Math 500, 9/20/04.

Let $G$ be a group. Define subgroups $G^{(i)}$ of $G$ by $G^{(1)} = [G, G]$ and, for $i > 1$, 
$G^{(i+1)} = [G^{(i)}, G^{(i)}]$. 

Then 
$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots$ 
is the derived series and $G^{(i)}$ the $i$th derived subgroup 
of $G$.

Exercise For all $i$, $G^{(i)}$ is normal in $G$.

Def $G$ is solvable if $G^{(n)} = \{e\}$ for some $n > 0$.

Example If $n \geq 5$, then $S_n$ is not solvable.

Indeed, we have 
$[S_n, S_n] = G^{(1)} \supseteq [A_n, A_n]$.

Since $[A_n, A_n] \neq \{e\}$ ($A_n$ is not abelian),
and $A_n$ is simple, it follows from the exercise 
that $[A_n, A_n] = A_n$. So $G^{(1)} \supseteq A_n$.

By induction, we get $G^{(n)} \supseteq A_n$ for all $n \geq 1$. 


Prop. Every nilpotent group is solvable.

Proof. By construction, \( G^{(i)} \leq G^{(i+1)} \) for all \( i \geq 1 \).
If \( G_n(G) = \{e\} \) then \( G_n = \{e\} \).

Def. A subnormal series
\[
G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{e\}
\]
is a composition series if each factor \( G_i/G_{i+1} \) is simple. The subnormal series is a solvable series if each \( G_i/G_{i+1} \) is abelian.

Def. A 1-step refinement of a subnormal series
\[
G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{e\}
\]
is a subnormal series of the form
\[
G = G_0 \supseteq G_1 \supseteq N \supseteq G_{i+1} \supseteq \ldots \supseteq G_n = \{e\}.
\]

A refinement of a subnormal series \( S \) is any subnormal series that can be obtained from \( S \) by a sequence of 1-step refinements.

The length of a subnormal series is the number of nontrivial subquotients \( G_i/G_{i+1} \).

A refinement is a proper refinement if its length is greater than the length of the original series.
Theorem

1) Every finite group has a composition series.
2) Every refinement of a solvable series is a solvable series.
3) A subnormal series is a composition series if and only if it has no proper refinements.

Proof. (1) By induction on the order of the group $G$, the case $|G| = 1$ being clear. For the inductive step, choose a maximal normal subgroup $N$ of $G$. By induction, $N$ has a composition series.

$$N = N_0 \supset N_1 \supset \cdots \supset N_n = e$$

Since $G/N$ is simple, $G$ has a composition series $G = G_0 \supset N = G_0 \supset N_1 \supset \cdots \supset N_n = e$.

(2) Suppose

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = e$$

is a solvable series, and let

$$G_0 \supset G_1 \supset \cdots \supset G_i \supset N \supset G_{i+1} \supset \cdots \supset G_n$$

be a 1-step refinement. Then, $G_i/N$ and $N/G_{i+1}$ are abelian by:

Exercise. Every subgroup and every quotient group of an abelian group is abelian.

So the refinement is a solvable series.
(3) Let
\[ G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{e\} \]
be a subnormal series, and
\[ G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i \supseteq N \supseteq G_{i+1} \supseteq \ldots \supseteq G_n = \{e\} \]
be a 1-step refinement. If this refinement is proper then \( G_{i+1} \nsubseteq N \subseteq G_i \) and \( N \) is normal in \( G_i \), so \( N / G_{i+1} \subseteq G_i / G_{i+1} \) is a nontrivial proper normal subgroup, so \( G \) cannot be a composition series. If \( G \) is not a composition series, then some \( G_i / G_{i+1} \) is not normal; letting \( K / G_{i+1} \subseteq G_i / G_{i+1} \) be a nontrivial proper normal subgroup, we get a proper refinement
\[ G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_i \supseteq K \supseteq G_{i+1} \supseteq \ldots \supseteq G_n = \{e\} \]
of \( G \).

**Theorem.** A group \( G \) is solvable iff it has a solvable series.

**Proof.** If \( G \) is solvable, then the derived series is solvable: indeed,
\[ G^{(i)}/G^{(i+1)} \text{ def } G^{(i)}/[G^{(i)}, G^{(i)}] \]
which is abelian by a homework problem.
Conversely, if
\[ G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{e\} \]
is any solvable series for \( G \), we claim that
\[ G_i \supseteq G^{(i)} \]
for all \( i \); we prove it by induction.

By definition, \( G_0/G_1 \) is abelian, so
\[ [G/G_1] \subseteq G_1 \]
by a homework problem. As the inductive step, we have

\[ G_i/G_{i+1} \text{ abelian } \Rightarrow G_{i+1} = [G^{(i)}, G_i] \subseteq [G_i, G_i] \subseteq G_{i+1}. \]

So \( G_i \supseteq G^{(i)} \) for all \( i \), and the series
\[ \{e\} = G_n \supseteq G^{(n)} \].
So \( G \) is solvable.

