# MTH 405

## 1. Group action on a set

**Theorem 1.1**

Let $H \leq G$, and define $N_G(H) = \{g \in G : g^{-1}Hg = H\}$. Then $H \leq N_G(H) \leq G$, and whenever $H \leq J \leq G$, then $J \leq N_G(H)$, i.e $N_G(H)$ is the largest subgroup of which $H$ is normal in. We call $N_G(H)$ the normaliser of $H$ in $G$.

proof

Certainly $N_G(H) \neq \emptyset$, since $H \leq N_G(H)$. Now, let $x, y \in N_G(H)$ (note that $y^{-1}Hy = H \Rightarrow yHy^{-1} = H$). Then,

$$\begin{aligned}(xy^{-1})^{-1}H(xy^{-1}) &= y(x^{-1}Hx)y^{-1} \\ &= yHy^{-1} \\ &= H.\end{aligned}$$

Hence, $xy^{-1} \in N_G(H)$. Therefore $N_G(H) \leq G$.

It is clear from the definition of $N_G(H)$ that $H \leq N_G(H)$. Finally, if $H \leq J \leq G$ and $x \in J$, then $x \in G$ and $x^{-1}Hx = H$. Hence by the definition of $N_G(H)$, $x \in N_G(H)$.

Thus, $J \leq N_G(H)$.

**Corollary 1.2**

Let $H \leq G$. Then $H \trianglelefteq G$ iff $N_G(H) = G$.

Definition

Let $G$ be a group and $X$ be a non-empty set. The group $G$ acts on the set $X$ if to each $g \in G$ and $x \in X$, there corresponds a unique element $xg \in X$ such that

i. $(xg_1)g_2 = x(g_1g_2)$ for all $g_1, g_2 \in G$

ii $xe = x$, $e$ the identity in $G$.

Remarks.

1. Under the conditions above, we say that $G$ acts on $X$ on the right. Action on the left are defined similarly.
2. We shall simply say $G$ acts on $X$, when we really mean it acts on $X$ on the right, and when we want to distinguish between the two, we shall mention whether the action is on the right or left.

Examples.

1. Let $X$ be any non-empty set and $G \leq S_X$. Then $G$ acts on $X$.

Solo

Let $g \in G$ be a map $X \longrightarrow X$ and for $x \in X$,

$xg$ is the image of $x$ under the map $g$. The condition $(xg_1)g_2 = x(g_1g_2)$ and $xe = x$ follows from the definition of the composition of mapping and the definition of the identity element. $e \in S_X$. This action is called the natural action of $G$ on $X$.

2. Let $V$ be a vector space $\neq 0$ over a field $F$. Then, with the usual vector space notation, if $a \in F$ and $v \in V$, then $av \in V$, and if $a_1, a_2 \in F$ and $v \in V$, then

$a_1(a_2v) = (a_1a_2)v$ and $1v = v$.

Thus, the multiplicative group $F^\times$ acts on the left on $V$ (regarded as a set).

Note :

The additive group $F^+$ does not act on the left on $V$. For if it does, we should have $a_1(a_2v) = (a_1 + a_2)v$ and $0v = v$ which is false.

Lemma 1.3

Let $G$ acts on the set $X$. We define a relation $\sim$ on $X$ by setting $x_1 \sim x_2$ if and only if $x_1, x_2 \in X$ and there is an element $g \in G$ such

that $x_1 g = x_2$. Then $\sim$ is an equivalence relation on $X$.

proof

For any $x \in X$, $x1 = x$, so that $x \sim x$.
If $x_1 \sim x_2$, then $x_1 g = x_2$ for some $g \in G$
hence $x_2 g^{-1} = (x_1 g) g^{-1} = x_1$ and so $x_2 \sim x_1$.
If $x_1 \sim x_2$ and $x_2 \sim x_3$, then $x_1 g_1 = x_2$
and $x_2 g_2 = x_3$ for $g_1, g_2 \in G$.
Hence,
$x_1 (g_1 g_2) = (x_1 g_1) g_2 = x_2 g_2 = x_3$
and so $x_1 \sim x_3$

Definition
Let $G$ acts on the set $X$. Then $X$ is partitioned in to disjoint equivalence classes with respect to the equivalence relation define in lemma 1.3 above. These equivalence classes are called the orbits of transitivity classes of the action.
For each $x \in X$, the orbit containing $x$ is called the orbit of $x$. Note that the orbit of $x$

$$orbt(x) = \{ xg \mid g \in G \}.$$

Proposition 1.4

Let $G$ acts on the set $X$ and let $x \in X$. Let $stab_G(x) = \{g \in G / xg = x\}$. Then $stab_G(x)$ is a subgroup of $G$, called the stabiliser of $x$ in $G$.

proof

From the definition of group action, $e \in stab_G(x)$, so that $stab_G(x) \neq \emptyset$.

Let $g_1, g_2 \in stab_G(x)$.

then $xg_1 = x = xg_2$

Hence,

$$x(g_1 g_2^{-1}) = (xg_1)g_2^{-1} = (xg_2)g^{-1} = xe = x$$

so that $g_1 g_2^{-1} \in stab_G(x)$.

Hence, $stab_G(x) \leq G$.

Examples

1. Let $n$ be a positive integer, $\sigma \in S_n$ and $G = \langle \sigma \rangle$. Suppose that $\sigma$ is expressed as a product of disjoint cycles as

$$\sigma = (a_{11}\, a_{12} \ldots a_{1n_1})(a_{21}\, a_{22} \ldots a_{2n_2}) \ldots (a_{s1}\, a_{s2} \ldots a_{sn_s})$$

where $s, n_1, \ldots, n_s$ are positive integers such that $n_1 + n_2 + \ldots + n_s = n$. Then the orbits of the natural action of $G$ on the set $\{1, 2, \ldots, n\}$

are the disjoint subsets $\{a_{11}, a_{12}, \ldots, a_{1n_1}\}$, $\{a_{21}, a_{22}, \ldots, a_{2n_2}\}, \ldots, \{a_{s1}, a_{s2}, \ldots, a_{sn_s}\}$.

For instance,

For $n=5$ and $\sigma=(123)(45)$, there are just two orbits $\{1,2,3\}$ and $\{4,5\}$. For $G=\langle\sigma\rangle$ $=\{(1), \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$ where $\sigma^2=(132)$, $\sigma^3=(45)$, $\sigma^4=(123)$ and $\sigma^5=(132)(45)$. The orbit containing 1 is

$$orbt(1)=\{ig \mid g\in G\}=\{1(1), 1\sigma, 1\sigma^2, 1\sigma^3, 1\sigma^4, 1\sigma^5\}$$
$$=\{1,2,3\}=orbt(2)=orbt(3).$$
$$orbt(4)=\{4g \mid g\in G\}=\{4,5\}=orbt(5).$$

Note:

$$stab_G(1)=stab_G(2)=stab_G(3)=\{(45),(1)\}$$
$$stab_G(4)=stab_G(5)=\{(1),(132),(123)\}$$

Since $|G|=6$, we see that for each $x=\{1,2,3,4,5\}$ the number of elements in the orbit of $x$ is equal to $[G: stab_G(x)]$

2. Let $H\leq G$. Then $H$ acts on $G$ (regarded as a set) by right multiplication in $G$; that is, where to each $h\in H$ and each $g\in G$ there corresponds the element $gh\in G$. that this does

define an action of H on G follows from the associative law of multiplication in G and the defining property of the identity element.

Now, for $g \in G$

$Stab_H(g) = \{h \in H : gh = g\} = \{e\}$

$orbt(g) = \{gh : h \in H\} = gh$

the left coset of H in G containing g.

(*) **Lemma 1.5 (orbit – stabilizer theorem)**

Let G act on the set X. and let $x \in X$. Then

$|orbt(x)| = [G : stab_G(x)]$.

proof

Let $X_1$ denote the orbit of x, Let $H = stab_G(x)$ and let J denote the set of right cosets of H in G.

Thus, $X_1 = \{xg / g \in G\}$

Define a mapping $\theta : X_1 \longrightarrow Y$ by $\theta(xg) = Hg$.

Note that this mapping is well-defined. For if $g_1, g_2 \in G$ and $xg_1 = xg_2$.

then,

$x(g_1 g_2^{-1}) = (xg_1)g_2^{-1} = (xg_2)g_2^{-1} = xe = x$

therefore $g_1 g_2^{-1} \in stab_G(x) = H$

i.e $Hg_1g_2^{-1} = H \Rightarrow Hg_1 = Hg_2$ as required.
Note also that $Hg_1 = Hg_2$, then $g_1g_2^{-1} \in H$ an
$x(g_1g_2^{-1}) = x$.
Thus
$xg_2 = (x(g_1g_2^{-1})g_2) = (xg_1)g_2^{-1}g_2 = xg_1$
This shows that $\theta$ is one-one mapping. It is
clear from its definition that $\theta$ is on to. Thus
$\theta$ is a bijection.
Hence
$$|X_1| = |Y|$$

Definition
Let G acts on the set X. The action is said
to be transitive if it has just one orbit. An
action which is non-transitive is called in-
transitive.

Example
Let n be a positive integer and let $X = \{1, 2, \ldots, n\}$. Then the natural action of $S_n$ on X is
transitive.
Note that : If we let $H \leq G$ and let X be
the set of right cosets of H in G. Then G acts

on X by right multiplication. For, to each $g \in G$ and each $Hx \in X$ (where $x \in G$) there corresponds the coset $Hxg \in X$. This defines an action of G on X; for if $x, g_1, g_2 \in G$, then

$$(Hxg_1)g_2 = Hxg_1g_2$$

and $$Hxe = Hx$$

The action is transitive; for any two right cosets of H in G are equivalent under the action: If $x_1, x_2 \in G$, then

$$x_1^{-1}x_2 \in G \text{ and } (Hx_1)x_1^{-1}x_2 = Hx_2$$

Next, let note that

$$\begin{aligned} \text{stab}_G(Hx) &= \{g \in G / Hxg = Hx\} \\ &= \{g \in G / xgx^{-1} \in H\} \\ &= x^{-1}Hx \end{aligned}$$

the conjugate of H by x. Note that by lemma 1.5, for every $x \in G$,

$$[G : x^{-1}Hx] = |X| = [G : H]$$

Next, we consider another important group action. G acts on itself by conjugation. In this case, for each $g \in G$ and each $x \in G$, we write $x^g$ for the element of G to which g moves x, so that by definition

(Note that group acts itself conjugation)

$x^g = g^{-1}xg$. the conjugate of $x$ by $g$.
This does define an action of $G$ on itself,
for if $x, g_1, g_2 \in G$, then

$$(x^{g_1})^{g_2} = g_2^{-1}(g_1^{-1}xg_1)g_2$$
$$= (g_1g_2)^{-1}x(g_1g_2)$$
$$= x^{g_1g_2}$$

and $x^e = e^{-1}xe = x$

Now, the orbit of $x$ is the set

$$\{x^g : g \in G\} = \{g^{-1}xg : g \in G\}$$

The conjugate class of $x$ in $G$; and

$$\text{Stab}_G(x) = \{g \in G / g^{-1}xg = x\}$$
$$= \{g \in G / xg = gx\}$$
$$= C_G(x)$$

the centraliser of $x$ in $G$.

