; then $H \triangleleft G$, and $G/H \simeq K$. The result follows from Theorem 3.11.

Theorem 3.13 Let G be a finite p -group. Then G is soluble.

Proof Since G is finite, it has a composition series. The composition factors of G are finite simple p -groups and so are cyclic of order p . Hence a composition series for G is a soluble series, and so G is soluble.

Now we will discuss a different approach to soluble groups.

Definition 3.14 Recall that an automorphism of a group G is an isomorphism $\varphi : G \rightarrow G$. A subgroup H of G is said to be **characteristic in G** (written $H \text{ char } G$) if $\varphi(H) = H$ for every automorphism φ of G . Equivalently, $H \text{ char } G$ iff $\varphi(H) \leq H$ for every φ .

For each $g \in G$, conjugation $x \mapsto g^{-1}xg$ is an automorphism of G . Hence every characteristic subgroup of G is normal.

Definition 3.15 Let G be a group, and $x, y \in G$. The expression $[x, y] = x^{-1}y^{-1}xy$ is called the **commutator** of x and y . Clearly $[x, y] = 1$ iff x, y commute since $xy = yx[x, y]$.

Lemma 3.16 Let G be a group, and $x, y \in G$. Then **any** group homomorphism $f : G \rightarrow H$ maps $[x, y]$ to $[f(x), f(y)]$. In particular, if H is abelian, then $[x, y] \in \ker f$.

Proof Obvious.

Consider the subgroup G' of G generated by all commutators in G . This is called the **commutator subgroup** or the **derived group** of G .

Lemma 3.16 implies that $G' \text{ char } G$, and so in particular, $G' \triangleleft G$. The quotient G/G' is abelian since $xy = yx[x, y] \forall x, y \in G$ and is sometimes written as G^{ab} . The group G^{ab} is often called the

abelianization of G or the group G made abelian.

Remark Suppose that A is an abelian group, and let $f : G \rightarrow A$ be any homomorphism. Lemma 3.16 implies that $G' \leq \ker f$, and so f induces a homomorphism $\bar{f} : G^{ab} \rightarrow A$.

Definition 3.17 The **higher commutator subgroups** of G are defined inductively by $G^{(0)} = G$, $G^{(i+1)} = G^{(i)'}$. The series $G \geq G^{(0)} \geq G^{(1)} \geq \dots$ is called the **derived series of G** . Notice that the derived series has abelian factors.

Lemma 3.18

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

Proof

1. Suppose that φ is an automorphism of G . Then $\varphi|_K$ is an automorphism of K , and so $\varphi(H) = (\varphi|_K)(H) = H$. Hence $H \text{ char } G$.
2. For each $g \in G$, conjugation by G gives an automorphism of K since $K \triangleleft G$. This automorphism of K sends H to itself since $H \text{ char } K$. Hence $g^{-1}Hg = H \forall g \in G$, i.e. $H \triangleleft G$.

Corollary 3.19 For every group G , the higher commutator subgroups $G^{(i)}$ are characteristic subgroups of G , and so $G^{(i)} \triangleleft G \forall i \geq 0$.

Proof The proof proceeds via induction on i . We've seen that the result is true for $i = 1$. Now $G^{(i+1)} = G^{(i)'}$ is a characteristic subgroup of $G^{(i)'}$ is a characteristic subgroup of $G^{(i)}$, and by induction we may assume that $G^{(i)} \text{ char } G$. Hence $G^{(i+1)} \text{ char } G$ via Lemma 3.18.

Corollary 3.19 implies that **if** the derived series $G = G^{(0)} \geq G^{(1)} \geq \dots$ terminates in 1, **then** it is a normal series.

Lemma 3.20 Suppose that G is soluble and that $G = G_0 \geq G_1 \geq \dots \geq G_n = 1$ is a soluble series for G . Then $G^{(i)} \leq G_i \forall i$.

Proof The proof is via induction on i . If $i = 0$, then $G_0 = G = G^{(0)}$. Now suppose that the result is true for all $0 \leq i \leq j$, and consider the natural map $\nu_j : G_j \rightarrow G_j/G_{j+1}$. Since G_j/G_{j+1} is abelian, Lemma 3.16 implies that $G_j' \leq \ker(\nu_j) = G_{j+1}$. By induction, $G^{(j)} \leq G_j$, and so $G^{(j)'} = G^{(j+1)} \leq G_{j+1}$.

Theorem 3.21 A group G is soluble iff $G^{(n)} = 1$ for some n .

Proof Let $G = G_0 \geq G_1 \geq \dots \geq G_n = 1$ be a soluble series for G . Lemma 3.20 implies that $G^{(i)} \leq G_i \forall i$; in particular, $G^{(n)} \leq G_n = 1$, and so $G^{(n)} = 1$. Conversely, if $G^{(n)} = 1$, then the derived series of G is a normal series. Since the derived series has abelian factors, it is a soluble series for G .

Corollary 3.22 A group G is soluble iff its derived series is a normal series.

Let us reprove some of our earlier theorems.

Theorem 3.9 Every subgroup H of a soluble group G is soluble.

Proof Suppose that $H \leq G$. Then $H^{(i)} \leq G^{(i)} \forall i$. Hence $G^{(n)} = 1$, and so $H^{(n)} = 1$, so H is soluble.

Theorem 3.10 Every quotient of a soluble group is soluble.

Proof Again we show that if G is soluble, and $f : G \rightarrow H$ is a surjective homomorphism, then H is soluble. Since f is surjective, $f(G^{(i)}) = f(G)^{(i)} = f |^{(i)}$. Hence if $G^{(n)} = 1$, then $H^{(n)} = 1$, so H is soluble.

Theorem 3.11 If $H \triangleleft G$, and if both H and G/H are soluble, then G is soluble.

Proof Set $K = G/H$, and let $\nu : G \rightarrow K$ be the natural quotient map. Suppose that $K^{(n)} = 1$. Then $\nu(G^{(n)}) \leq K^{(n)} = 1$. This implies that $G^{(n)} \leq H$. If $H^{(m)} = 1$, then we have $G^{(n)(m)} \leq H^{(m)} = 1$. However, $G^{(m)(n)} = G^{(m+n)}$, and so G is soluble.

Definition 3.23 Let H be a normal subgroup of G . Then H is said to be a **minimal normal subgroup** if $H \neq 1$, and there is no normal subgroup K of G with $1 < K < H$.

