Proof ($\Leftarrow$). A composition series with abelian factors is a subnormal series with abelian factors.

($\Rightarrow$). Suppose G is finite solvable group with subnormal series

$$\{1\} = H_0 < H_1 < \ldots < H_n = G$$

where the factors are abelian. If this series is not a composition series, then some factor H_i/H_{i-1} is not simple and we can insert some K, such that $H_{i-1} < K < H_i$, to get a longer series. Notice that $K/H_{i-1} \leq H_i/H_{i-1}$ and thus abelian. Also we have by the 3rd Isomorphism Theorem that

$$H_i/K \cong \frac{H_i/H_{i-1}}{K/H_{i-1}}$$

that is a quotient of the abelian group H_i/H_{i-1} and thus abelian. Thus the new longer series also has abelian factors. Continuing adding terms until we get a composition series, gives us then a composition series with abelian factors and thus factors that are cyclic of prime order. $\Box$

How common are finite solvable groups? In fact surprisingly common. We mention two famous results.

Theorem A (Burnside's (p,q)-Theorem, 1904) Let p, q be prime numbers. Any group of order $p^n q^m$ is solvable.

Theorem B. (The odd order Theorem, Feit-Thompson, 1963). Any group of odd order is solvable.

(This is really a magnificent result. The proof is almost 300 pages and takes up a whole issue of a mathematics journal. Thompson received the Field's medal for his contribution).

4 Permutation groups and group actions

I. Permutation groups and the simplicity of A_n, $n \geq 5$

Convention. We will work with permutations from right to left. So if $\alpha, \beta \in S_n$ then for $\alpha\beta$, we apply β first and then α.

Lemma 4.1 *Let $\alpha \in S_n$. Then*

$$\alpha(i_1\ i_2\ \ldots\ i_m)\alpha^{-1} = (\alpha(i_1)\ \alpha(i_2)\ \ldots\ \alpha(i_m)).$$

Proof First suppose that $k = \alpha(j)$ is not in $\{\alpha(i_1), \alpha(i_2), \cdots, \alpha(i_m)\}$. Then j is not in $\{i_1, i_2, \cdots, i_m\}$ and

$$\alpha(i_1\ i_2\ \ldots\ i_m)\alpha^{-1}(\alpha(j)) = \alpha(i_1\ i_2\ \ldots\ i_m)(j) = \alpha(j).$$

This shows that $\alpha(i_1\ i_2\ \ldots\ i_m)\alpha^{-1}$ fixes the elements outside $\{\alpha(i_1), \alpha(i_2), \cdots, \alpha(i_m)\}$. It remains to show that this map cyclically permutes $\alpha(i_1), \alpha(i_2), \cdots, \alpha(i_m)$. But

$$\alpha(i_1\ i_2\ \cdots\ i_m)\alpha^{-1}(\alpha(i_r)) = \alpha(i_1\ i_2\ \cdots\ i_m)(i_r) = \alpha(i_{r+1})$$

where i_{m+1} is interpreted as i_1. This finishes the proof. $\Box$

Orbits. Let $i \in \{1, \ldots, n\}$. Recall that the α-orbit containing i is the subset $\{\alpha^r(i) : r \in \mathbb{Z}\}$ and that $\{1, \ldots, n\}$ partitions into a pairwise disjoint union of α-orbits.

Cycle structure. Suppose that the orbits of $\alpha \in S_n$ are $O_1, O_2, \ldots, O_r$ of sizes $l_1 \geq l_2 \geq \cdots \geq l_r$. We then say that α has a cycle structure of type $(l_1, \ldots, l_r)$.

Example. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\ 3\ 4\ 2\ 5)(6\ 7)(8).$$

Then α is of type $(5, 2, 1)$.

Definition. Let G be a group and $x \in G$. The *conjugacy class* of G containing x is $x^G = \{x^g : g \in G\}$.

On sheet 6, we see that G is a pairwise disjoint union of its conjugacy classes.