Corollary 1.6

For each $x \in G$;

|the conjugacy class of $x$ in $G$| $= [G : C_G(x)]$

Corollary 1.7 (The class equation)
If $G$ is a finite group with $k$ distinct conjugacy classes of elements, and if $x_1, x_2, \ldots, x_k$ are elements of $G$, one from each of these $k$ classes, then

$$|G| = \sum_{i=1}^{k} |G : C_G(x_i)|$$

The positive integer $k$ is called the class number of $G$, which we denote by $k(G)$.

Definition
A group $G$ is called a $p$-group if for all $a \in G$, the order of $a$ is a power of the prime $p$.

Definition
A subgroup of a $p$-group $G$ is called a $p$-subgroup of $G$ if the subgroup is itself a $p$-group.

Theorem 1.8 (Cauchy's theorem)
Let $p$ be a prime, let $G$ be a finite group and let $p$ divides $|G|$. Then $G$ has an element of order $p$ and, consequently, a subgroup of order $p$. OR

Proof

Let $G$ be a finite group and $p$ a prime such that $p$ divides the order of $G$. Then $G$ contains a subgroup of order $p$.

proof

We will use induction on the order of $G$. If $|G| = p$, then clearly $G$ must have an element of order $p$. Now assume that every group of order $k$, where $p \leq k < n$ and $p$ divides $k$, has an element of order $p$. Assume that $|G| = n$ and $p | n$ and consider the class equation of $G$:

$$|G| = |Z(G)| + |G : C(x_1)| + |G : C(x_2)| + \ldots + |G : C(x_k)|$$

We have two cases.

Case 1:

The order of one of the centralizer subgroups, $C(x_i)$, is divisible by $p$ for some $i$, $i = 1, 2, \ldots, k$. In this case, by our induction hypothesis, we are done. Since $C(x_i)$ is a proper subgroup of $G$ and $p$ divides $|C(x_i)|$, $C(x_i)$ must contain an element of order $p$. Hence, $G$ must contain an element of order $p$.

Case 2.

The order of no centralizer subgroup is divisible by $p$. Then $p$ divides $[G : C(x_i)]$, the order of each conjugacy class in the class equation; hence, $p$ must divide the centre of $G$, $Z(G)$. Since $Z(G)$ is abelian, it must have a subgroup of order $p$ by the fundamental theorem of finite Abelian Groups. Therefore, the centre of $G$ contains an element of order $p$.

Corollary 1.9

If is a finite $p$-group, then $|G| = p^n$ for some $n \in \mathbb{N}$.

proof

Since $G$ is a $p$-group, we know that every element of $G$ has order $p$. By cauchy's theorem, for every prime $q$ that divides the order of $G$ there is an element of $G$ with order $q$, thus because every element has order $p$ or a power of $p$, there can be no other primes that divide the order of $G$, and so $|G| = p^n$ for some $n \in \mathbb{N}$ as desired.

Proposition 1.10 (subgroup lemma).
Let $p$ be a prime number. If $G$ is a $p$-group such that $|G| = p^n$ then $G$ has a normal subgroup of order $p^m$ for all $m$ such that $1 \leq m < n$

pmf

We will induct on $|G|$. for $|G| = p$ we are done, we now assume that the result is true for every $p$-group smaller than $G$.
Let $x \in G$. By corollary 1.6, the conjugate class of $x$ contains just one element if and only if $C_G(x) = G$, that is, if and only if $x \in Z(G)$. Thus the class equation can be expressed as

$$|G| = |Z(G)| + \sum_{[G : C_G(x_i)] > 1} [G : C_G(x_i)]$$

Each of $[G : C_G(x_i)]$ must divide $|G|$ by corollary 1.6 and Lagrange's theorem. Since $G$ is a $p$-group, $[G : C_G(x_i)]$ is a power of $p$. Thus by the class equation $|Z(G)|$ is also divisible by $p$. Let us say that $|Z(G)| = mp$ for some $m \in \mathbb{N}$. Now, by Cauchy's theorem we know that there exist $a \in Z(G)$ with order $p$. The subgroup $\langle a \rangle$ is normal in $G$,

because $a$ is in the centre of $G$, and so the group $|G/\langle a\rangle| = p^{n-1}$, and so by the induction hypothesis it has normal subgroups of order $P, P^2, \cdots, P^{n-2}$.
Now, let $S$ be a normal subgroup of order $p^i$, $1 \leq i < n-1$. By the correspondence theorem, there exists $S^*$ of $G$ such that $S \cong S^*/\langle a\rangle$.
We know $S$ and $\langle a\rangle$ are both normal subgroup, thus $S^*$ is also normal and
$|S^*| = |S||\langle a\rangle| = p^i p^1 = p^{i+1}$ for $1 \leq j < n-1$.
This implies that $G$ has a normal subgroup of order $p^m$ for $2 \leq m < n$. We previously defined $\langle a\rangle$ as a normal subgroups of order $p$, so we have subgroup (normal) of $G$ with order $p^m$ for $1 \leq m < n$, and the result follows

(*) Theorem 1.11
If $|G| = p^n$, where $n$ is a positive integer, then $z(G) \neq \{e\}$.

pmf → For each $x \in G$,
Let $x \in G$. By corollary 1.6, the conjugate class of $x$ containing just one element if and only $C_G(x) = G$, that is, if and only if

$x \in Z(G)$. Hence if $Z(G) = \{e\}$, the class equation gives

$$p^n = 1 + m_2 + m_3 + \cdots + m_k,$$

where each of the positive integers $m_2, m_3, \ldots, m_k$ is a divisor of $p^n$ and is greater than 1. By Corollary 1.6 $m_i = [G : C_G(x_i)]$. But then, since $p$ is a prime, each of $m_2, \ldots, m_k$ is a power of $p$ to a positive exponent. The equation above implies that 1 is divisible by $p$, a contradiction. We conclude that $Z(G) \neq \{e\}$.

**Corollary 1.12**

Every group of order $p^2$ is abelian.

*Proof*

We prove this result by contradiction. i.e Suppose that $|G| = p^2$ and $G$ is non-abelian. Then $Z(G) \subsetneq G$ (proper) and so by theorem 1.11 and Lagrange's theorem, $|Z(G)| = p$. Hence, $|G| \cdot Z(G) = p$, and so $G/Z(G)$ is cyclic, and it follows that $G$ is abelian, a contradiction.

Definition

Let $G$ acts on the set $X$. Then the fixed point subset of $X$ is defined to be

$$Fix_X(G) = \{x \in X / xg = x \ \forall g \in G\}$$
$$= \{x \in X / stab_G(x) = G\}.$$

Thus $Fix_X(G)$ consist of those element of $X$ each of which forms an orbit by itself.

Remarks

It may happens that $Fix_X(G) = \emptyset$. in particular if $G$ acts transitively on $X$, then $Fix_X(G) = \emptyset$ unless $|X| = 1$.

Examples

If $G \leq S_4$ and $G$ acts naturally on the set $X = \{1, 2, 3, 4\}$, then for $G = \langle (123) \rangle$, $Fix_X(G) = \{4\}$, while for $G = \langle (12)(34) \rangle$, $Fix_X(G) = \emptyset$.

Lemma 1.10

Let $G$ be a finite $p$-groups which acts on the finite set $X$, then

$$|Fix_X(G)| \equiv |X| \bmod p.$$

proof

Let the orbits of the action be $X_1, X_2, \ldots, X_k$. where $k$ is a positive integer. Then

$$|X| = \sum_{i=1}^{k} |X_i|$$

By Lemma 1.5, each $|X_i|$ is a divisor of $|G|$ and hence, since $p$ is a prime, must be a power of $p$. If there are just $j$ orbits consisting of single elements, where $0 \leq j \leq k$, then $|Fix_X(G)| = j$ and the equation above gives $|X| = j +$ a sum of powers of $p$ to positive exponents

Hence

$$|Fix_X(G)| = j \equiv |X| \bmod p.$$

Theorem 1.13 (Burnside's Lemma)

Let $G$ be a finite group which acts on a finite set $X$. If $r$ is the number of orbits in $X$ under $G$, then

$$r|G| = \sum_{g} |Fix_X(g)|$$

where

$$Fix_X(g) = \{x \in X \mid gx = x\}$$

OR

If $G$ is a finite group of permutation on a set $S$, then the number of orbits of elements of $S$ under $G$ is

$$\frac{1}{|G|}\sum_{\phi \in G} |fix(\phi)|$$

Proof

Consider all pairs $(g, x)$ where $gx = x$ and let $N$ be the number of such pairs. For each $g \in G$ there are $|Fix_X(g)|$ pairs having $g$ as first members. Thus

$$N = \sum_{g \in G} |Fix_X(g)| \quad \text{---------- (1)}$$

On the other hand, for each $x \in X$, there are $|stab_G(x)|$ pairs having $x$ as a second member. Thus we also have

$$N = \sum_{x \in X} |stab_G(x)| \quad \text{---------- (2)}$$

By Lemma 1.5 $|orbt(x)| = [G : stab_G(x)]$. But we know that $[G : stab_G(x)] = \frac{|G|}{|stab_G(x)|}$ so we obtain $|stab_G(x)| = \frac{|G|}{|orbt(x)|}$, then from (2) we have

$$N = \sum_{x \in X} \frac{|G|}{|orbt(x)|} = |G| \sum_{x \in X} \frac{1}{|orbt(x)|} \quad \text{---(3)}$$

Now $1/|orbt(x)|$ has the value for all $x$ in

the same orbit, and if we let $\theta$ be any orbit, then

$$\sum_{x \in \theta} \frac{1}{|orbit(x)|} = \sum_{x \in \theta} \frac{1}{|\theta|} = 1 \quad \text{---} \quad (4)$$

Substituting (4) in (3) we have obtain

$N = |G|$ (number of orbits in X under G)

$N = |G| . r$ ——————— (5)

comparing equation (5) and (1) we have

$$r|G| = \sum_{g \in G} |fix_x(g)| .$$

Corollary 1.14

If G is a finite group which acts on a finite set X, then

$$(\text{number of orbits in X under G}) = \frac{1}{|G|} \sum_{g \in G} |Fix_x(g)|$$

## 2. SYLOW Theorem.

We shall see in our subsequent lectures, that the fundamental theorem for finite generated abelian groups gives us complete information about all finite abelian groups. The study of finite non-abelian groups is much more complicated. The Sylow theorem gives us some important information about them.