Nontrivial finite groups always have minimal normal subgroups.

Theorem 3.24 Let G be a finite soluble group. Then every minimal normal subgroup of G is elementary abelian, i.e. isomorphic to the direct product of cyclic groups of order p for some prime p .

Proof Let H be a minimal normal subgroup of G . If K is any characteristic subgroup of H , then $K \triangleleft G$ by Lemma 3.18(ii). Since H is minimal, this implies that either $K = H$ or $K = 1$. Now H' char H , and so either $H' = 1$ or $H' = H$. Since G is soluble, so is H , and therefore we must have $H' = 1$ from Theorem 3.21. Hence H is abelian.

Now suppose $p \mid |H|$, where p is a prime. Then $K = \{x \in H \mid x^p = 1\}$ char H . Hence $H = K$, and so H is elementary abelian.

Definition 3.25 A group G is said to be **characteristically simple** if its only characteristic subgroups are G and 1 .

Theorem 3.26 Every finite characteristically simple group G is either simple or the direct product of finite simple groups.

Proof Let H be a normal subgroup of G whose order is minimal amongst all nontrivial normal subgroups (so H is minimal). Set $H = H_1$. Consider all subgroups of G of the form $H_1 \times H_2 \times \cdots \times H_n$, with $n \geq 1$, with $H_i \triangleleft G$, and $H_i \simeq H$. Let M be such a subgroup of largest possible order. We claim that M char G , and so $M = G$. It suffices to show that $\varphi(H_i) \leq M$ for every i and for all automorphisms φ of G . First observe that $\varphi(H_i) \triangleleft G$: if $g \in G$, then $g = \varphi(g')$ for some $g' \in G$, so $g\varphi(H_i)g^{-1} = \varphi(g'H_i g'^{-1}) = \varphi(H_i)$ since $H_i \triangleleft G$. Next, note that if $\varphi(H_i) \not\leq M$, then $\varphi(H_i) \cap M \neq \varphi(H_i)$, and so $|\varphi(H_i) \cap M| < |\varphi(H_i)| = |H|$. Since $\varphi(H_i) \cap M \triangleleft G$, and H is

minimal, it follows that $\varphi(H_i) \cap M = 1$. Hence $M \times \varphi(H_i)$ is a subgroup of G of the same type as M but of larger order, which is a contradiction. Therefore $M \text{ char } G$, and so $M = G$. If N is a nontrivial normal subgroup of H , then $|N| < |H|$, and N is a nontrivial normal subgroup of $M = H_1 \times H_2 \times \cdots \times H_n = G$. This contradicts the minimal choice of H , so H is simple.

Corollary 3.27 Let H be a minimal normal subgroup of a finite group G . Then either H is simple, or H is a direct product of isomorphic simple groups.

Proof Suppose that $N \text{ char } H$. Then $N \triangleleft G$ by Lemma 3.18(ii), and so $N = 1$ or $N = H$ since H is a minimal normal subgroup. Hence H is characteristically simple. Now the result follows from Theorem 3.26.

We shall now describe some generalizations of Sylow's theorems that characterize finite soluble groups.

Theorem 3.28 (P. Hall) Let G be a soluble group of order mn , with $(m, n) = 1$. Then G contains a subgroup of order m , and any two subgroups of order m are conjugate.

Proof The proof proceeds via induction on $|G|$. There are two cases to consider.

Case 1: G has a nontrivial normal subgroup of order m_1n_1 , where $m_1 \mid m$, $n_1 \mid n$, and $n_1 < n$.

Case 2: All nontrivial normal subgroups of G have orders of the form m_1n , where $m_1 \mid m$.

Case 1: Suppose that $K \triangleleft G$, with $|K| = m_1n_1$. Then $|G/K| = \frac{mn}{m_1n_1} = \left(\frac{m}{m_1}\right)\left(\frac{n}{n_1}\right) < mn$, and G/K is soluble. Therefore by induction, G/K has a subgroup S/K with $|S/K| = m/m_1$. Now $|S| = |S/K||K| = \frac{m}{m_1}m_1n_1 = mn_1 < mn$, and S is soluble. Therefore by induction, S has a subgroup of order m , and therefore G has a subgroup of order m .

Now we must prove conjugation. Suppose $M_1, M_2 \leq G$, with $|M_1| = |M_2| = m$. Consider M_iK/K ($i = 1, 2$). We have $M_iK/K \simeq M_i/M_i \cap K$ by the Second Isomorphism Theorem. Now $M_i \cap K \leq K$, and so $|M_i \cap K| \mid m_1$, and so $|M_i \cap K| = m_1/\alpha_i$. Therefore $|M_iK/K| = m \frac{\alpha_i}{m_1}$. Lagrange's Theorem implies that $|M_iK/K| \mid |G/K|$, i.e. $\frac{mn}{m_1n_1} \frac{m_1}{m\alpha_i} = \frac{n}{n_1} \frac{1}{\alpha_i}$ is an integer. Since $\alpha_i \mid m_1$ and $(m_1, n/n_1) = 1$, it follows that $\alpha_i = 1$. Thus $|M_iK/K| = \frac{m}{m_1}$. Now G/K is soluble, and so by induction, it follows that the groups $M_1K/K, M_2K/K$ are conjugate in G/K , i.e. $\exists x \in G$ such that $M_1K/K = (xK)M_2K/K(xK)^{-1}$ implies $M_1K = xM_2Kx^{-1}$ (via the Correspondence Theorem). Hence $xM_2x^{-1} \leq M_1K$. Since M_1K is soluble with $|M_1K| < mn$, (in fact $|M_1K| = \frac{m}{m_1}m_1n_1 < mn$) it follows by induction that M_1, xM_2x^{-1} are conjugate in M_1K . Therefore M_1, M_2 are conjugate in G . Case 2: Suppose that all nontrivial normal subgroups of G have orders of the form m_1n , where $m_1 \mid m$. Let K be a nontrivial minimal normal subgroup of G . Since G is soluble, K is elementary abelian by Theorem 3.24. Hence $|K| = p^\alpha$ for some prime p . This implies that $n = p^\alpha$, and so K is a Sylow p -subgroup for some prime p .