Example

\[ D_n = \langle a, b \mid a^n = b^2, aba = b \rangle. \]
Then
\[ \langle a \rangle \trianglelefteq D_n \]
has index 2, so it's normal.

Thus \( \{e\} \trianglelefteq \langle a \rangle \trianglelefteq D_n \) forms a solvable series for \( D_n \), so \( D_n \) is solvable.
Def Two subnormal series \( S \) and \( T \) of a group \( G \) are equivalent if there is a one-to-one correspondence between the nontrivial subquotients of \( S \) and the nontrivial subquotients of \( T \) such that corresponding factors are isomorphic groups.

Lemma If \( S \) is a composition series of a group \( G \), then any refinement of \( S \) is equivalent to \( S \).

Proof. A composition series has no proper refinements, so any refinement has the same list of nontrivial subquotients.

Zassenhaus Lemma [Butterfly Lemma].

Let \( H_1, H_2, K_1, K_2 \) be subgroups of \( G \), with \( K_i \) normal in \( H_i \) \( (i=1,2) \). Then

\[
\frac{(H_1 \cap H_2)K_1}{(H_1 \cap K_2)K_1} \cong \frac{(H_1 \cap H_2)K_2}{(K_1 \cap H_2)K_2}
\]

[Each denominator is normal in the numerator.]

Remark Zassenhaus proved it at the age of 21.
Claim.* Two upward lines meeting at a vertex means that vertex is the product of the two lower vertices. Two downward lines meet in the intersection of the upper vertices.

Proof of Lemma. For normality of \((H_1 \cap K_2)K_1\) in \((H_1 \cap H_2)K_1\), observe that, since \(K_2\) is normal in \(H_2\), it follows [exercise!] that \(H_1 \cap K_2\) is normal in \(H_1 \cap H_2\). Thus the product of \((H_1 \cap K_2)\) with \(K_1\) is normal in the product of \((H_1 \cap H_2)\) with \(K_1\). Switching the roles of \(i=1\) and \(i=2\) gives the other normality claim.

* This is routine, if slightly painful, to check.
Now we apply the Second Isomorphism Theorem:

\[
\frac{K_1 (H_1 \cap H_2)}{K_1 (H_1 \cap K_2)} = \frac{[K_1 (H_1 \cap K_2)] \cdot [H_1 \cap H_2]}{K_1 (H_1 \cap K_2)}
\]

by the butterfly diagram.

\[
\cong \frac{H_1 \cap H_2}{[K_1 (H_1 \cap K_2)] \cap (H_1 \cap H_2)} \quad \text{by the 2nd iso. thm.}
\]

\[
= \frac{H_1 \cap H_2}{(K_1 \cap H_2) (H_1 \cap K_2)} \quad \text{by the butterfly diagram.}
\]

The symmetric argument, switching \( i = 1 \) and \( i = 2 \), gives

\[
\frac{(H_1 \cap H_2) K_2}{(K_1 \cap H_2) K_2} \cong \frac{H_1 \cap H_2}{(K_1 \cap H_2) (H_1 \cap K_2)}
\]

This completes the proof.

Schreier Refinement Theorem: Any two subnormal series of a group \( G \) have subnormal refinements that are equivalent.

Before we prove it, we consider:
Jordan–Hölder Theorem

Any two composition series of a group are equivalent.

Proof. Composition series are subnormal series; hence by the Schreier refinement theorem they admit equivalent refinements. By our first lemma of the day, these refinements are equivalent to the two original composition series. \[\square\]

Proof of Schreier Refinement Theorem.

Let \( G = G_0 \supseteq \ldots \supseteq G_n = \emptyset \) and \( H = H_0 \supseteq \ldots \supseteq H_n = \emptyset \) be subnormal series.

Let \( G(i,j) = G_i \cap (G_i \cap H_j) \) and \( H(i,j) = H_j \cap (G_i \cap H_j) \). For all \( i, j \).

The Zassenhaus lemma applied to \( G_i, G_{i+1}, H_j, H_{j+1} \) tells us that
\( G(i,j;i) = G(i,i; (G(i,Hj;i)) \) is normal in \( G(i,i; (G(i,Hj;i))) = G(i,i) \).

So

\( G = G(0,0) \geq G(0,1) \geq \cdots \geq G(0,m) \geq G(1,0) \geq G(1,1) \)

gives a subnormal series; since \( G(i,0) = G_i \),
it refines the series \( \{G_i\} \). A symmetric argument shows that the \( H(i,j) \) refine the series of \( H_j \).