We know from the Lagrange's theorem that the order of a subgroup of a finite group G must divide $|G|$. If G is abelian, then there exist subgroups of every order dividing $|G|$. We have seen in Math 206 that $A_4$, which has order 12, has no subgroup of order 6. Thus a non-abelian group G may have no subgroup of some order d dividing $|G|$; the "converse of the theorem of Lagrange" does not hold.

The Sylow theorem gives a weak converse namely, it show that if d is a power of a prime and d divides $|G|$, then G does contain a subgroup of order d.

Note: that 6 is not a power of prime

The Sylow theorem also give some information concerning the number of such subgroups and their relationship to each other.

Theorem 2.1 (Cauchy' theorem)
Let $p$ be a prime. Let $G$ be a finite group and let $p$ divide $|G|$. Then $G$ has an element of order $p$ and, consequently, a subgroup of order $p$.

Lemma 2.2
Let $H$ be a $p$-subgroup of a finite group $G$. then

$$[N(H) : H] \equiv [G : H] \pmod{p}$$

proof
Let $X$ be the set of all left cosets of $H$ in $G$, and let $H$ acts on $X$ by left multiplication, so that
$h(aH) = (ha)H$. (This can easily be seen to be an action of $H$ on $X$).
Note that $|X| = [G : H]$.
$Fix_X(H) = \{xH \in X / h(xH) = xH \ \forall \ h \in H$

$= \{xH \in X \mid H = x^{-1}hxH \ \forall h \in H\}$

$= \{xH \in X \mid x^{-1}hx \in H \ \forall h \in H\}$.

$= \{xH \in X \mid x^{-1}h(x^{-1})^{-1} \in H \text{ for all } h \in H\}$

$= \{xH \in X \mid x^{-1} \in N(H)\}$

$= \{xH \in X \mid x \in N(H)\}$

Thus left cosets in $fix_X(H)$ are those contained in $N(H)$. The number of such cosets is $[N(H) : H]$, so $|fix_X(H)| = [N(H) : H]$

Since $H$ is a $p$-group, it has order a power of $p$ and by lemma 1.10 we have

$$|Fix_X(H)| \equiv |X| \bmod p.$$

i.e $[N(H) : H] \equiv [G : H] \bmod p$.

(*) **Theorem 2.3**

Let $G$ be a finite group and let $|G| = p^n m$ where $n \geq 1$ and $p$ does not divide $m$. Then

i. $G$ contains a subgroup of order $p^i$ for each $i$, where $1 \leq i \leq n$

ii. Every subgroup $H$ of $G$ of order $p^i$ is a normal subgroup of a subgroup of order $p^{i+1}$ for $1 \leq i < n$

proof

i. From theorem 2.1, G contains a subgroup of order p. We now use an induction argument and show that the existence of a subgroup of order $p^i$ for $i < n$ implies the existence of a subgroup of order $p^{i+1}$

Since $i < n$, p divides $[G:H]$. By lemma 2.2, we have that p divides $[N(H):H]$. Since H is a normal subgroup of $N(H)$, the group $N(H)/H$ exists, and we see that p divides $|N(H)/H|$. By cauchi's theorem (theorem 2.1) $N(H)/H$ has a subgroup K which is of order p. If we let $\gamma: N(H) \longrightarrow N(H)/H$ be the canonical homomorphism, then $\gamma^{-1}(K) = \{x \in N(H) / \gamma(x) \in K\}$ is a subgroup of $N(H)$ and hence of G. This subgroup contains H and is of order $p^{i+1}$.

ii. We note from (i) above that $H \leq \gamma^{-1}(K) \leq N(H)$ where $|\gamma^{-1}(K)| = p^{i+1}$ since H is normal in $N(H)$, it is of course normal in the possible smaller group $\gamma^{-1}(K)$.

Definition (Sylow p-subgroup)

A sylow p-subgroup P of a group G is a maximal p-subgroup of G, that is, p-subgroup contained in no larger p-subgroup.

OR

Let G be a finite group and let p be a prime divisor of $|G|$. If $p^k$ divides $|G|$ and $p^{k+1}$ does not divide $|G|$, then any subgroup of G of order $p^k$ is called a sylow p-subgroup of G.

~~Theorem 2.3 (second~~

(*) Theorem 2.4 (First sylow theorem)

If G is a finite group of order $p^n m$, where $(p,m)=1$, then G has a subgroup of order $p^n$.

pmf

We use induction on $n=|G|$.

If $n=1$ then $m=1$ and the statement is trivial.

Assume that the statement is true for every finite group having order less than a given $n \in \mathbb{N}$. We prove it for the groups of order n. Obviously we may assume that $m>0$. Then $n=|G|$ is a

multiple of p. There are two cases.

i. $|Z(G)|$ is a multiple of p. Then by lemma 1, $Z(G)$ contains an element h of order p. Let $H = \langle h \rangle$. The $H \trianglelefteq G$ (why?) and $|G/H| = \frac{?}{p}$ which is divisible by $p^{m-1}$. Therefore, by the induction assumption, $G/H$ contains a subgroup $K/H$ of order $p^{m-1}$. Thus

$$|K| = |K/H| \cdot |H| = p^m$$

ii. $|Z(G)|$ is not a multiple of p. Then, by the class equation formula

$$|G| = |Z(G)| + \sum_{Cl(x) \neq \{x\}} |G : C_G(x)| \quad (*)$$

and from $p \mid |G|$ and $p \nmid |Z(G)|$ we deduce that there exist an $x \in G$ such that $Cl(x) \neq \{x\}$ and $p \nmid |G : C_G(x)|$. Then $p^m \mid |C_G(x)|$ and, since $Cl(x) \neq \{x\}$ implies $x \notin Z(G)$, $|C_G(x)|$ is a proper subgroup of $|G|$. Again, by the induction assumption, we get that $C_G(x)$ has a subgroup of order $p^m$. The theorem is now completely proved.

Theorem 2.5 (second sylow theorem).

Let $P_1$ and $P_2$ be a sylow p-subgroups of a finite group $G$. Then $P_1$ and $P_2$ are conjugate subgroup of $G$

proof

Here we will let one of the subgroup act on left cosets of the other, and use lemma 1.10. Let $X$ be the collection of left cosets of $P_1$, and let $P_2$ act on $X$ by $y(xP_1) = (yx)P_1$ for $y \in P_1$. Then this clearly defined an action of $P_2$ on $X$. By lemma 1.10 $|Fix_X(P_2)| \equiv |X| \bmod p$, and $|X| = [G : P_1]$ is not divisible by $P$, so $|Fix_X(P_2)| \neq 0$. Let $xP_1 \in Fix_X(P_2)$. then $yxP_1 = xP_1$ for all $y \in P_2$. so $x^{-1}yxP_1 = P_1$ for all $y \in P_2$. Thus $x^{-1}yx \in P_1$ for all $y \in P_2$, so $x^{-1}P_2x \leq P_1$ since $|P_1| = |P_2|$ we must have $P_1 = x^{-1}P_2x$, so $P_1$ and $P_2$ are indeed conjugate subgroups.

Theorem 2.6 (Third sylow theorem)

If $G$ is a finite group and $p$ divides $|G|$, then the number of sylow $P$-subgroups is congruent to 1 modulo $p$ and divides $|G|$.

Proof

Let P be a sylow p-subgroup of G. Let X be the set of all sylow p-subgroups and let P act on X by conjugation, so that $x \in P$ carries $T \in X$ in to $xTx^{-1}$. By lemma 1.10 $|X| = |Fix_X(P)| \bmod p$. Let us find $Fix_X(P)$. If $T \in Fix_X(P)$, then $xTx^{-1} = T$ for all $x \in P$. Thus $P \leq N(T)$. Of course $T \leq N(T)$ also, since P and T are both sylow p-subgroups of G, they are also sylow p-subgroups of $N(T)$. But then they are conjugate in $N(T)$ by theorem 2.5. Since T is a normal subgroup of $N(T)$, it is only conjugate in $N(T)$. Thus $T = P$. Then $fix_X(P) = \{P\}$. since $|X| = |fix_X(P)| = 1 \pmod p$, we see that the number of sylow p-subgroups is congruent to 1 modulo p.

Now, let G act on X by conjugation. Since all p-subgroup are conjugate, there is only one orbit in X under G. If $P \in X$, then $|X| = |\text{orbit of } P| = [G : stab_G(x)]$.

By lemma 1.5 $[stab_G(P)$ is, in fact the normaliser of P. For $stab_G(P) = \{x \in G : xPx^{-1} = P\} = N(P)]$. But $[G : stab_G(P)]$ is a divisor of $|G|$, so the number of Sylow p-subgroups divide $|G|$.

(8) Corollary 2.7

A finite group G has a unique sylow p-subgroup P for some prime P, if and only if $P \trianglelefteq G$.

Proof

If G has only one sylow p-subgroup P, then $P \trianglelefteq G$, for any conjugate of P is also a sylow p-subgroup. Conversely, if P is a normal sylow P-subgroup of G, then it is unique, for all sylow p-subgroups of G are conjugate.

Examples

(1) Let $G = S_3$, then $|G| = 6 = 2.3$. The sylow 2-subgroups of $S_3$ have order 2. The subgroups of order 2 are $\{(1),(12)\}, \{(1),(13)\}, \{(1),(23)\}$

Note that: there are three subgroups and that $3 \equiv 1 \bmod 2$. Also, 3 divides 6, the order of $S_3$.

(2) Show that a group of order 15 cannot be simple.

Sol'n

Let $|G| = 15 = 3.5$. By theorem 2.4 G has at least one subgroup of order 5, and by theorem 2.6, the number of such subgroups is

congruent to 1 modulas and divided 15. since 1, 6 and 11 are the only positive numbers less than 15 that are congruent to 1 modulo 5, and since among these only the number 1 divides 15, we see that G has exactly one subgroup P of order 5. By corolary 2.7 $P \trianglelefteq G$. Hence G is not simple

(3). No group of order $p^r$ for $r > 1$ is simple where p is a prime.

Sol:

By theorem 2.3 Such a group G contains a subgroup of order $p^{r-1}$ normal in a subgroup of order $p^r$, which must be all of G. Thus a group of order 16 is not simple; It has a normal subgroup of order 8.

(4) No group of 20 is simple, for such a group G contains Sylow 5-subgroups in number congruent to 1 modulo 5 and a divisor of 20, hence only. This Sylow 5-subgroups is then normal, since all conjugate of it must be itself

Proposition 2.8

Let $G$ be a finite non-abelian simple group and let $p$ be a prime divisor of $|G|$. Then the number $n$ of sylow $p$-subgroups of $G$ is greater than 1.