Since all Sylow p -subgroups are conjugate, K is the unique minimal normal subgroup of G . Furthermore, since, by hypothesis, all nontrivial normal subgroups of G have orders of the form m_1p^α (with $m_1 \mid m$), K is contained in any nontrivial normal subgroup of G . Now since G/K is soluble, it has a minimal normal subgroup L/K with $|L/K| = q^\beta$ with $p \neq q$ and $\beta > 0$. Thus $|L| = q^\beta|K| = p^\alpha q^\beta$, and we have $L \triangleleft G$ via the Correspondence Theorem.

Sylow's Theorem implies that L has a subgroup Q with $|Q| = q^\beta$. Plainly $L = KQ$ since $|KQ| = p^\alpha q^\beta$. The Frattini Argument (Theorem 2.6) implies that $G = LN_G(Q) = KQN_G(Q) = KN_G(Q)$. Consider $D = K \cap N_G(Q)$. Since K is the unique minimal normal subgroup of G , it is a characteristic subgroup of G . Furthermore $D \triangleleft K$ since K is abelian. Thus $D \triangleleft G$ by Lemma 3.18(2). Since K is minimal, either $D = K$ or $D = 1$. If $D = K$, then $G = KN_G(Q) = N_G(Q)$. Thus $Q \triangleleft G$. Since $|Q| = q^\beta$, this contradicts the hypothesis that all nontrivial normal subgroups of G have orders of the form $m_1 n$, where $m_1 \mid m$. Therefore $D = 1$, i.e. $G = KN_G(Q)$, with $K \cap N_G(Q) = 1$. So $|N_G(Q)| = m$, and this is what we want.

Now we must prove conjugacy. Let M be any other subgroup of G of order m . Consider the subgroup LM of G . $|LM|$ is divisible by $|L| = p^\alpha q^\beta$. $|LN|$ is divisible by $|M| = m$. Hence, since $(p, m) = 1$, $|LM|$ is divisible by $p^\alpha m = |G|$. So $LM = G$. Thus $G/L \simeq LM/L \simeq M/M \cap L$. Hence $\frac{mp^\alpha}{p^\alpha q^\beta} = \frac{m}{|M \cap L|}$, which implies that $|M \cap L| = q^\beta = |Q|$. Therefore by induction $M \cap L$ and Q are conjugate in L . Thus $N_G(M \cap L)$ and $N_G(Q)$ are conjugate in G . Thus $|N_G(M \cap L)| = |N_G(Q)| = m$. But $m \leq N_G(M \cap L)$ since $L \triangleleft G$, and so $M = N_G(M \cap L)$ since $|M| = m$. Thus M and $N_G(Q)$ are conjugate in G .

Definition 3.29 Let G be a finite group. A **Hall subgroup** of G is a subgroup H such that $(|H|, |G : H|) = 1$.

If π is any set of primes, then a **π -number** is an integer n all of whose prime factors lie in π . The complement of π is written π' .

Definition 3.30 Let π be a set of primes. A group G is a **π -group** if the order of each of its elements is a π -number. G is a **π' -group** if the order of each of its elements is a π' -number.

Remarks

1. Every Sylow p -subgroup of a finite group is a Hall p -group.
2. Theorem 3.28 says that Hall π -groups always exist in finite soluble groups.

Definition 3.31 Let G be a finite group of order ap^n , where p is a prime, and $p \nmid a$. A **p -complement** in G is a subgroup of order a . Suppose that $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where the p_i s are distinct primes, and let S_1, S_2, \dots, S_k be subgroups of G with $|G : S_i| = p_i^{\alpha_i}$. The set $\{S_1, S_2, \dots, S_k\}$ is called a system of complements for G . So Theorem 3.28 implies that every finite soluble group has a system of complements.

Lemma 3.32 Let G be a finite group, and suppose that $N \triangleleft G$. Let H be a p -complement in G . Then $H \cap N$ is a p -complement in N , and HN/N is a p -complement in G/N .

Proof Clearly $(|H \cap N|, p) = 1$ since $(|H|, p) = 1$ and $|H \cap N| \mid |H|$. Now $|HN| = \frac{|H||N|}{|H \cap N|}$ implies that $\frac{|HN|}{|H|} = \frac{|N|}{|H \cap N|}$. Since $N \triangleleft G$, we have $HN \leq G$, and so $|HN| \mid |G|$. This implies that $|HN|/|H|$ is a power of p since the same is true of $|G|/|H|$. Hence $|N : H \cap N|$ is a power of p , and it follows that $H \cap N$ is a p -complement in N . Now consider G/N . The Correspondence Theorem implies that $|G/N : HN/N| = |G : H|$ is a power of p . Also $|HN/N| = |H/H \cap N|$, which is coprime to p . Thus HN/N is a p -complement in G/N .

Theorem 3.33 (Burnside's $p^\alpha q^\beta$ Theorem) Let G be a group of order $p^\alpha q^\beta$, where p and q are

primes. Then G is soluble.

Theorem 3.34 (Hall's Criterion for Soluble Groups) Let G be a finite group of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (p_1, p_2, \dots, p_k distinct primes). Suppose that G has a system of complements S_1, S_2, \dots, S_k with $|G : S_1| = p_i^{\alpha_i}$. Then G is soluble.

Remark Hence every finite group with a system of complements is soluble, and every finite soluble group has a system of complements.

Proof The proof proceeds by induction on $|G|$. If $k = 1$, then G is a p -group and so is soluble (Theorem 3.13). If $k = 2$, then G is soluble by Burnside's $p^\alpha q^\beta$ Theorem (Theorem 3.33). Hence we may assume that $k \geq 3$.

Now consider the product $S_1 S_i$ ($i \neq 1$). We have $|S_1 S_i| = \frac{|S_1||S_i|}{|S_1 \cap S_i|}$. Hence $|S_1| \mid |S_1 S_i|$ and $|S_i| \mid |S_1 S_i|$. This implies that $p_j^{\alpha_j} \mid |S_1 S_j|$ for all j , and so $S_1 S_i = G$. Furthermore,

$$|S_1 \cap S_i| = \frac{|S_1||S_i|}{|S_1 S_i|} = \frac{|S_1||S_i|}{|G|} = p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}. \quad (*)$$

Hence $\{S_1 \cap S_i : i \neq 1\}$ is a system of complements for S_1 . It now follows by induction that S_1 is soluble.