For each \( i,j \), the Zassenhaus Lemma gives

\[
\frac{G(i,j)}{G(i,j+1)} = \frac{G(i,i; (G(i,Hj;i)))}{G(i,i; (G(i,Hj;i)))} \simeq \frac{(G(i,Hj;i))Hj+i}{(G(i,Hj;i))Hj+i} = \frac{H(i,j)}{H(i,Hj)}
\]

This gives the desired one-to-one correspondence of the refinements. \( \square \).
Suppose
\[ G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\} \]
is a composition series for \( G \). The factors \( G_i/G_{i+1} \) are simple groups. If \( G \) is finite, its composition factors are finite.

The finite simple groups have been classified.

In principle, then, the problem of classifying all finite groups may be reduced to the following problem: given known groups \( G, H \) [both finite], what are the possible groups \( L \) such that \( G \) is a normal subgroup of \( L \) and \( L/G \cong H \) ? Indeed, if we can solve that problem, then we start with a list \( C_1, \ldots, C_n \) of composition factors from among the finite simple groups. Supposing that a group \( G \) has a composition series as above with \( G_i/G_{i+1} \cong C_{i+1} \), \( C_{n-1} \), we can enumerate all possibilities for \( C_{n-1} \). Since \( C_n = G_n \) is normal in \( G_{n-1} \) with quotient (isomorphic to) \( C_{n-1} \); then, starting from each such possible \( G_{n-1} \), we can enumerate all possible \( G_{n-2} \) since \( G_{n-1} \) is normal in \( G_{n-2} \) with known quotient \( G_{n-2}/G_{n-1} \cong C_{n-1} \); and so on.
We write
\[ \cdots \rightarrow G_{a+1} \xrightarrow{d_{a+1}} G_a \xrightarrow{d_a} G_{a-1} \rightarrow \cdots \]
for a sequence of groups and homomorphisms.

It is called a complex if \(\text{Im}(d_{a+1}) \leq \text{ker}(d_a)\)
for all \(a\), and an exact sequence if
\(\text{Im}(d_a) = \text{ker}(d_{a+1})\) for all \(a\).

An exact sequence
\[ (*) \quad 1 \rightarrow G_2 \xrightarrow{\alpha} G_1 \xrightarrow{\beta} G_0 \rightarrow 1 \]
where 1 stands for the trivial group is called
an extension or a 1-extension. Note that \(\alpha\) is injective, \(\alpha(G_2) = \ker(\beta)\), and
\(G_0 \cong G_1 / \ker(\beta)\) in this case.

A lifting of \((*)\) is a function \(l : G_0 \rightarrow G_1\)
with \(\beta \circ l = 1_{G_0}\); note that this function
is not assumed to be a homomorphism.

A lifting that is a homomorphism is called a
splitting of \((*)\).

Example Suppose a group \(G\) has a subgroup \(H\) and a
normal subgroup \(N\) such that \(G = N \rtimes H\) and
\(NH = G = \{e\}\). Then we call \(G\) the (internal)
semidirect product of \(N\) by \(H\), written
\(G = N \times H\).
If $H$ were also normal in $G$, then $G$ would be isomorphic to the direct product $N \times H$.

Facts (i) Each $g \in G$ can be written uniquely as $g = nh$ with $n \in N$, $h \in H$.

Proof. If $n_1 h_1 = n_2 h_2$, $n_1 \in N$, $h_1 \in H$, then $n_2^{-1} n_1 = h_2 h_1^{-1} \in H \cap N = e G$, so $n_1 = n_2$, $h_1 = h_2$. □

(ii). Define

$$\phi_h : N \to N \text{ by } \phi_h(n) = hnh^{-1} \text{ for each } h \in H.$$

Then

(a) $\phi_h$ is an automorphism of $N$.
(b) $h \mapsto \phi_h$ defines a homomorphism

$$H \to \text{Aut}(N).$$

(c) For any $n_1 \in N$, $h \in H$, we have

$$(\phi_{h_1}(n_1 h_2))(n_2 h_2) = n_1 h_1 n_2 h_1^{-1} h_1 h_2 = n_1 \phi_{h_1}(n_2) h_1 h_2 \in NH.$$

Conversely, let $N$ and $H$ be groups, and let

$\Psi : H \to \text{Aut}(N)$ be a homomorphism,

written $h \mapsto \phi_h \in \text{Aut}(N)$.

Define a binary operation $\ast : (N \times H) \times (N \times H) \to N \times H$ by
(n_1, h_1) * (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2).

Prop * is a group operation on N x H.