Prof

Let $P$ be a sylow $p$-subgroup of $G$. (Ex. If $G$ is a finite non-abelian simple group, then $|G|$ is divisible by at least two distint primes]. Then $|G|$ is divisible by at least two distinct primes, and so $\{1\} < P < G$. If $P$ is the only subgroup of $G$ of order $|P|$, then $P$ will be normal in $G$, in contradiction to the simplicity of $G$. Hence $n > 1$.

Theorem 2.9

If $|G| = pq$, where $p, q$ are distinct primes such that $q \not\equiv 1 \bmod p$, then $G$ has a normal sylow $p$-subgroup.

Prof

By Sylow's theorem, the number $n$ of distinct sylow $p$-subgroup of $G$ is a divisor of $q$, and $n \equiv 1 \bmod p$. Since $q$ is a prime, $n$ is

either 1 or q, and since, by hypothesis $q \neq 1 \bmod p$, it follows that $n = 1$. Thus $G$ has a unique sylow $p$-subgroup $P$ say, and so $P \trianglelefteq G$.

Corollary 2.10

If $|G| = pq$, where $p, q$ are distinct primes, then $G$ is not simple.

Proof

We may assume without loss of generality that $p > q$. Then $q^{-1}$ cannot be divisible by $p$, and so, by theorem 2.8, $G$ has a normal sylow $p$-subgroup $P$. Since $\{1\} < P < G$, $G$ is not simple.

(*) Theorem 2.11

If $|G| = p^2q$, where $p, q$ are distinct primes, then $G$ has either a normal sylow $p$-subgroup or a normal sylow $q$-subgroup, and so $G$ is not simple.

Proof

Let $n_p$ and $n_q$ be respectively the number of sylow $p$-subgroups and the number sylow $q$-

subgroups.

suppose contrary to what we wish to show, that $n_p > 1$ and $n_q > 1$. By Sylow's theorem, $n_p$ divides $q$, which is prime, hence $n_p = q$. Also $n_p \equiv 1 \bmod p$ so that it follows that $q > p$. Again by Sylow's theorem, $n_q$ divides $p^2$, so that $n_q$ is either $p$ or $p^2$. Now any element of order $q$ in $G$ generates a subgroup of order $q$, which is a Sylow $q$-subgroup of $G$. Any two distinct subgroups of $G$ of order $q$ intersect in 1, and so there are in $G$ $n_q(q-1)$ distinct element of order $q$. Hence if $n_q = p^2$, there are in $G$ just $p^2q - p^2(q-1) = p^2$ elements which are not of order $q$. But then, since no element of Sylow $p$-subgroup $P$ of $G$ has order $q$ and since $|P| = p^2$, $P$ must be a unique Sylow $p$-subgroup of $G$, in contradiction that $n_p > 1$. Therefor $n_q = p$. But since also $n_q \equiv 1 \bmod q$ this implies that $p > q$, a final contradiction.

(*) Theorem 2.12

If $|G| = pqr$, where $p, q, r$ are distinct primes, then $G$ is not simple.

proof

We may assume that $p \geq q > r$. Suppose contrary to what we want to show, that, there is a simple group $G$ of order $pqr$. Let $n_p, n_q, n_r$ be respectively, the number of sylow $p$-1 ; sylow $q$-1, and sylow $r$-subgroups of $G$. By proposition 2.8, these numbers are all greater than 1. ~~Hence $n_p$ sylow $p$-subgroups of $G$ intersect~~ in note that any two distinct sylow $p$-subgroups of $G$ intersect in 1. Hence $n_p$ sylow $p$-subgroups of $G$ contains $n_p(p-1)$ distinct elements of order $p$. Similarly, the $n_q$ sylow $q$-subgroups of $G$ contain $n_q(q-1)$ distinct elements of order $q$ and the $n_r$ sylow $r$-subsubgroups of $G$ contains $n_r(r-1)$ distinct elements of order $r$. Therefore

$$|G| = pqr \geq 1 + n_p(p-1) + n_q(q-1) + n_r(r-1)$$

By sylow's theorem, $n_p$ divides $qr$ and $n_p \equiv 1 \pmod{p}$. since $n_p > 1$ and $p > q$, $p > r$ It follows

that $n_p = qr$. Also, $n_q$ divides $pr$ and $n_q \equiv 1 \mod q$. Since $n_q > 1$ and $q > r$, $n_q \geq p$. Finally, $n_r > 1$ and $n_r$ divides $pq$. So that $n_r \geq q$.

Now we have

$pqr \geq 1 + qr(p-1) + p(q-1) + q(r-1)$ and hence

$0 \geq (p-1)(q-1)$.

Which is plainful false.

Topic

## Direct Products & Finite Abelian Groups

Let $H$ and $K$ be groups, then we can defined a multiplication of elements of the cartesian product $H \times K$ as follows:

Let $(h_1, k_1), (h_2, k_2) \in H \times K$ and defined

Let $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$ —— (*)

where $h_1 h_2$ and $k_1 k_2$ are the products in the group $H$ and $K$ respectively. With this multiplication defined on $H \times K$, it is easy to see that $H \times K$ is a group.

(i) the multiplication is clearly a binary operation.

(ii) If $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$, then

$$\begin{aligned}[(h_1, k_1)(h_2, k_2)] \cdot (h_3, k_3) &= (h_1 h_2, k_1 k_2)(h_3 k_3) \\ &= ((h_1 h_2) h_3, (k_1 k_2) k_3) \\ &= h_1 (h_2 h_3), k_1 (k_2 k_3) \\ &= (h_1, k_1)(h_2 h_3, k_2 k_3) \\ &= (h_1, k_1)[(h_2, k_2)(h_3, k_3)]\end{aligned}$$

Multiplication is therefore an associative binary operation on $H \times K$.

(iii) Let $1$ stands simultaneously for the identity of $H$ and $K$ and $(h, k) \in H \times K$

$$(1, 1)(h, k) = (h, k) = (h, k)(1, 1)$$

so that $(1,1)$ is the identity of $H \times K$.

(iv) If $(h,k) \in H \times K$, then $(h^{-1}, k^{-1})$ is its inverse. for $(h,k)(h^{-1}, k^{-1}) = (hh^{-1}, kk^{-1}) = (1,1)$

The group $H \times K$ with the binary operation defined in (*) is called the external direct product of the groups $H$ and $K$.

Remarks.

1. If $H$ and $K$ are finite groups, then it is clear that $|H \times K| = |H||K|$
2. If $|H| \neq 1$ and $|K| \neq 1$ and are finite, then $H \times K$ is neither isomorphic to $H$ nor $K$, because $|H \times K| \neq |H|$ and $|H \times K| \neq |K|$

From the above remarks we see that the direct product gives us a simple way of constructing new finite groups.

Example

Let $C_2$ be the cyclic group of order 2 generated by $g$, i.e $C_2 = \{1, g\}$. Then

$$C_2 \times C_2 = \{(1,g), (1,1), (g,1), (g,g)\}$$

note that $|C_2 \times C_2| = 4$, so we have two

non-isomorphic groups of order 4, namely the cyclic group of order 4, $C_4 = \{1, b, b^2, b^3\}$ where $b^4 = 1$, and the group $C_2 \times C_2$. Note that all the elements of $C_2 \times C_2$ are of order 2. Hence $C_4$ is not isomorphic to $C_2 \times C_2$. $C_2 \times C_2$ is called the klein four group or simply the four group.

Theorem 3.1

Let $G$ be a group with subgroups $H$ and $K$ such that $H \cap K = \{1\}$, the elements of $H$ commute with those of $K$, and $HK = G$ then $G \cong H \times K$.

proof

We first show that any element $g \in G$ can be written uniquely in the form $g = hk$, where $h \in H$ and $k \in K$. since $G = HK$, $g = hk$ for some $h \in H$ and $k \in K$. Suppose $g = h_1k_1$ and $g = h_2k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then $h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1}$, But $H \cap K = \{1\}$ and so $h_2^{-1}h_1 = 1$ and $k_2k_1^{-1} = 1$. Hence $h_1 = h_2$ and $k_1 = k_2$.

Now, define $\alpha : G \longrightarrow H \times K$ by $\alpha(g) = (h, k)$, where $g = hk \in G$. $\alpha$ is a one-one mapping, for we have shown that there is one and one way of writing $g$ in the form $g = hk$, and the elements of $H \times K$ are of the unique form $(h, k)$.

To prove $\alpha$ is a homomorphism, let $g_1 = h_1 k_1$ and $g_2 = h_2 k_2$ be any two elements in $G$, then

$$\begin{aligned}
\alpha(g_1 g_2) &= \alpha(h_1 k_1 h_2 k_2) \\
&= \alpha(h_1 h_2 k_1 k_2) \\
&= (h_1 h_2, k_1 k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= \alpha(h_1 k_1)\alpha(h_2 k_2) \\
&= \alpha(g_1)\alpha(g_2)
\end{aligned}$$

Hence $\alpha$ is a homomorphism and the result follows.

## Lemma 3.2

If $H$ and $K$ are normal subgroups of a group $G$ with $H \cap K = \{1\}$, then $H$ and $K$ commute element-wise.

proof

Let $h \in H$ and $k \in K$. Then

$h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k \in K$ as $K \trianglelefteq G$

$= h^{-1}(k^{-1}hk) \in H$ as $H \trianglelefteq G$

Therefore, $h^{-1}k^{-1}hk \in H \cap K = \{1\}$, and so, $h^{-1}k^{-1}hk = 1$ from which $hk = kh$.

Corollary 3.3

Let $G$ be a group with normal subgroups $H$ and $K$, and suppose $H \cap K = \{1\}$ and $HK = G$. Then $G \cong H \times K$.