Now let $N \triangleleft S_1$ be a minimal normal subgroup. Then N is elementary abelian (Theorem 3.24). Without loss of generality, we may assume that $|N| = p_2^b$, say. From (*), we have that $|S_1 \cap S_3| = p_2^{\alpha_2} p_4^{\alpha_4} p_5^{\alpha_5} \cdots p_k^{\alpha_k}$. Hence Sylow's Theorem implies that there exists a subgroup Q of $S_1 \cap S_3$ with $|Q| = p_2^{\alpha_2}$. Since $N \triangleleft S_1$, N is contained in every Sylow p_2 -subgroup of S_1 . Hence $N \leq Q$. Consider $M = \langle N^g = g^{-1} N g \mid g \in G \rangle$. Then $1 < M \triangleleft G$. We now claim that M is a proper subgroup of G . To prove this claim, recall that $G = S_1 S_3$. If $g \in G$ with $g = S_1 S_3$ ($s_i \in S_i$), then $N^g = N^{s_1 s_3} = N^{s_3} \leq S_3$. Hence $M \leq S_3$ (and in fact $M \triangleleft S_3$). Thus M is a nontrivial proper normal subgroup of G . Now Lemma 3.47 implies that $\{S_i \cap M_i \mid 1 \leq i \leq k\}$ is a system of complements for M , and $\{S_i M/M : 1 \leq i \leq k\}$ is a system of complements for G/M . Now, by induction, M and G/M are soluble. This implies that G is soluble by Theorem 3.11.

Theorem 3.35 (Feit–Thompson) Every finite group of odd order is soluble.

Proof *Pacific Journal of Mathematics* 13 (1963) 775–1029.

3.2 Some Finite Simple Groups

3.2.1 Alternating Groups

A_2, A_3 are simple since they are cyclic of prime order. A_4 contains a subgroup of order 4 consisting of all permutations of type $(2, 2)$. Hence A_4 is not simple.

Lemma 3.36

1. The alternating group A_n is generated by the totality of 3-cycles.

2. If $n \geq 5$, then A_n is generated by the totality of permutations of type $(2, 2)$.

Proof

1. A_n is generated by elements which are the products of two transpositions, and we have $(ab)(ac) = (abc)$ and $(ab)(cd) = (abc)(cad)$.
2. If $n \geq 5$, then for any given (abc) , we can find d, e such that $(abc) = ((ab)(de))((de)(ac))$.

Theorem 3.37 If $n \geq 5$, then any nontrivial normal subgroup N of S_n contains A_n .

Proof We first observe that N contains a permutation $\sigma \neq 1$. Choose $i \in \{1, 2, \dots, n\}$ such that $\sigma(i) \neq i$. Then the transposition $\tau = (i, j)$ ($j \neq 1, \sigma(i)$) does not commute with σ .

The element $p = [0, 1] = \sigma\tau\sigma^{-1}\tau^{-1}$ is an element of N and is the product of three transpositions. Thus p is either a 3-cycle or of type $(2, 2)$. Since permutations of the same type are conjugate in S_n , it follows that N either contains all 3-cycles or all permutations of type $(2, 2)$. Thus $A_n < N$.

Theorem 3.38 If $n \geq 5$, then A_n is simple.

Proof Let N be a proper normal subgroup of A_n . Suppose that τ is any transposition in S_n . Then, since $S_n = \langle A_n, \tau \rangle$, Lemma 3.36 implies that $\tau N \tau^{-1} \neq N$. Now the groups $\langle N, \tau N \tau^{-1} \rangle$ and $N \cap \tau N \tau^{-1}$ are normal subgroups of A_n that are invariant under conjugation by τ . Hence Lemma 3.36 implies that $A_n = N(\tau N \tau^{-1})$, and $N \cap \tau N \tau^{-1} = \{1\}$. It follows therefore that $A_n \simeq N \times \tau N \tau^{-1}$. Thus $|A_n| = |N|^2$, and N is even (since $N \geq 5$). Sylow's Theorem implies that N contains an element σ of order 2. Hence σ is a product of disjoint transpositions, and so σ commutes with some transposition ρ , say. This implies that $\sigma \in N \cap \rho N \rho^{-1}$, which is a contradiction.

3.2.2 Groups of Order 168

Proposition 3.39 All groups of order properly dividing 168 are soluble.

Proof Recall that a group is soluble iff it has Hall subgroups of all possible orders. $168 = 2^3 \cdot 3 \cdot 7$. Sylow's Theorem implies that subgroups of order $2^\alpha \cdot 3$, $2^\alpha \cdot 7$, and $3 \cdot 7$ ($\alpha = 1, 2$, or 3) satisfy the above criterion and so are soluble. Thus the only cases left are subgroups of order $2 \cdot 3 \cdot 7$ or $2^2 \cdot 3 \cdot 7$. Sylow's Theorem implies that any subgroup G_1 of order $2 \cdot 3 \cdot 7$ has precisely one subgroup G_7 of order 7. Now G_7 is soluble, and $|G_1/G_7| = 6$, so G_1/G_7 is soluble. Similarly, Sylow's Theorem implies that any group G_2 of order $2^2 \cdot 3 \cdot 7$ has a normal subgroup G_7 of order 7. Now $|G_2/G_7| = 12 = 2^2 \cdot 3$, and Sylow's Theorem implies that any group of order 12 contains subgroups of orders 4 and 3 and so is soluble by Hall's Criterion. Hence G_2 is soluble.

Corollary 3.40 Every group of order 168 is either soluble or simple.

Proof Suppose that $|G| = 168$ with $1 < N \triangleleft G$. Then $|G/N| \mid 168$ and $|N| \mid 168$. Hence both N and G/N are soluble and so G is soluble. Thus every group of order 168 is either soluble or simple.

Remark The group $GL_3(\mathbb{F}_2)$ is simple. $|GL_3(\mathbb{F}_2)| = 168$.

3.3 Central Series and Nilpotent Groups

Definition 3.41 Suppose that $H, K \leq G$. Then $[H, K] = \langle [h, k] : h \in H, k \in K \rangle$, where $[h, k] = hkh^{-1}k^{-1}$.