By Lemma 4.1, we have that if α is a permutation of some type $(l_1, \ldots, l_r)$, then the conjugacy class α^{S_n} consists of all permutations of that type. It follows also that if a normal subgroup N contains a permutation of type $(l_1, l_2, \ldots, l_r)$ then it contains all permutations of that type.

Example. $[(1\ 2)(3\ 4)]^{S_4} = \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$.

Remarks. We have the following formula (check it)

$$(i_1\ i_2\ \cdots i_m) = (i_1\ i_m)(i_1\ i_{m-1})\cdots(i_1\ i_2). \tag{3}$$

Remark As every permutation in S_n can be written as a product of disjoint cycles, this formula implies that every permutation in S_n can be written as a product of 2-cycles.

Recall. A permutation $\alpha \in S_n$ is said to be even/odd if it can be written as a product of even/odd number of 2-cycles. We also know that no permutation is both even and odd and thus S_n gets partitioned into even and odd elements. We denote by A_n the collection of all even elements. This is a subgroup that contains half the elements of S_n and for any odd element a in S_n, we have

$$S_n = A_n \cup aA_n.$$

In particular A_n is of index 2 in S_n and is thus normal.

Remark. By (3) we have that $(i_1\ \cdots\ i_m)$ is a even/odd permutation if and only if m is odd/even.

Remark Any even permutation in A_n can be written as a product of even number of 2-cycles. So every permutation in A_n is a product of elements of one the following forms (for i, j, r and s distinct)

$$(i\ j)(i\ r) = (i\ r\ j)$$

$$(i\ j)(r\ s) = (i\ j)(i\ r)(r\ i)(r\ s) = (i\ r\ j)(r\ s\ i).$$

It follows that any permutation in A_n can be written as a product of 3-cycles.

Lemma 4.2

(a) If $N \trianglelefteq S_n$ contains a 2-cycle then $N = S_n$.
(b) If $N \trianglelefteq A_n$ contains a 3-cycle then $N = A_n$.

Proof (a) Let $(i_1\ i_2)$ be a 2-cycle of N. Let $(j_1\ j_2)$ be any other 2-cycle of S_n. Let α be a permutation that maps i_k to j_k. By Lemma 4.1 we have that $(j_1\ j_2) = \alpha(i_1\ i_2)\alpha^{-1}$ which being a conjugate of $(i_1\ i_2)$ is also in N. So every 2-cycle is in N and as S_n is generated by 2-cycles it follows that $N = S_n$.

(b) The proof is similar. Let $(i_1\ i_2\ i_3)$ be a 3-cycle of N and let $(j_1\ j_2\ j_3)$ be any other 3-cycle of A_n. Let $\alpha \in S_n$ be a permutation that maps i_k to j_k. If $\alpha \in A_n$ then $(j_1\ j_2\ j_3) = \alpha(i_1\ i_2\ i_3)\alpha^{-1}$ is in N as before. If α on the other hand is odd then consider first instead $\beta = (j_1\ j_2)\alpha \in A_n$. The element

$$(j_2\ j_1\ j_3) = \beta(i_1\ i_2\ i_3)\beta^{-1}$$

is then in N and then also $(j_1\ j_2\ j_3) = (j_2\ j_1\ j_3)^{-1}$. So all the 3-cycles are contained in N and as A_n is generated by the 3-cycles, it follows that $N = A_n$. $\Box$

Lemma 4.3 *Suppose $n \geq 5$ and that $\{id\} \neq N \trianglelefteq A_n$. Then $|N| > n$.*

Proof As $N \neq \{\mathrm{id}\}$, we have some $\mathrm{id} \neq x \in A_n$. It suffices to show then x^{A_n} has at least n elements since then N would contain these elements plus the identity and thus more than n elements. Write x as a product of disjoint cycles and suppose that the longest cycle in the product has length m. There are two possibilities.

Case 1. $m \geq 3$.