Proposition 3.4

If $G$ is a finite group with subgroup $H$ and $K$, then

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

proof

Let $\bar{I} = H \cap K$, $\bar{I}$ is a subgroup of $G$ and since $\bar{I} \subseteq K$, $\bar{I}$ is a subgroup of $K$. Let $\bar{I}k_1$, $\bar{I}k_2, \ldots, \bar{I}k_n$ be the $n$ distinct cosets of $\bar{I}$ in $K$. Thus $K = \bar{I}k_1 \cup \bar{I}k_2 \cup \ldots \cup \bar{I}k_n$ and

$$n = \frac{|K|}{|\bar{I}|} = \frac{|K|}{|H \cap K|}.$$

We now claim that $HK = Hk_1 \cup Hk_2 \cup \dots \cup Hk_n$.
For if $hk \in HK$, then $k = Ik_j$ for some $I \in \bar{I}$, $j$ is an integer between 1 and $n$. Hence $hk = h(Ik_j) = (hI)k_j = h'k_j$ where $h' \in H$ as both $h, I$ belong to $H$. Thus

$$HK = Hk_1 \cup Hk_2 \cup \dots \cup Hk_n.$$

Now, suppose $Hk_i \cap Hk_j \neq \emptyset$ for some integers $i$ and $j$. Then $hk_i = h'k_j$ for some $h, h' \in H$. Consequently $(h')^{-1}h = k_j k_i^{-1}$, so that $k_j k_i^{-1} \in \bar{I} = H \cap K$. But $k_j k_i^{-1} \Rightarrow k_j \in \bar{I}k_i$.
Since two cosets are either equal or disjoint, $\bar{I}k_j = \bar{I}k_i$. Hence $Ik_j = Ik_i$. Thus
$Hk_i \cap Hk_j = \emptyset$ for $i \neq j$ and
$|HK| = |Hk_1| + |Hk_2| + \dots + |Hk_n|$
Now, $|Hk_i| = |H|$, because $h_1k_1 = h_2k_2$ if and only if $h_1 = h_2$. Therefore

$$|HK| = n|H| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Since $n|H| = \dfrac{|H| \cdot |K|}{|H \cap K|}$

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

Example

Let $G$ be a group of order 28 and $H_1$ and $H_2$ be a subgroup of $G$ of order 7 and 4 respectively, $H_1 \cap H_2 = \{1\}$, because any element in $H_1$ and also in $H_2$ must have order dividing 7 and 4. Accordingly.

$$|H_1 H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = 28 = |G| \quad \text{and}$$

$G = H_1 H_2$

Using proposition 3.4, we can replace theorem 3.1 in the case of finite groups.

**Theorem 3.5**

Let $G$ be a finite group with normal subgroups $H$ and $K$ where $|H||K| = |G|$. If either

i $H \cap K = \{1\}$ or

ii $HK = G$, then

$G \cong H \times K$.

Proof

(i) $H \cap K = \{1\}$ and $|H||K| = |G| \Rightarrow |HK| = |G|$. since $|HK| = |G|$ we can conclude $HK = G$. But then by corollary 3.5, $G \cong H \times K$.

If $HK = G$, $|HK| = |G|$. Therefore $|G| = |HK|$
$= \frac{|H||K|}{|H \cap K|}$ or $|H \cap K||G| = |H||K|$ but $|H||K| = |G|$
by hypothesis. Hence $H \cap K = \{1\}$ and by corollary 3.4 $G \cong H \times K$.

The concept of direct product can be generalised

$$G = G_1 \times G_2 \times \cdots \times G_n$$
$$= \prod_{i=1}^{n} G_i \quad \square$$

We now present a number of results that determine the structure of finite abelian groups. These results establish isomorphism classes for finite abelian groups of a given order, so that if we are given an abelian group $A$ of order $n$, then we know that $A$ must be isomorphic to one of the groups in the class corresponding to the number $n$. By using some additional information about the group $A$, we can determine which of the groups in the class is actually isomorphic to $A$.

Following the usual custom with abelian groups, all groups are written in additive notation. The following may be useful for translating from multiplicative to additive notation.

| Multiplicative notation | Additive notation |
|---|---|
| $ab$ | $a+b$ |
| $e$ | $0$ |
| $a^k$ | $ka$ |
| $a^k = e$ | $ka = 0$ |
| $MN = \{mn \mid m \in M, n \in N\}$ | $M+N = \{m+n \mid m \in M, n \in N\}$ |
| direct product $M \times N$ | direct sum $M \oplus N$ |

We begin by listing some known results in additive notation that will be used frequently.

## Lemma 3.6

Let $G$ be a group and let $a \in G$

i. If $a$ has order $n$, then $ka = 0$ iff $n \mid k$.

ii. If $a$ has order $td$, then $ta$ has order $d$.

## Theorem 3.7

If $N_1, N_2, \ldots, N_k$ are normal subgroups of a group $G$ such that every element of $G$ can be written uniquely in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$, then $G \cong N_1 \oplus N_2 \oplus \cdots \oplus N_k$.

## Definition

Let $G$ be a group and $p$ a prime, the set denoted by $G(p)$ is the set of elements in $G$ which have order a power of $p$, i.e

$G(p) = \{a \in G \mid o(a) = p^n \text{ for some } n \geq 0\}$

It is easy to verify that $G(p)$ is closed under addition and that the inverse of any element in $G(p)$ is also in $G(p)$. Therefore $G(p)$ is a subgroup of $G$.

Example.

1. Let $G = \mathbb{Z}_{12}$. Then $G(2) = \{0, 3, 6, 9\}$ i.e elements having order $2^0, 2^1, 2^2$ etc

$G(3) = \{0, 4, 8\}$.

2. If $G = \mathbb{Z}_3 + \mathbb{Z}_3$, then $G(3) = G$, since every non-zero element in $G$ has order 3

Lemma 3.8

Let $G$ be an abelian group and $a \in G$. an element of finite order. Then $a = a_1 + a_2 + \cdots + a_k$, with $a_i \in G(p_i)$, where $p_1, p_2, \cdots, p_k$ are the distinct positive primes that divide the order of $a$.

proof

The proof is by induction on the number of distinct primes that divide the order of $G$. If $o(a)$ is divisible only by the single prime $p_1$, then the order of $a$ is a power of $p$ and hence $a \in G(p_1)$. so the result is true in this case.

Assume inductively that the result is true for all elements whose order is divisible by at-least $p-1$ distinct primes and that $|a|$ is divisible by the distinct primes ~~and that $|a|$ is divisible by the~~ $p_1, p_2, \cdots, p_k$. Then

$$o(a) = p_1^{r_1} p_2^{r_2}, \cdots, p_k^{r_k}$$

with $r_i > 0$. Let $m = p_2^{r_2} \cdots p_k^{r_k}$ and $n = p_1^{r_1}$. so that $o(a) = mn$. Then $(m, n) = 1$ and there exists integers $u, v$ such that

$1 = mu + nN$. Hence

$a = 1a = (mu + nv)a = mua + nva$

But $mua \in G(p_i)$ because $a$ has order $m$ and hence $p_i^{r_i}(mva) = (nm)ua = u(mna) = u0 = 0$. Similarly, $m(nva) = 0$ so by Lemma 3.6 (4) the order of $nva$ divides $m$, an integer with only $k-1$ distinct prime divisors. Therefore by the induction assumption $nva = a_2 + a_3 + \dots + a_k$, with $a_i \in G(p_i)$. Let $a_1 = mua$, then

$a = mua + nva = a_1 + a_2 + \dots + a_k$ with $a_i \in G(p_i)$

## Theorem 3.9

Let $G$ be a finite abelian group, and let $p_1, p_2, \dots, p_k$ be the distinct primes that divide the order of $G$. Then $G$ is isomorphic to the direct sum of the $G(p_i)$, i.e $G \cong G(p_1) \oplus G(p_2) \oplus \dots \oplus G(p_k)$.

### proof

If $a \in G$, then its order divides $|G|$. Hence $a = a_1 + a_2 + \dots + a_k$ with $a_i \in G(p_i)$. by Lemma 3.8 (where $a_i = 0$ if the prime $p_i$ does not

divide $o(a)$). To prove that this expression is unique, suppose $a_1 + a_2 + \cdots + a_k = b_1 + b_2 + \cdots + b_k$, with $a_i, b_i \in G(p_i)$.

Since $G$ is abelian

$$a_1 - b_1 = (b_2 - a_2) + (b_3 - a_3) + \cdots + (b_k - a_k).$$

for each $i$, $b_i - a_i \in G(p_i)$ and hence has order a power of $p_i$, say $p_i^{r_i}$. If $m = p_2^{r_2} \cdots p_k^{r_k}$, then $m(b_i - a_i) = 0$ for $i \geq 2$, so that

$$m(a_1 - b_1) = m(b_2 - a_2) + \cdots + m(b_k - a_k)$$
$$= 0 + \cdots + 0 = 0$$

Consequently, the order of $a_1 - b_1$ must divide $m$. But $a_1 - b_1 \in G(p_1)$. so its order is a power of $p_1$. The only power of $p_1$ that divides $m = p_2^{r_2} \cdots p_t^{r_t}$ is $p^0 = 1$. Therefore $a_1 - b_1 = 0$ or $a_1 = b_1$.

Similarly against for $i = 2, \ldots, k$ show that $a_i = b_i$ for every $i$. Therefore every element of $G$ can be written uniquely in the form $a_1 + \cdots + a_k$ with $a_i \in G(p_i)$ and hence $G \cong G(p_1) \oplus \cdots \oplus G(p_k)$ by theorem 3.7

Lemma 3.10

Let $G$ be a finite abelian $p$-group and $a$ an element of maximal order in $G$. Then there is a subgroup $K$ of $G$ such that

$$G = \langle a \rangle \oplus K.$$

Lemma 3.11

Every finite cyclic group of order $n$ is isomorphic to $Z_n$.

(*) Theorem 3.12 (The fundamental theorem of finite Abelian groups)

Every finite abelian group $G$ is the direct sum of cyclic groups, and each of prime power order.

proof

By Theorem 3.9 $G$ is the direct sum of its subgroups $G(p)$, one for each prime $p$ that divides $|G|$. Each $G(p)$ is a $p$-group. So to complete the proof, we need only to show that every finite abelian $p$-group $H$ is a direct sum of cyclic groups, each of order a power of $p$. We prove this by induction on the order of $H$. The

assertion is true when $H$ has order 2. by lemma 3.11. Assume inductively that it is true for all groups whose order is less than $|H|$ and let $a$ be an element of maximal order $p^m$ in $H$. Then $H = \langle a \rangle \oplus K$ by lemma 3.10. By induction $K$ is a direct sum of cyclic groups, each with order a power of $p$. Therefore, the same is true of $H = \langle a \rangle \oplus K$.

Example

The number 36 can be written as product of prime powers in just four ways

$$36 = 2.2.3.3$$
$$= 2.2.3^2$$
$$= 2^2.3.3$$
$$= 2^2.3^2$$

By theorem 3.12. Every abelian group of order 36 must be isomorphic to one of the following:

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_4 \oplus \mathbb{Z}_9$.

you can easily verify that no two of these groups are isomorphic (the number of elements of order 2 or 3 is different for each group). Thus we have a complete classification of all groups of order 36 up to isomorphism.

Remarks:

A familiar group of order 36 namely $\mathbb{Z}_{36}$, does not appear explicitely on the list above. However, it is isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_9$ as we show.

Lemma 3.13

If $(m,k)=1$, then $\mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}$.

Proof

Take the element $(1,1)$ which we know be in $\mathbb{Z}_m \oplus \mathbb{Z}_k$. The order of $(1,1)$ in $\mathbb{Z}_m \oplus \mathbb{Z}_k$ is the smallest $t \in \mathbb{Z}$ such that $t(1,1)=(0,0)$. We know $t(1,1)=(t,t)$, so for this to be equal to $(0,0)$ we must have $t \equiv 0 \pmod{m}$ and $t \equiv 0 \pmod{k}$; with this we have that $m/t$ and $k/t$, which then becomes $mk/t$ because $(m,k)=1$, and so $mk \leq t$. Since we

know $mk(1,1) = (0,0)$ and because $t$ was defined as the smallest such integer, then $t = mk$.

thus, $\mathbb{Z}_m \oplus \mathbb{Z}_k$ is a cyclic group of order $mk$, and by lemma 3.11 then we see that $\mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}$ as desired.