Remark

1. Suppose that $H, K \leq G$. We say that K normalizes H if $K \leq N_G(H)$. K normalizes H iff $[H, K] \leq H$.
2. If $H \leq G$, recall that the centralizer of H in G is $C_G(H) = \{x \in G \mid xh = hx \forall h \in H\}$, i.e. $C_G(H) = \{x \in G \mid [x, h] = 1 \forall h \in H\}$. Say that $K \leq G$ **centralizes** H if $K \leq C_G(H)$. Then K centralizes H iff $[H, K] = 1$.
3. Suppose that $x, y \in G$, and $K \triangleleft G$. Suppose also that $[x, y] \in K$. Then $xKyK = yKxK$ in G/K .

Lemma 3.42

1. If $K \triangleleft G$ and $K \leq H \leq G$, then $[H, G] \leq K$ iff $H/K \leq Z(G/K)$.
2. If $H, K \leq G$ and $f : G \rightarrow L$ is a homomorphism, then $f([H, K]) = [f(H), f(K)]$.
3. Let H, J, K be normal subgroups of G such that $J \leq H$. Suppose that $H/J \leq Z(G/J)$. Then $HK/JK \leq Z(G/JK)$.

Proof

1. Suppose that $h \in H$ and $g \in G$. Then $hKgK = gKhK$ iff $[h, g]K = K$ iff $[H, G] \in K$.
2. Both $f([H, K])$ and $[f(H), f(K)]$ are generated by all elements of the form $f([h, k]) = [f(h), f(k)]$, $h \in H, k \in K$.
3. We use (1) above. Since $H/J \leq Z(G/J)$, we have $[H, G] \leq J$. Next, observe that $[HK, G] = [KH, G]$. Suppose that $g \in G, h \in H, k \in K$. Then $[kh, g] = (kh)g(kh)^{-1}g^{-1} = khgh^{-1}g^{-1}gk^{-1}g^{-1} = kjgkjg^{-1}$ (for some $j \in J$ since $[H, G] \leq J$) $= kjk_1$ (since $K \triangleleft G$) $= j_1k_2k_1$ (since $KJ = JK$) $\in JK$. Hence $[KH, G] = [HK, G] \leq JK$, and so (from (1) above) we have $HK/JK \leq Z(G/JK)$ as asserted.

Definition 3.43 A normal series $G = G_1 \geq G_2 \geq \dots \geq G_n = 1$ with each $G_i \triangleleft G$, and $G_i/G_{i+1} \leq Z(G/G_{i+1})$ is called a **central series**. The factors G_i/G_{i+1} are called **central factors**. The group G is said to be **nilpotent** if it has a central series.

Example A central series is certainly a soluble series, and therefore all nilpotent groups are soluble. Soluble groups are not necessarily nilpotent. Let $G = S_3$, and let $K \leq G$ be the unique subgroup of G of order 3. Then $G \geq K \geq 1$ is a soluble series for G , and so G is soluble. On the other hand, $Z(S_3) = 1$, and so S_3 cannot have a central series, so S_3 is nilpotent.

Amongst all the central series of a nilpotent group, there is one which descends most rapidly and one which ascends most rapidly.

Definition 3.44 Define subgroups $\gamma_i(G)$ by induction as follows: $\gamma_1(G) = G$, $\gamma_{i+1}(G) = [\gamma_i(G), G]$. It is clear (by induction) that $\gamma_{i+1}(G) \text{ char } G \forall i$ (and so in particular $\gamma_i(G) \triangleleft G$). Furthermore,

if $x \in \gamma_{i-1}(G)$ and $g \in G$, then $xgx^{-1}g^{-1} = x(gx^{-1}g^{-1}) \in \gamma_{i-1}(G)$. This implies that $\gamma_{i+1}(G) \leq \gamma_i(G)$. Also, since $\gamma_{i+1}(G) = [\gamma_i(G), G]$, it follows from Lemma 3.42(1) that $\gamma_i(G)/\gamma_{i+1}(G) \leq Z(G/\gamma_{i+1}(G))$.

Definition 3.45 The **lower central series** of G is the series $G = \gamma_1(G) \geq \gamma_2(G) \geq \dots$. (Note that this series may not reach 1 and so need not be a normal series.)

Definition 3.46 Define subgroups $\zeta^i(G)$ by induction as $\zeta^0(G) = 1$, $\zeta^{i+1}(G)/\zeta^i(G) = Z(G/\zeta^i(G))$.

Exercise Prove (by induction) that $\zeta^i(G) \text{ char } G$ (and so in particular $\zeta^i \triangleleft G$).

If $\nu_i : G \rightarrow G/\zeta^i(G)$ is the natural map, then $\zeta^{i+1}(G)$ is the inverse image of the center of $G/\zeta^i(G)$. The groups $\zeta^i(G)$ are called the **higher centers of G** . We have $\zeta^0(G) = 1$, $\zeta^1(G) = Z(G)$, $\gamma_2(G) = G'$. However, $\gamma_3(G) \neq G''$ in general. We shall frequently write ζ^i for $\zeta^i(G)$ and γ_i for $\gamma_i(G)$.

Theorem 3.47

1. The following are equivalent:

- (a) G is nilpotent.
- (b) $\gamma_n(G) = 1$ for some integer n .
- (c) $\zeta^n(G) = G$ for some integer n .
- (d) $\zeta^n(G) = G$ for some integer n .

2. Suppose that G is nilpotent. Then for any central series $1 = G_0 \leq G_1 \leq \dots \leq G_r = G$, we have $\gamma_{r-i+1}(G) \leq G_i \leq \zeta^i(G)$ for each $i = 0, 1, 2, \dots, r$. Furthermore, the least integer i such that $\gamma_{i+1}(G) = 1$ is equal to the least integer i such that $\zeta^i(G) = G$. This integer i is called the **class** of the nilpotent group G .

Proof If $\gamma_n(G) = 1$ for some n , then $G = \gamma_1(G) \geq \gamma_2(G) \geq \dots \geq \gamma_n(G) = 1$ is a central series of G , and so G is nilpotent. Similarly if $\zeta^n(G) = G$ for some n , then $1 = \zeta^0(G) \leq \zeta^1(G) \leq \dots \leq \zeta^n(G) = G$ is a central series of G , and so G is nilpotent.