Here x is of the form
$$x = (i\ j\ k\ \cdots)y$$
where $(i\ j\ k\ \cdots)$ is one of the cycles of longest length and y is the product of the remaining cycles. Now take any distinct $r, s, t, u, v \in \{1, 2, \ldots, n\}$. Let $\alpha \in S_n$ such that $\alpha(i) = r$, $\alpha(j) = s$ and $\alpha(k) = t$. Notice that by Lemma 4.1, we have
$$x^{\alpha^{-1}} = (r\ s\ t\ ...)y^{\alpha^{-1}}.$$
The same is true if α is replaced by $(u\ v)\alpha$ (notice that we are using $n \geq 5$ here), so we can assume that α is even. It follows that we can choose r, s, t to be any elements in $\{1, 2, \ldots, n\}$ that we like. We can now easily find at least n elments in x^{A_n}. For example we can take the elements
$$(1\ 2\ 3\ \cdots)y_1,\ (1\ 2\ 4\ \cdots)y_2,\ (1\ 3\ 2\ \cdots)y_3,\ (1\ 4\ 2\ \cdots)y_4,\ \cdots,\ (1\ n\ 2\ \cdots)y_n$$
Case 2. $m = 2$.

As x is even we have to have at least two 2-cycles in the product. It follows that
$$x = (i\ j)(k\ l)y$$
where $(i\ j), (k\ l)$ are two of the 2-cycles and y is the product of the remaining cycles.

Now take any distinct $r, s, t, u \in \{1, 2, \ldots, n\}$. Let $\alpha \in S_n$ such that $\alpha(i) = r$, $\alpha(j) = s$, $\alpha(k) = t$ and $\alpha(l) = u$. Notice that
$$x^{\alpha^{-1}} = (r\ s)(t\ u)y^{\alpha^{-1}}$$
and the same holds when α is replaced by $(r\ s)\alpha$ (as $(s\ r) = (r\ s)$). We can therefore again suppose that α is even. As r, s, t, u can be chosen arbitrarily we can now again easily find at least n elments in x^{A_n}. For example we can take these to be
$$(1\ 2)(3\ 4)y_1,\ (1\ 2)(3\ 5)y_2,\ (1\ 3)(2\ 4)y_3,\ (1\ 4)(2\ 3)y_4,\ \cdots,\ (1\ n)(2\ 3)y_n.$$
So in both cases we have at least n elments in x^{A_n} and as N also contains the identity element, it follows that N has at least $n+1$ elements. $\Box$

Theorem 4.4 *The group A_n is simple for $n \geq 5$.*

Proof We prove this by induction on $n \geq 5$. The induction basis, $n = 5$, is dealt with on Sheet 7. Now for the induction step, suppose $n \geq 6$ and that we know that A_{n-1} is simple. Let $G(n) = \{\alpha \in A_n :\ \alpha(n) = n\}$. Notice that $G(n) \cong A_{n-1}$ and thus simple by induction hypothesis. Now let $\{\mathrm{id}\} \neq N \trianglelefteq A_n$, we want to show that $N = A_n$.

Step 1. $N \cap G(n) \neq \{\mathrm{id}\}$.

We argue by contradiction and suppose that $N \cap G(n) = \{\mathrm{id}\}$. This means that the only element in N that fixes n is id. Now take $\alpha, \beta \in N$ and suppose that $\alpha(n) = \beta(n)$. Then $\alpha^{-1}\beta(n) = \alpha^{-1}(\alpha(n)) = n$ and by what we have just said it follows that $\alpha^{-1}\beta = \mathrm{id}$ or $\alpha = \beta$. Hence, a permutation α in N is determined by $\alpha(n)$ and since there are at most n values, we have that $|N| \leq n$. But his contradicts Lemma 4.3.

Step 2. $N = A_n$.

Now $\{\mathrm{id}\} \neq N \cap G(n) \trianglelefteq G(n)$ (by the 2nd Isomorphism Theorem) and since $G(n)$ is simple by induction hypothesis, it follows that $N \cap G(n) = G(n)$. In particular, N contains a 3-cycle and thus $N = A_n$ by Lemma 4.2. $\square$