**Theorem 3.14**

If $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, where $p_1, p_2, \ldots, p_t$ are distinct primes, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$$

**proof**

The theorem is true for groups of order 2. Assume inductively that it is true for group of order less than $n$. Apply lemma 3.13 with $p_1^{n_1}$ and $k = p_2^{n_2} \cdots p_t^{n_t}$. Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_k$, and the induction hypothesis shows that

$$\mathbb{Z}_k \cong \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}.$$

combining theorem 3.12 and 3.14 we have a second way of expressing a finite abelian group as the direct sum of cyclic groups.

Example

consider the group $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$.

Arrange the prime power orders of the cyclic factors by size, with one row for each prime

| | | | |
|---|---|---|---|
| 2 | 2 | $2^2$ | $2^3$ |
| | 3 | 3 | 3 |
| | | 5 | $5^2$ |

Now, rearrange the cyclic factors of G using the columns of this array as a guide and apply theorem 3.14.

$G \cong (\mathbb{Z}_2) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25})$.

$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{600}$.

This last decomposition of G as a sum of cyclic groups is sometimes more convinient than the original prime power decomposition. There are fewer cyclic factors, and the order of each cyclic factor divides the order of the next one. Impact the same process works in the general case.

## Theorem 3.15

Every finite abelian group is the direct sum of cyclic groups of orders $m_1, m_2, \ldots, m_t$, where $m_1 | m_2, m_2 | m_3, \ldots, m_{t-1} | m_t$.

If $G$ is a finite abelian group, then the integers $m_1, \ldots, m_t$ in theorem 3.15 are called the invariant factors of $G$.

When $G$ is written as a direct sum of cyclic groups of prime power orders as in theorem 3.12, the prime powers are called elementary divisors of $G$. Theorems 3.12 and 3.15 show that the order of $G$ is the product of its elementary divisors and also the product of its invariant factors.

### Example

All abelian groups of order 36 can be classified up to isomorphism in terms of their elementary divisors (as in the example preceding lemma 3.13) or in terms of their invariant factors

| Groups | Elementary Divisors | Invariant factors | Isomorphic groups. |
|---|---|---|---|
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ | $2, 2, 3, 3$ | $6, 6$ | $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$ | $2, 2, 3^2$ | $2, 18$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_{18}$ |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ | $2^2, 3, 3$ | $3, 12$ | $\mathbb{Z}_3 \oplus \mathbb{Z}_{12}$ |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_9$ | $2^2, 3^2$ | $36$ | $\mathbb{Z}_{36}$ |

The fundamental theorem 3.12 can be used to obtain a list of all possible abelian groups of a given order. To complete the classification of such groups we must show that no two groups on the list are isomorphic, that is the elementary divisors of a group are uniquely determined.

## Theorem 3.16

Let $G$ and $H$ be finite abelian groups. Then $G$ is isomorphic to $H$ if and only if $G$ and $H$ have the same elementary divisors.

(It is also true that $G \cong H$ if and only if $G$ and $H$ have the same invariant factors).

Topic: Classification of all Groups of low order, up to 15.

There is up to isomorphism, clearly one group of order 1.

If $p$ is a prime, any group of order $p$ is cyclic up to isomorphism, there is one and only one cyclic group of order $p$.

Since any two cyclic groups of the same order are isomorphic, thus there is one and the only one group of order $P$, $P$ a prime since every cyclic group is Abelian, by the fundamental theorems of finite Abelian groups, this group must be isomorphic to $\mathbb{Z}_p$.

In particular, the groups of order 2, 3, 5, 7, 11 and 13 are $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$.

Recall that for any prime $p$, a group of order $p^2$ is Abelian (Corollary 1.12). Again by the fundamental theorem of finite Abelian groups, these groups are $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

In particular, there are precisely two non-isomorphic groups of orders 4 and 9, namely $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_9$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Theorem 4.1

If $p$ and $q$ are distinct prime with $p<q$, then every group $G$ of order $pq$ has a single subgroup of order $q$, and this subgroup is normal in $G$. Hence $G$ is not simple. If $q \not\equiv 1 \bmod p$, then $G$ is abelian and cyclic.

proof

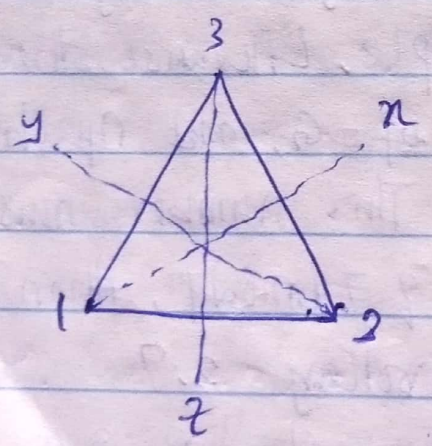
Let $n_q$ be the number of Sylow $q$-subgroup of $G$, then by third Sylow's theorem, $n_q \equiv 1 \bmod q$, and divides $pq$. and therefore must divide $p$. since $p<q$, the only possibly is $n_q = 1$. Thus, there is only one Sylow $q$-subgroup $Q$ of $G$. and by corollary 2.7 $Q \trianglelefteq G$. Thus $G$ is not simple. Likewise, there is a Sylow $p$-subgroup $P$ of $G$, and $n_p$ divides $pq$ and $n_p \equiv 1 \bmod p$. This number must either be 1 or $q$. If $q \not\equiv 1 \bmod p$, then $n_p = 1$ and thus $P \trianglelefteq G$ by corollary 2.7

Now since every element in $Q$ other than $e$ is of order $q$, and every element in $P$ other than $e$ is of order $p$, we have $Q \cap P = \{e\}$. Thus $|QP| = |P||Q| = pq = |G|$ and $P \trianglelefteq G$, $Q \trianglelefteq G$. By corollary 3.3 $G \cong Q \times P$. But $Q \cong \mathbb{Z}_q$ and $P \cong \mathbb{Z}_p$.

Hence, $G \cong \mathbb{Z}_q \times \mathbb{Z}_p$ and thus $G$ is abelian and cyclic.

In particular if $G$ is a group of order 15, and since $15 = (3)(5)$, $3 < 5$ and $5 \not\equiv 1 \bmod 3$. By theorem 4.1, $G$ is abelian and cyclic. Thus $G \cong \mathbb{Z}_{15}$.

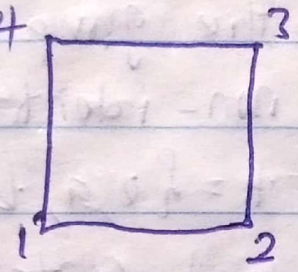
Consider the group $S_3 = \{(1), (123), (132), (23), (13), (12)\}$. Let us denote $\rho_0 = (1)$, $\rho_1 = (123)$; $\rho_2 = (132)$, $M_1 = (23)$, $M_2 = (13)$ and $M_3 = (12)$. Also, consider the equilateral triangle below




We observe that $\rho_1$ is rotation of the triangle clockwise by $2\pi/3$ and $\rho_2$ is rotation by $4\pi/3$, while $\rho_0$ is rotation by $2\pi$ a identity rotation. While $M_1$, $M_2$ and $M_3$ are the reflections

about the line x, y and z. For this reason, $S_3$ is also the group $D_3$ of symmetries of an equilateral triangle. Thus $S_3 \cong D_3$. The notation $D_3$ stands for third dihedral group. the nth dihedral group $D_n$ is the group of symmetries of the regular n-gon. $|D_n| = 2n$.

Consider the group of symmetries of a square $D_4$




Let $\rho_0 = (1)$, $\rho_1 = (1234)$, $\rho_2 = (13)(24)$, $\rho_3 = (1432)$
$\mu_1 = (12)(34)$, $\mu_2 = (14)(23)$, $\mu_3 = (13)$, $\mu_4 = (24)$.
Then $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \mu_3, \mu_4\}$.

The group $D_n$ can be represented by

$$D_n = \langle a, b : a^n = b^2 = e, ab = ba^{-1} \rangle$$

Any group generated by two elements satisfying these relation must necessary be isomorphic to $D_n$.

Theorem 4.2

Let $p$ be an odd prime and $G$ be a group of order $2p$. Then $G$ is either cyclic i.e $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.

proof

Suppose $G$ is not cyclic. By Lagrange's theorem every element in $G$ must have order 1, 2 or $p$. We must show that $G \cong D_p$.

Suppose there is no element of order $p$. i.e all elements of the group are of order 1 or 2. Thus every non-identity element is its an inverse. Let $H = \{e, a, b, ab\}$. It is clear that $H$ is closed and contains an identity element and is finite. Hence $H \leq G$. But $|H| = 4$ and does not divide $2p$ by Lagrange's theorem. This is a contradiction. Hence $G$ must contain an element of order $p$. Let $a \in G$, $o(a) = p$. Then $\langle a \rangle = \{e, a, a^2, \ldots, a^{p-1}\}$. Let $b \in G$ and $b \notin \langle a \rangle$. The order of $b$ must be 2, for if $\phi(e) = p$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$ and $|\langle a \rangle \langle b \rangle| = |\langle a \rangle||\langle b \rangle| = p^2 \geq 2p$. This is a contradiction since $|\langle a \rangle \langle b \rangle| \leq 2p$. Thus, we must must have $o(b) = 2$. Now the element $ab \notin \langle a \rangle$

and so $o(ab) = 2$. Hence

$ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$

so finally we have

$G \cong \langle a, b : a^4 = b^2 = 1, ab = ba^{-1} \rangle$

thus $A \cong D_8$.

The arrangement of this theorem is ordered that there are only two groups of order that there are only two groups of order 6, 10 and 14. The groups are $\mathbb{Z}_6, D_3, \mathbb{Z}_{14}, D_7$.

theorem 4.3

Let $G$ be a group of order 8, then up to isomorphic there are exactly five groups of order 8.

proof

If $G$ is an abelian group, then $G$ must be isomorphic to one of $\mathbb{Z}_8$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Thus there are 3 abelian groups of order 8 up to isomorphism.

If $G$ is non-abelian group of order 8, we will show that $G$ has exactly two distinct non-abelian group of order 8, up to

isomorphism: the quaterium group $Q_8$ and the dihedral group $D_4$:

common con

Topic. Isomorphism theorems and series of subgroups

We begin with the first isomorphism theorem which we come across in MATH 206. We will however state and prove it here for completeness.