Now suppose conversely that G is nilpotent, and let $1 = G_0 \leq G_1 \leq \dots \leq G_r = G$ be a central series of G . We first prove by induction on i that $G_i \leq \zeta^i(G)$ for each $i = 0, 1, 2, \dots, r$. This is trivial for $i = 0$. Assume that $i > 0$ and inductively that $G_{i-1} \leq \zeta^{i-1}(G)$. Then $G_{i-1}\zeta^{i-1}(G) = \zeta^{i-1}(G)$. By hypothesis, $G_i/G_{i-1} \leq Z(G/G_{i-1})$. Now apply Lemma 3.42(3) (with $H = G_i$, $J = G_{i-1}$, $K = \zeta^{i-1}(G)$). This yields

$$\frac{G_i\zeta^{i-1}(G)}{\zeta^{i-1}(G)} \leq Z\left(\frac{G}{\zeta^{i-1}(G)}\right) = \frac{\zeta^i(G)}{\zeta^{i-1}(G)}.$$

Hence $G_i \leq \zeta^i(G)$, and so the result follows by induction. In particular, since $G = G_r \leq \zeta^r(G)$, we have $\zeta^r(G) = G$.

Next, we prove by induction on j that $\gamma_{j+1}(G) \leq G_{r-j}$ for each $j = 0, 1, 2, \dots, r$. This is trivial for $j = 0$. Assume that $j > 0$ and that $\gamma_j(G) \leq G_{r-j+1}$. Since $G_{r-j+1}/G_{r-j} \leq Z(G/G_{r-j})$,

by hypothesis, Lemma 3.42(1) implies that $[G_{r-j+1}, G] \leq G_{r-j}$. Hence $\gamma_{j+1}(G) = [\gamma_j(G), G] \leq [G_{r-j+1}, G] \leq G_0 = 1$, we have $\gamma_{r+1}(G) = 1$. So we've shown that

$$\gamma_{r-i+1}(G) \leq G_i \leq \zeta^i(G) \quad (*)$$

for each $i = 0, 1, 2, \dots, r$. Now let c be the smallest integer i such that $\zeta^i(G) = G$. Then for a central series, we may choose $G_i = \zeta^i(G)$ and $r = c$. Then $(*)$ implies that $\gamma_{c+1}(G) \leq G_0 = 1$, i.e. $\gamma_{c+1}(G) = 1$.

We claim that if $c > 0$, then $\gamma_i(G) \neq 1$. Suppose on the contrary that $\gamma_c(G) = 1$. Then for a central series, we may choose $G_i = \gamma_{c-i}(G)$ for $i = 0, 1, 2, \dots, c-1$ and $r = c-1$. By then $(*)$ implies that $G_{c-1} = G \leq \zeta^{c-1}(G)$, i.e. $\zeta^{c-1}(G) = G$, and this contradicts the definition of c . Hence $\gamma_c(G) \neq 1$, and c is also the least integer such that $\gamma_{c+1}(G) = 1$.

Theorem 3.48 Every finite p -group is nilpotent.

Proof If P is a nontrivial finite p -group, then $Z(P) \neq 1$ by Theorem 2.9. Suppose that for some i , $\zeta^i(P) < P$. Then $Z(P/\zeta^i(P)) \neq 1$, and so $\zeta^i(P) < \zeta^{i+1}(P)$. Since P is finite, we have $\zeta^i(P) = P$ for some i , and so P is nilpotent.

Theorem 3.49 Suppose that G is a nontrivial nilpotent group. Then $Z(G) \neq 1$.

Proof Suppose that G is nilpotent of class c , so $\gamma_{c+1}(G) = 1$, $\gamma_c(G) \neq 1$. Then Theorem 3.47(2) tells us that $\gamma_c(G) \leq \zeta^1(G) = Z(G)$. Hence $Z(G) \neq 1$.

Theorem 3.50

1. Every subgroup H of a nilpotent group G is nilpotent. If G is nilpotent of class c , then H is nilpotent of class $\leq c$.
2. If G is nilpotent of class c , and $H \triangleleft G$ then G/H is also nilpotent of class $\leq c$.
3. If H, K are nilpotent (of classes c and d , respectively), then $H \times K$ is nilpotent.

Proof

1. Plainly $H \leq G$ implies that $\gamma_i(H) \leq \gamma_i(G) \forall i$. Hence if $\gamma_{c+1}(G) = 1$, then $\gamma_{c+1}(H) = 1$ also, and so H is nilpotent.
2. Let $\nu : G \rightarrow G/H$ be the natural quotient map. Then $\gamma_i(G/H) = \nu(\gamma_i(G))$ from Lemma 3.42(2). Hence if $\gamma_{c+1}(G) = 1$, then $\gamma_{c+1}(G/H) = 1$ also, and so G/H is nilpotent.

[**Remark:** It is not true that if $H \triangleleft G$, with both H and G/H nilpotent, then G is nilpotent, e.g. take $G = S_3$.]

3. We have $\gamma_i(H \times K) \leq \gamma_i(H) \times \gamma_i(K)$. Hence if $M = \max\{c, d\}$, then $\gamma_{M+1}(H \times K) = 1$, so $H \times K$ is nilpotent.

Definition 3.51 Suppose that G is a group. Then G is said to satisfy the **normalizer condition** if $H < N_G(H)$ for all proper subgroups H of G .

Theorem 3.52 Let G be a nilpotent group. Then G satisfies the normalizer condition.

Proof Observe that the lower central series of G is a descending series of subgroups, starting with G and ending at 1. This implies that there is an integer i such that $\gamma_{i+1}(G) \leq H$ and $\gamma_i(G) \not\leq H$. Then $[\gamma_i(G), H] \leq [\gamma_i(G), G] = \gamma_{i+1}(G) \leq H$. Hence $\gamma_i(G)$ normalizes H , i.e. $\gamma_i(G) \leq N_G(H)$. This implies that H is a proper subgroup of $N_G(H)$.

Lemma 3.53 Let G be a finite group, and let $P \leq G$ be a Sylow p -subgroup. If $N_G(P) \leq H \leq G$, then $H = N_G(H)$.

Proof Observe that $H \triangleleft N_G(H)$, and P is a Sylow subgroup of H . Hence the Frattini Argument (Theorem 2.6) implies that $N_G(H) = HN_G(P) = H$.

Theorem 3.54 A finite group G is nilpotent iff it is the direct product of its Sylow subgroups.

Proof Suppose that G is the direct product of its Sylow subgroups. Then it follows from Theorem 3.48 and Theorem 3.50(3) that G is nilpotent. Suppose conversely that G is nilpotent and P a Sylow p -subgroup of G . Lemma 3.53 implies that $N_G(P)$ is equal to its own normalizer. It follows that $N_G(P) = G$, and so $P \triangleleft G$. This implies that G is the direct product of its Sylow subgroups.