Proof:

\[
\begin{align*}
[(n_1, h_1) * (n_2, h_2)] * (n_3, h_3) &= (n_1 \phi_{h_1}(n_2), h_1 h_2) * (n_3, h_3) \\
&= (n_1 \phi_{h_1}(n_2), \phi_{h_1}(n_3), h_1 h_2 h_3)
\end{align*}
\]

while

\[
(n_1, h_1) * [(n_2, h_2) * (n_3, h_3)] = (n_1, h_1) * (n_2 \phi_{h_2}(n_3), h_2 h_3)
\]

\[
\begin{align*}
&= (n_1 \phi_{h_1}(n_2), \phi_{h_1}(n_3), h_1 h_2 h_3) \\
&= (n_1 \phi_{h_1}(n_2), \phi_{h_1 h_2}(n_3), h_1 h_2 h_3)
\end{align*}
\]

So * is associative.

\[
(n, h) * (e, e) = (n \phi_{h}(e), h e) = (n, h) = (e, e) * (n, h)
\]

by a similar computation.

So (e, e) is an identity element.

\[
\begin{align*}
(n, h) * (\phi_{h^{-1}}(n^{-1}), h^{-1}) &= (n,\phi_{h} \phi_{h^{-1}}(n^{-1}), h h^{-1}) \\
&= (n, \delta_{e}(n^{-1}), h h^{-1}) = (n^{n^{-1}}, h h^{-1}) = (e, e)
\end{align*}
\]

So inverses exist.

Thus * is a group operation.

Thus we write \( N \times H \) for this group.
Example Consider the homomorphism

$$\mathbb{Z}/2\mathbb{Z} \to \text{Aut}(\mathbb{Z}/n\mathbb{Z})$$

taking $$1 \mapsto \psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

$$\psi(k) = -k.$$ 

The semidirect product

$$\mathbb{Z}/n\mathbb{Z} \rtimes_{\psi} \mathbb{Z}/2\mathbb{Z}$$ has elements

$$a = (1,0)$$ and $$b = (0,1)$$, of orders $$n$$ and $$2$$, respectively. Moreover,

$$bab^{-1} = (0,1) \rtimes (1,1) = (-1,0) = a^{-1}.$$ 

So, this is the dihedral group $$D_n.$$  

In the semidirect product $$N \rtimes_{\psi} H,$$ the functions

$$N \to N \rtimes_{\psi} H,$$ $$H \to N \rtimes_{\psi} H$$ given by inclusions of factors are homomorphisms. Moreover, $$N$$

is normal: for $$n \in N,$$ $$h \in H,$$

$$hnh^{-1} = (e, h) \rtimes (n, e) \rtimes (e, h^{-1})$$

$$= (\psi_h(n), h) \rtimes (e, h^{-1})$$

$$= (\psi_h(n), e) \in N.$$ 

So $$N \rtimes_{\psi} H$$ is the semidirect product of $$N$$ by $$H.$$
Prop. Let

\[ 1 \rightarrow N \rightarrow G \xrightarrow{\beta} H \rightarrow 1 \]

be an extension.

Then G is a semi-direct product

\[ G \cong N \rtimes H \]

in such a way that \( \beta \) is the composite

\[ G \cong N \times H \quad \xrightarrow{\beta} \quad H \]

if and only if the extension is split.

Pr. Suppose that \( \lambda : H \rightarrow G \) is a splitting of the extension. Then \( \lambda(H) \) and \( N \) are subgroups of \( G \) with \( N \) normal in \( G \). If \( g \in G \), let

\[ a = \lambda\beta(g) \].

Then

\[ ga^{-1} = g\lambda\beta(g^{-1}) \] and so

\[ \beta(ga^{-1}) = \beta(g)\beta\lambda\beta(g^{-1}) = \beta(g)\beta(g^{-1}) = e \].

Thus \( ga^{-1} \in N \), say \( ga^{-1} = n \), and

\[ g = na, \quad n \in N, \quad a \in \lambda(H) \].

So \( G = N \cdot \lambda(H) \).

If \( g \in N \cap \lambda(H) \), then

\[ \beta(g) = e \]; but also \( g = \lambda(h) \) for some \( h \in H \),

so \( \lambda(h) = \lambda\beta(g) = \lambda\beta\lambda(h) = \lambda \beta(e) \lambda(h) \)

\[ = \lambda(h) = g \], so \( g = e \).

Thus \( G = N \times \lambda(H) \).
Conversely, suppose

\[ G \cong N \times H, \text{ and that, with a choice} \]

\[ G \xrightarrow{\phi} N \times H \] of such an isomorphism, the composite diagram

\[
\begin{array}{ccc}
N \times H & \xrightarrow{\phi} & G \\
\downarrow{\pi} & & \downarrow{\beta} \\
N \times H / N & \xrightarrow{i} & H
\end{array}
\]

commutes.

Then, considering \( H \) as a subgroup of \( N \times H \) by \( h \mapsto (e, h) \), we have a homomorphism \( \psi_H : H \to G \) such that

\[ \beta \circ \psi_H (h) = i \pi (h) = h \text{ for all } h \in H. \]

So \( \psi_H \) gives a splitting of \( \beta \). \qed