**Theorem 5.1 (First Isomorphism theorem).**
Let $G$ and $H$ be groups and let $\theta: G \to H$ be a homomorphism. Then $\text{Im}\,\theta \cong G/\ker\theta$.

**proof.**
Let $K = \ker\theta$, the group $G/K$ exists since $\ker\theta$ is a normal subgroup of $G$.
Define the mapping $\phi: G/K \to \text{Im}\,\theta$ by $\phi(xK) = \theta(x)$. Then $\phi$ is well-defined for if

$$xK = yK \iff x^{-1}y \in K$$
$$\iff \theta(x^{-1}y) = e_H$$
$$\iff (\theta(x))^{-1}\cdot\theta(y) = e_H$$
$$\iff \theta(x) = \theta(y).$$

Now, for $x, y \in G$, $\theta(x) = \theta(y) \Rightarrow xK = yK$ from above, thus the mapping $\phi$ is one-one. We also observe that

$$\text{Im}\,\theta = \{\theta(\{xK\}) : x \in G\}$$
$$= \{\theta(xg) ; x \in G\} = \text{Im}\,\theta$$

Finally, we show that $\theta$ is a homomorphism.

For $x, y \in G$

$\theta(xk \cdot yk) = \theta(xyk)$

$= \theta(xy)$

$= \theta(x)\,\theta(y)$

$= \theta(xk)\,\theta(yk)$.

It therefore follows that

$\text{Im}\theta \cong G/k$ i.e $\text{Im}\theta \cong G/\text{ker}\,\theta$.

⊛ Theorem 5.2 (Second Isomorphism).

Let $H \leq G$ and $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$, $HN$ is a subgroup of $G$ and

$H/(H \cap N) \cong HN/N$

proof.

If $n \in H \cap N$ and $h \in H$, then $h^{-1}nh \in N$ as $N \trianglelefteq G$ and $h^{-1}nh \in H$ as $n \in H$. Therefore, $h^{-1}nh \in H \cap N$, that is $H \cap N \trianglelefteq H$.

$HN$ is a subgroup of $G$, for it is not empty, and if $n_1, n_2 \in HN$, then

$n_1 = h_1 n_1$, $n_2 = h_2 n_2$ and

$n_1 n_2^{-1} = h_1 n_1 n_2^{-1} \cdot h_2^{-1}$

$= h_1 n_3 h_2^{-1}$

$= h_1 h_2^{-1} \cdot h_2 n_3 h_2^{-1}$

$= hn_4$

where $n_3 = n_1 n_2^{-1} \in N$, $h_1 h_2^{-1} = h \in H$ and $h_2 n_3 h_2^{-1} = n_4 \in N$ as $N \trianglelefteq G$. Hence $n_1 n_2^{-1} \in HN$ and $HN$ is a subgroup of $G$.

Let $\theta : H \longrightarrow HN/N$ be defined by $h\theta = Nh$. Then $\theta$ is clearly onto, i.e $H\theta = HN/N$. Also $\theta$ is a homomorphism $(h_1 h_2)\theta = N(h_1 h_2) = Nh_1 Nh_2 = h_1\theta h_2\theta$.

Thus, by the first isomorphism theorem

$$H\theta \cong H/\ker\theta$$

$$\ker\theta = \{x : x \in H, x\theta = N\}$$
$$= \{x : x \in H, Nx = N\}$$
$$= \{x : x \in H, x \in N\}$$
$$= H \cap N$$

Hence, $HN/N \cong H/H\cap N$.

(8) Theorem 5.3 (Third isomorphism theorem). Let $G$ be a group and $N \trianglelefteq G$. If the factor group $G/N$ has a normal subgroup $M/N$, $M \geq N$, then $M \trianglelefteq G$ and $G/M \cong (G/N)/(M/N)$.

proof

Let $\rho : G \longrightarrow G/N$ be the natural homomorphism of $G \longrightarrow G/N$. Let $\beta : G/N \longrightarrow (G/N)/(M/N)$

be the natural homomorphism of $G/N \longrightarrow (G/N)/(M/N)$. put $\theta = \alpha\beta$. Then $\theta$ is homomorphism of $G$ to $(G/N)/(M/N)$, and since $\alpha$ is onto $G/N$, and $\beta$ is onto $(G/N)/(M/N)$, $\theta$ is onto $(G/N)/(M/N)$

Therefore

$G/\ker(\alpha\beta) \cong (G/N)/(M/N)$

by the first isomorphism theorem.

If $g \in G$, $g\theta = Ng$ and $(Ng)\beta = (M/N)Ng$.

Note that, here $(M/N)Ng$ is a coset of the normal subgroup $M/N$ in $G/N$, i.e an element in the group $(G/N)/(M/N)$.

Now, the elements of $M/N$ are all the cosets $Nm$, $m \in M$. The identity of $(G/N)/(M/N)$ is $M/N$.

$\ker\theta = \{g \in G / g\theta = (M/N)Ng = M/N\}$

But in that case $Ng \in M/N$, i.e $Ng = Nm$ for some $m \in M$. Hence $g = nm$ where $n \in N$. But $M \supseteq N$. Therefore $g \in M$ and so $\ker\theta \subseteq M$.

Note that if $m \in M$

Thus $M \subseteq \ker\theta$; Hence $\ker\theta = M$. Thus $M$ as a kernel of a homomorphism is a normal

subgroup of $G$, and
$G/M \cong (G/N)/(M/N)$.

⊛ Definition

A subnormal (or subinvariant) series of a group $G$ is a finite sequence of subgroups of $G$:
$H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = G$ such that $H_i \trianglelefteq H_{i+1}$ (that is $H_i$ is normal subgroup of $H_{i+1}$).

⊛ Definition.

A normal (or invariant) series of a group $G$ is a finite sequence of subgroups of $G$
$H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = G$ such that $H_i \trianglelefteq G$ (that is, $H_i$ is a normal subgroups of $G$ for all $i$)

Note that a normal series is always a subnormal series, but the converse need not be true. If $G$ is an abelian group, then every finite sequence of subgroups
$H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = G$

is both a subnormal and a normal series.

Example

1. Let $G = S_3$. Then $\{(1)\} \trianglelefteq S_3$ and $\{(1)\} \trianglelefteq A_3 \trianglelefteq S_3$ are the only two normal series for $S_3$

2. If $G = A_4$ and $K = \{(1), (12)(34), (13)(24), (14)(23)\}$ Then $\{(1)\} \trianglelefteq K \trianglelefteq A_4$ is a normal series for $A_4$. While $\{(1)\} \trianglelefteq \langle (12)(34) \rangle \trianglelefteq K \trianglelefteq A_4$ is a subnormal series for $A_4$ that is not a normal series.

3. If $G = \mathbb{Z}_{12}$. Then any subnormal series for G is a normal series. The following are two normal series for $\mathbb{Z}_{12}$.

$\{0\} \trianglelefteq \langle 6 \rangle \trianglelefteq \langle 3 \rangle \trianglelefteq \mathbb{Z}_{12}$

$\{0\} \trianglelefteq \langle 4 \rangle \trianglelefteq \langle 2 \rangle \trianglelefteq \mathbb{Z}_{12}$

Suppose G is a simple group, that is, a group with non-trivial normal subgroup then $\{1\} \trianglelefteq G$ is the only normal (subnormal) series for G.

Definition

A subnormal / normal series $\{K_j\}$ is $\{H_i\}$ of a group G, if $\{H_i\} \subseteq \{K_j\}$, that is, if each $H_i$ is one of the $K_j$

(*) Definition

A subnormal / normal series $\{K_i\}$ is a refinement of a subnormal / normal series $\{H_i\}$ of a group $G$, if $\{H_i\} \subseteq \{K_j\}$, that is, if each $H_i$ is one of the $K_j$.

Examples

1. The series $\{0\} \trianglelefteq 72\mathbb{Z} \trianglelefteq 24\mathbb{Z} \trianglelefteq 8\mathbb{Z} \trianglelefteq 4\mathbb{Z} \trianglelefteq \mathbb{Z}$ is a refinement of the series $\{0\} \trianglelefteq 72\mathbb{Z} \trianglelefteq 8\mathbb{Z} \trianglelefteq \mathbb{Z}$.

2. $\{(1)\} \trianglelefteq \langle (12)(34) \rangle \trianglelefteq K \trianglelefteq A_4$ is a refinement of $\{(1)\} \trianglelefteq K \trianglelefteq A_4$.

If $H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_n = G$ is a subnormal or normal series of $G$, then $H_i \trianglelefteq H_{i+1}$ is always true. Many structural properties of $G$ can be disclosed by studying the factor groups $H_{i+1}/H_i$.

(*) Definition

Two subnormal / normal series $\{H_i\}$ and $\{K_j\}$ of the same group $G$ are equivalent, if there is a one-one correspondence between the collections of factor groups $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$ such that the corresponding factor are isomorphic.

Examples

1. The series $\{0\} \trianglelefteq \langle 12 \rangle \trianglelefteq \langle 4 \rangle \trianglelefteq \mathbb{Z}_{24}$ and $\{0\} \trianglelefteq \langle 6 \rangle \trianglelefteq \langle 3 \rangle \trianglelefteq \mathbb{Z}_{24}$ of $\mathbb{Z}_{24}$ are equivalent.

2. The series $\{0\} \trianglelefteq 24\mathbb{Z} \trianglelefteq 4\mathbb{Z} \trianglelefteq \mathbb{Z}$ and $\{0\} \trianglelefteq 12\mathbb{Z} \trianglelefteq 6\mathbb{Z} \trianglelefteq 3\mathbb{Z} \trianglelefteq \mathbb{Z}$ are isomorphic series.

(*) Definition

A subnormal series $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = G$ is said to be a composition series for $G$, if each $H_i$ is a maximal proper normal subgroup of $H_{i+1}$, that is

i. $H_i \trianglelefteq H_{i+1}$ (normal subgroup)

ii. $H_i \neq H_{i+1}$ (proper)

iii. $H_i \trianglelefteq L \trianglelefteq H_{i+1}$ (maximal)

For $L \leq G$ implies $L = H_i$ or $L = H_{i+1}$. If the series above is a normal series then it called a principal or chief series.

(*) Theorem 5.4

The factors of a composition series of a group $G$ are simple groups.

Proof

Suppose $H_{i+1}/H_i$ is a non-trivial factor of a composition series of a group $G$. If $H_{i+1}/H_i$ is not simple, then there is a normal subgroup $N/H_i \trianglelefteq H_{i+1}/H_i$. The correspondence between a group and its factor groups allow us to conclude that $N$ is a proper normal subgroup of $H_{i+1}$, contradicting the fact that $H_i$ is a maximal proper normal subgroup of $H_{i+1}$. The result follows.

* Theorem 5.5

(i) Every finite group has a composition series

(ii) A normal series is a composition series if and only if it has no proper refinement.