Nilpotent groups behave like p -groups in a number of ways. In any group, every subgroup of prime index is a maximal subgroup. The converse is true for finite p -groups. The converse is not true in general (exercise). However, the converse is true for nilpotent groups.

Theorem 3.55 Suppose that G is a nilpotent group. Then every maximal subgroup H is normal and has prime index.

Proof Since G is nilpotent, it satisfies the normalizer condition (Theorem 3.52), and so $H < N_G(H)$. Since H is maximal, this implies that $N_G(H) = G$, and so $H \triangleleft G$. It now follows that G/H is of prime order.

Theorem 3.56 Suppose that G is a nilpotent group.

1. If H is a nontrivial normal subgroup of G , then $H \cap Z(G) \neq 1$.
2. If A is a maximal abelian normal subgroup of G , then $A = C_G(A)$.

Proof

1. Since G is nilpotent, we know that $\zeta^0(G) = 1$, and $\zeta^c(G) = G$ for some c . Hence there is an integer i such that $\zeta^i(G) \cap H \neq 1$. Let m be the smallest such integer. Now H is normal in G , and so $[H \cap \zeta^m(G), G] \leq H \cap [\zeta^m(G), G] \leq H \cap \zeta^{m-1}(G) = 1$. This implies that $H \cap \zeta^m(G) \leq Z(G)$ and $1 \neq H \cap \zeta^m(G) \leq H \cap Z(G)$.
2. First observe that since A is abelian, $A \leq C_G(A)$. Now suppose that $A < C_G(A)$. If H is any subgroup of G , we have $C_G(H^g) = C_G(H)^{g^{-1}} \forall g \in G$. Hence, since $A \triangleleft G$, we have $C_G(A)^g = C_G(A^{g^{-1}}) = C_G(A)$, and so $C_G(A) \triangleleft G$. It follows therefore that $C_G(A)^g = C_g(A)/A$ is a nontrivial normal subgroup of the nilpotent group G/A . Hence (1) above implies that there is a nontrivial element $Ax \in (C_G(A)/A) \cap Z(G/A)$. It follows from the Correspondence

Theorem that $\langle A, x \rangle$ is a normal abelian subgroup of G which properly contains A . This contradicts the maximality of A . Hence $A = C_G(A)$.

Remark Clearly all subgroups of an abelian group are normal. There are nonabelian groups all of whose subgroups are normal, e.g. H_8 , the quaternion group of order 8 ($\langle a, b \rangle, a^4 = b^2 = 1, bab^{-1} = a^{-1}$). All such nonabelian groups are nilpotent of class 2 (Dedekind).

Theorem 3.57 (Roseblade) Suppose that G is any group for which there is a positive integer n such that for every subgroup H of G , there is a normal series of length n from G to H . Then G is nilpotent, and the class of G is bounded above by a function of n .

Proof *Journal of Algebra* 2 (1965) 402-412.

Definition 3.58 We say that a group G is of exponent e if $x^e = 1 \forall x \in G$.

Definition 3.59 Let G be a group. The **Frattini subgroup** $\Phi(G)$ of G is defined to be the intersection of all maximal subgroups of G . If G has no maximal subgroups, e.g. \mathbb{Q} , then we define $\Phi(G) = G$.

Clearly $\Phi(G) \text{ char } G$, and so $\Phi(G) \triangleleft (G)$.

Definition 3.60 An element $x \in G$ is called a **non-generator** if it may be omitted from **any** generating set, i.e. $G = \langle x, y \rangle$ implies that $G = \langle y \rangle \forall y$ such that $G = \langle x, y \rangle$.

Independent Statement 3.61 (The Axiom of Choice) Suppose that $\{E_\alpha\}_{\alpha \in A}$ is a family of sets and that each of the sets E_α is nonempty. Then $\prod_{\alpha \in A} E_\alpha$ is nonempty, i.e. \exists an element $(C_\alpha)_{\alpha \in A}$ in this product.)

Definition 3.62 A relation \leq on a set S is said to be a **partial order** if

1. $x \leq x \forall x \in S$.
2. If $x \leq y$ and $y \leq z$, then $x \leq z \forall x, y, z \in S$.
3. If $x \leq y$ and $y \leq x$, then $x = y$.

Definition 3.63 A partially ordered set S is **totally ordered** if any two elements in S can be compared.

Definition 3.64 A nonempty subset C of a partially ordered set S is a **chain** if it is totally ordered in the ordering inherited from S .

Definition 3.65 If A is a subset of a partially ordered set S , then an element $x \in S$ is an **upper bound** for A if $a \leq x \forall a \in A$.

Definition 3.66 An element x of a partially ordered set S is **maximal** in S if whenever $x \leq y$, then in fact $x = y$.

Independent Statement 3.67 (Zorn's Lemma) Suppose that S is a nonempty partially ordered set with the property that every chain in S has an upper bound. Then S has at least one maximal

element.

Lemma 3.68 Let G be any group. Suppose that $H \leq G$, and let $x \in G$ be such that $x \notin H$. Then \exists a subgroup K of G which is maximal with respect to the properties $H \leq K$ and $x \notin K$.

Proof Let S be the set of all subgroups of G which contain H but not x . Then $S \neq \emptyset$ since $H \in S$. Plainly S is partially ordered by inclusion. The union of any chain in S is in S , and so it follows that every chain in S has an upper bound. Hence, by Zorn's Lemma, S has a maximal element K .

Theorem 3.69 For any group G , $\Phi(G)$ is the set of all non-generators in G .

Proof Let M be a subgroup of G that is maximal with respect to the properties $\langle y \rangle \leq M$ and $x \notin M$. Then M is a maximal subgroup of G , for if $M < H \leq G$, then $x \in H$, and so $H = G$. Thus $x \in M$ for all maximal subgroups M , i.e. $x \in \Phi(G)$. Suppose conversely that $z \in \Phi(G)$ and assume that $G = \langle z, y \rangle$ and that $G \neq \langle y \rangle$. Then we may find a maximal subgroup N such that $\langle y \rangle \leq N$. However, $z \in \Phi(G)$, so $z \in N$, and so $G = \langle z, y \rangle \leq N$, which is a contradiction. So z is a non-generator.

Theorem 3.70 Let G be a finite group.

1. $\Phi(G)$ is nilpotent.
2. If G is a finite p -group, then $\Phi(G) = G'G^p$, where G^p is the subgroup of G generated by all p th powers.
3. If G is a finite p -group, then $G/\Phi(G)$ is of exponent p .

Proof

1. Let P be a Sylow p -subgroup of $\Phi(G)$. Since $\Phi(G) \triangleleft G$, the Frattini argument implies that $G = \Phi(G)N_G(P)$. Since $\Phi(G)$ consists of non-generators of G , it follows that $G = N_G(P)$. So $P \triangleleft G$, and therefore $P \triangleleft \Phi(G)$. This implies that $\Phi(G)$ is the direct product of its Sylow subgroups, i.e. $\Phi(G)$ is nilpotent.
2. Suppose that G is a finite p -group, and let M be a maximal subgroup of G . Then $M \triangleleft G$ by Proposition 2.12, and $|G : M| = p$ by Corollary 2.13. Hence G/M is abelian, which implies that $G' \leq M$. Since G/M is of exponent p , we have $x^p \in M \forall x \in G$. Hence $G'G^p \leq \Phi(G)$. Note that $G'G^p$ char G , so $G'G^p \triangleleft G$. To show the reverse inclusion, observe that $G/G'G^p$ is elementary abelian. It follows that $\Phi(G/G'G^p) = 1$. Now if $H \triangleleft G$, with $H \leq \Phi(G)$, we have that $\Phi(G)$ is the inverse image of $\Phi(G/H)$ under the natural quotient map $G \rightarrow G/H$. (Exercise.) This implies that $\Phi(G) = G'G^p$.
3. Since $\Phi(G) = G'G^p$, it follows that $G/\Phi(G)$ is an abelian group of exponent p .

What about arbitrary groups?

Theorem 3.71 Let G be an arbitrary group. Then $G' \cap Z(G) \leq \Phi(G)$.

Proof Set $D = G' \cap Z(G)$. Suppose that $D \not\leq \Phi(G)$. Then \exists a maximal subgroup M of G such that $D \not\leq M$. Hence $G = MD$, and so each element $g \in G$ is of the form $md, m \in M, d \in D$.

We have $gMg^{-1} = (md)M(md)^{-1} = mdMd^{-1}m^{-1} = mMm^{-1} = M$, and so $M \triangleleft G$. This implies that G/M is cyclic of prime order and so is abelian. Hence $G' \leq M$. Since $D \leq G' \leq M$, this is a contradiction. Hence $D \leq \Phi(G)$.

Proposition 3.72 Let G be a group, and let U be a subgroup of G . Then U is a subgroup of $\Phi(G)$ whenever U satisfies the following condition: For any proper subgroup H of G ,

$$\langle U, H \rangle < G. \quad (*)$$

When G is finitely generated, this condition is both necessary and sufficient. In particular, we have that $H\Phi(G) < G$ for every proper subgroup H of G .

Proof If $(*)$ holds, then for any maximal subgroup M of G , we have $M \leq \langle U, M \rangle < G$. Hence $M = \langle U, M \rangle$, and so $U \leq M$. Therefore $U \leq \Phi(G)$. Now assume that G is finitely generated. If $U \leq \Phi(G)$, and H is a proper subgroup of G , then there is a maximal subgroup M of G containing H . (Exercise: Use Zorn's Lemma.) But also $U \leq M$. So $\langle U, H \rangle \leq M < G$, i.e. $(*)$ holds.

Lemma 3.73 Let G be any group, and let N be a finitely generated normal subgroup of G . Then $\Phi(N) \leq \Phi(G)$.

Proof $\Phi(N) \text{ char } N$, and so $\Phi(N) \triangleleft G$. Let M be a maximal subgroup of G , and suppose that $\Phi(N) \not\leq M$. Then $\Phi(N)M = G$. Since $\Phi(N) \leq N$, we have $N = \Phi(N)M \cap N = \Phi(N)(M \cap N)$. (Exercise.) Hence we have $\langle \Phi(N), M \cap N \rangle = N$. Proposition 3.72 implies that $M \cap N = N$ implies that $N \leq M$ implies that $\Phi(N) \leq M$, which is a contradiction. Hence $\Phi(N) \leq M$ for any maximal subgroup M of G , and so $\Phi(N) \leq \Phi(G)$.

Remark If N is not a normal subgroup of G , then Lemma 3.73 need not hold, e.g. take $G =$ any suitable finite simple group (so $\Phi(G) = 1$ and $N =$ any suitable cyclic subgroup of G).

Lemma 3.74 Let G be a finite group, and $N, K \triangleleft G$ such that $N \leq K \cap \Phi(G)$. If K/N is nilpotent, then so is K .

Proof Let P be a Sylow p -subgroup of K . Then PN/N is a Sylow p -subgroup of KN/N . Then KN/N is nilpotent, which implies that $PN/N \triangleleft K/N$. Now $PN/N \text{ char } K/N$, which implies that $PN/N \triangleleft G/N$, which implies that $PN \triangleleft G$. Since P is a Sylow p -subgroup of PN , the Frattini Argument gives $G = PNN_G(P) = NPN_G(P) = NN_G(P)$. Since, by hypothesis, $N \leq \Phi(G)$, Proposition 3.72 implies that $N_G(P) = G$, so $P \triangleleft G$, and hence $P \triangleleft K$. Since this holds for all P , it follows that K is nilpotent.

Proposition 3.75 (Wielandt) Let G be a finite group, and let $N \triangleleft G$. Then N is nilpotent iff $N' \leq \Phi(G)$.

Proof Suppose that $N' \leq \Phi(G)$. Then $N' \triangleleft G$, and N/N' is abelian (and therefore nilpotent). Thus Lemma 3.74 implies that N is nilpotent. Conversely, suppose that N is nilpotent. Then every maximal subgroup of M is normal of prime index by Theorem 3.55 and so contains N' . Hence $N' \leq \Phi(G)$ by Lemma 3.73.

Theorem 3.76 (Frattini) $\Phi(G)$ is nilpotent for any finite group G .

Proof Take $N = \Phi(G)$ in Proposition 3.75.

Theorem 3.77 (Wielandt) A finite group G is nilpotent iff $G' \leq \Phi(G)$.

Proof Take $N = G$ in Proposition 3.75.