Proof

i. The proof is by induction on $|G|$. The case $|G| = 1$ is trivial. Assume that the result is true for groups of order less than $|G|$. If $G$ is simple, then $\{1\} \trianglelefteq G$ is a composition series for $G$. If $G$ is not simple, then there exists a maximal proper normal subgroup $N \trianglelefteq G$.

By induction, $N$ has a composition series $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = N$.

But, then

$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = N \trianglelefteq G$ is a composition series for $G$.

(ii) Note that if $H_i \trianglelefteq H_{i+1}$ can be properly refined to $H_i \trianglelefteq N \trianglelefteq H_{i+1}$, then $H_i$ cannot be a maximal normal subgroup of $H_{i+1}$. Conversely, if a series cannot be refined, then each subgroup must be a maximal normal subgroup of its successor.

theorem 5.5 (Shreier theorem 1928)
Any two subnormal (normal) series of a group $G$ have equivalent refinement.

⊛ Corollary 5.7
Any subnormal (normal) series can be refined to a composition series.

proof
Suppose $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$ is a subnormal series for a group $G$ and $\{1\} = G_0 \trianglelefteq$

$G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$ is a composition series for $G$. Schreier's theorem asserts that both series have equivalent refinement. But a composition series has no proper refinement. Therefore, the first subnormal series can be refined to obtain a series equivalent to a composition series for $G$. Since a series equivalent to a composition series is itself a composition series, the proof is complete.

Theorem 5.8 (Jordan Hölder theorem 1889)
Any two composition (principal) series for a group $G$ are equivalent.

proof
Let $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$ and $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$ be two composition series for a group $G$. By Schreier's theorem, these series have equivalent refinement, since a composition series has no proper refinement, these series must already be equivalent.

Defn.

A group $G$ is said to be solvable if it has a subnormal (normal) series whose factors are abelian, that is there exists subgroups (normal subgroups) $\{H_0, H_1, \ldots, H_n\}$ such that

$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$ and $H_{i+1}/H_i$ is an abelian group for $i = 0, 1, 2, 3, \ldots, n-1$.

The chain of subgroups $\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$ is called the solvable series for $G$.

Theorem 5.9

i. A solvable group $G$ has a composition series if and only if it is finite.

ii. A finite group $G$ is solvable if and only if all its composition factors are cyclic of prime order.

Examples.

1. Let $G = S_3$, then $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ is a solvable series for $S_3$; for $A_3/\{(1)\}$ and $S_3/A_3$ are abelian. Therefore $S_3$ is solvable.

2. Let $G = S_4$, $G_1 = K = \{(1), (12)(34), (13)(24), (14)(23)\}$, $G_2 = A_4$, and $G_3 = G = S_4$. Then $\{(1)\} \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$ is a normal series. Moreover, $K/\{(1)\}$, $A_4/K \cong \mathbb{Z}_3$ and $S_4/A_4 \cong \mathbb{Z}_2$ are abelian; therefore $S_4$ is solvable.

Theorem 5.10

1. If $N \trianglelefteq G$ and $G_1 \trianglelefteq G_2 \trianglelefteq G$. Then $NG_1 \trianglelefteq NG_2$
2. If $N \trianglelefteq G$, $G_1 \trianglelefteq G$ and $G_1 \trianglelefteq G_2 \trianglelefteq G$, then $NG_1 \cap G_2 \trianglelefteq G_2$ and $G_2/(NG_1 \cap G_2)$ is isomorphic to a factor group of $G_2/G_1$

Theorem 5.11

Let $N \trianglelefteq G$ where $G$ is a solvable group. Then $G/N$ is solvable.

proof

Let $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ be a solvable series for $G$. Since $G_i \trianglelefteq G_{i+1}$, then $NG_i \trianglelefteq NG_{i+1}$ and $N/N = NG_0/N \trianglelefteq NG_1/N \trianglelefteq \cdots \trianglelefteq NG_n/N = G/N$ is a subnormal (normal) series for $G/N$. To show

that the series is a solvable series for $G$, we must verify that each factor group is abelian.

By the third isomorphism theorems, we have

$$(N G_{i+1}/N)/(N G_i/N) \cong N G_{i+1}/N G_i$$

But $G_i \trianglelefteq G_{i+1} \Rightarrow N G_{i+1} = (N G_i) G_{i+1}$, so that $N G_{i+1}/N G_i \cong (N G_i) G_{i+1}/N G_i \cong G_{i+1}/(N G_i \cap G_{i+1})$ by the second isomorphism theorem. Now $G_{i+1}/G_i$ is abelian and $G_{i+1}/(N G_i \cap G_{i+1})$. Now $G_{i+1}/G_i$ is abelian and $G_{i+1}/(N G_i \cap G_{i+1})$ is isomorphic to a factor group of $G_{i+1}/G_i$. Therefore, $G_{i+1}/(N G_i \cap G_{i+1})$ is abelian for $i = 0, 1, \ldots, n-1$ and the result follows.

Theorem 5.12

Let $H \leq G$ where $G$ is a solvable group. Then $H$ is solvable.

Proof

Let $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ be a solvable series for $G$. Set $H_i = G_i \cap H$ for $i = 0, 1, 2, \ldots, n$. We claim that $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = H$ is a solvable series for $H$.

First, since $G_i \trianglelefteq G$, then $H_i = G_i \cap H \leq G \cap H = H$. further more, if $h \in H_i = G_i \cap H$ and $x \in H_{i+1} = G_{i+1} \cap H$, since $G_i \trianglelefteq G_{i+1}$ implies that $xhx^{-1} \in G_i \cap H = H_i$. Thus $H_i \trianglelefteq H_{i+1}$, for $i = 0, 1, \ldots, n-1$. We therefore only need to show that $H_{i+1}/H_i$ is abelian for $i = 0, 1, 2, \ldots, n-1$. Now

$$H_{i+1}/H_i = (G_{i+1} \cap H) / (G_i \cap H)$$

since $H_i = G_i \cap H = (G_i \cap H) \cap G_{i+1}$, we can use the second isomorphism theorem to obtain

$$H_{i+1}/H_i \cong (G_{i+1} \cap H) / (G_{i+1} \cap H) \cap G_i$$
$$\cong (G_{i+1} \cap H) / G_i / G_i$$

But $(G_{i+1} \cap H) G_i / G_i \trianglelefteq G_{i+1}/G_i$ is an abelian group. Therefore $H_{i+1}/H_i$ is abelian for $i = 0, 1, 2, \ldots, n-1$, an $H$ is solvable.

Theorem 5.13

If $N \trianglelefteq G$ and both $G/N$ are solvable group, then $G$ is a solvable group.

Proof

Let $\phi : G \longrightarrow G/N$ be the homomorphism defined $\theta(g) = gN$. If $N/N = B_0 \trianglelefteq B_1 \trianglelefteq \ldots \trianglelefteq B_m = G/N$ and $\{1\} = A_0 \trianglelefteq A_1 \trianglelefteq \ldots \trianglelefteq A_n = N$ are solvable series for $G/N$ and $N$, respectively, then let

$C_i = \phi^{-1}(B_i)$. By the correspondence theorem, we have $C_i \leq G$, $B_i = C_i/N$ and $C_i \trianglelefteq C_{i+1}$, with $C_0 = N$ and $C_m = G$. But, then we can easily see that $\{1\} = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_n = N = C_0 \trianglelefteq C_1 \trianglelefteq \cdots \trianglelefteq C_m = G$ is a solvable series for $G$. since

$$C_{i+1}/C_i \cong (C_{i+1}/N)/(C_i/N) = B_{i+1}/B_i$$

is abelian for $i = 0, 1, 2, \cdots, n-1$.

(*) Theorem 5.14

Let $p$ be a prime and $P$ a $p$-group. Then $P$ is solvable.

proof

We will induct on $|P|$, with the case $|P| = 1$ being trivial. Assume that the result is true for all $p$-groups of order less than $|P|$. Since $P$ is a non-trivial group, it contains a non-trivial centre $Z(P)$. If $Z(P) = P$, then $P$ is abelian and therefore solvable. If $Z(P) \neq P$, then both $Z(P)$ and $P/Z(P)$ are $p$-groups of order less than $|P|$. By our induction hypothesis, both $Z(P)$ and $P/Z(P)$

are solvable. The result follows immediately from theorem 5.13.

Remarks

Non solvable groups do exist, infact a non-abelian simple group is non-solvable. An example of such a group is $A_n$ for $n \geq 5$. However, it is not necessarily true that every non solvable group is simple.

Defn

A group $G$ is said to have an Upper central series of length $r$ if $\{1\} = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_r = G$ where $Z_i/Z_{i-1}$ is the centre of $G/Z_{i-1}$. We define $Z_0 = \{1\}$, and $Z_1$ to be the centre of $G$. To define $Z_2$, we look at $G/Z_1$. Since every subgroup of $G/Z_1$ is uniquely of the form $H/Z_1$ where $H$ is a subgroup of $G$ containing $Z_1$. The centre of $G/Z_1$ is of the form $Z_2/Z_1$. Notice that as the centre is always a normal subgroup, $Z_2$ is a normal subgroup of $G$. In general, once $Z_i$ has been

defined and proved to be a normal subgroup of G, we define $Z_{i+1}/Z_i$ to be the centre of $G/Z_i$ and therefore $Z_{i+1} \trianglelefteq G$

(*) Defn:
A group G is called nilpotent if its upper central series ascend to G in a finite number of steps.

Theorem 5.15
A finite P-group is nilpotent.

Proof
If $|G| = 1$, there is nothing to prove.
If $|G| \neq 1$, then G has a non trivial centre (i.e $Z_1 \neq \{1\}$). If $G/Z_1$ is not the identity, the centre of $G/Z_1 = Z_2/Z_1 \neq Z_1/Z_1$, (i.e is non trivial). Notice that if $Z_1 \neq G$, then $Z_2 \neq Z_1$. Similarly if $G \neq Z_2$, $Z_3 \neq Z_2$. By induction we can show that if $Z_i \neq G$, $Z_{i+1} \neq Z_i$ and that $\{1\} = Z_0 \subset Z_1 \subset \cdots \subset Z_i \subset Z_{i+1}$. Since G is finite, $Z_k = G$ for some k. Therefore G is nilpotent.

Remarks

The successive quotients of an upper central series are abelian, so nilpotent groups are solvable, but the converse is false. for example, $S_3$ is solvable but not nilpotent.

Theorem 5.16

1. Any subgroup of a nilpotent group is nilpotent
2. If G is nilpotent and $H \trianglelefteq G$ then $G/H$ is nilpotent.

Defn.

A group G is called super solvable if it has a normal series whose factor are cyclic.

Theorem 5.17

1. Finite nilpotent groups are super solvable
2. A finite group is super solvable if all its principal (chief) factors have prime order.