Theorem 2.9 *(The Fundamental Theorem for finite abelian groups). Let G be a finite abelian group. G can be written as an internal direct sum of non-trival cyclic groups of prime power order. Furthermore the number of cyclic summands for any given order is unique for G.*

Remark. Suppose that $G = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n$ is a direct sum of cyclic group of prime power order. Notice that

$$G = \mathbb{Z}x_{\sigma(1)} + \mathbb{Z}_{\sigma(2)} + \cdots + \mathbb{Z}_{\sigma(n)}$$

for all $\sigma \in S_n$.

Convention. We order the cyclic summands as follows. First we order them with respect to the primes involved in ascending order. Then for each prime we order the summands in ascending order.

Example. If G is finite abelian group written as an internal direct sum

$$G = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3 + \mathbb{Z}x_4 + \mathbb{Z}x_5$$

of cyclic groups of orders $9, 2, 4, 3, 4$, then we order the summands so that they come instead in orders $2, 4, 4, 3, 9$. Notice then that G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

Remarks. (1) This discussion shows that any finite abelian group is isomorphic to a unique external direct sum

$$\mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{e_r}}$$

where $p_1 \leq p_2 \leq \cdots \leq p_r$ and if $p_i = p_{i+1}$ then $e_i \leq e_{i+1}$.

(2) Finding all abelian groups of a given order $n = p_1^{m_1} \cdots p_r^{m_r}$, where $p_1 < p_2 < \cdots < p_r$ are primes, reduces then to the problem of finding, for $i = 1, \ldots, r$, all possible partitions $(p_i^{e_1}, \ldots, p_i^{e_l})$ of the number $p_i^{m_i}$. This means that

$$1 \leq e_1 \leq e_2 \leq \ldots \leq e_l \text{ and } e_1 + \cdots + e_l = m_i.$$

Example. Find (up to isomorphism) all abelian groups of order 72.

Solution. We have $72 = 2^3 \cdot 3^2$. The possible partitions of 2^3 are $(8),\ (2, 4),\ (2, 2, 2)$ whereas the possible partions for 3^2 are $(3^2),\ (3, 3)$. We then have that the abelian groups of order 72 are

$$\begin{array}{lll} \mathbb{Z}_8 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, \\ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3. \end{array}$$

We now turn to the proof of Proposition 2.8. First as a preparation here are two subgroups that will play an important part in the proof.

Some useful subgroups. Let G be a finite abelian group. The following subgroups are going to play an important role in the proof of our next main result. That these are subgroups is shown on exercise sheet 3 (using multiplicative notation).

$$PG = \{px : x \in G\}, \quad G[p] = \{x \in G : px = 0\}.$$

As $G[p]$ is of exponent p it can be viewed as a vector space over $\mathbb{Z}_p$.

Proof of Proposition 2.8 First we deal with the existence of such a decomposition into a direct sum.

Let the exponent of G be p^n. We prove the proposition by induction on n. If $n = 1$ then the result holds by Lemma 2.6. Now suppose that $n \geq 2$ and that the result holds for smaller values of n. The exponent of pG is p^{n-1} and by the induction hypothesis we have that pG is a direct sum of non-trivial cyclic groups, say

$$pG = \mathbb{Z}px_1 + \cdots + \mathbb{Z}px_r. \tag{1}$$

Suppose the order of x_i is p^{m_i} (notice that $m_i \geq 2$ as $px_i \neq 0$). Then $p^{m_1-1}x_1, \ldots, p^{m_r-1}x_r$ are in $G[p]$. As $G[p]$ is of exponent p, it can be viewed as a vector space over $\mathbb{Z}_p$ and we can then extend to a basis $(p^{m_1-1}x_1, \ldots, p^{m_r-1}x_r, x_{r+1}, \ldots, x_s)$ for $G[p]$. It follows that we have a direct sum

$$G[p] = \mathbb{Z}p^{m_i-1}x_1 + \cdots + \mathbb{Z}p^{m_r-1}x_r + \mathbb{Z}x_{r+1} + \cdots + \mathbb{Z}x_s. \tag{2}$$

We now want to show that $G = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$ is a direct sum.

First we show that $x_1, \ldots, x_s$ generate G. Let $x \in G$. Then by (1)

$$px = a_1px_1 + \cdots + a_rpx_r$$

for some integers $a_1, \ldots, a_r$. Thus $x - (a_1x_1 + \cdots + a_rx_r)$ is in $G[p]$ and thus by (2) in $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$. Hence x is also in $\mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$.

It remains to see that the sum $G = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s$ is direct. Suppose that

$$a_1x_1 + \cdots + a_sx_s = 0.$$

We want to show that $a_1x_1 = \ldots = a_sx_s = 0$. Now multiplying by p we get

$$a_1px_1 + \cdots + a_rpx_r = 0$$

and since the $\mathbb{Z}px_1 + \cdots + \mathbb{Z}px_r$ is direct, it follows that $pa_1x_1 = \ldots = pa_rx_r = 0$. Thus p^{m_j-1} divides a_j for $j = 1, \ldots, r$, say $a_j = b_jp^{m_j-1}$. So we have

$$b_1p^{m_1-1}x_1 + \cdots + b_rp^{m_r-1}x_r + a_{r+1}x_{r+1} + \ldots + a_sx_s = 0.$$

As $G[p] = \mathbb{Z}p^{m_1-1}x_1 + \cdots + \mathbb{Z}p^{m_r-1}x_r + \mathbb{Z}x_{r+1} + \cdots + \mathbb{Z}x_s$ is direct we must have $b_1p^{m_1-1}x_1 = \ldots = b_rp^{m_r-1}x_r = a_{r+1}x_{r+1} = \ldots = a_sx_r = 0$. That is $a_1x_1 = \ldots = a_sx_s = 0$. This finishes the inductive proof.

To deal with uniqueness part, write G as a direct sum of cyclic groups of p-power order

$$G = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_r + \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_s$$

where $a_1, \dots, a_r$ have order at most p^{m-1} whereas $b_1, \dots, b_s$ have order at least p^m (notice that as G is a p-group the orders of all these elements are powers of p). Then

$$|\frac{p^{m-1}G}{p^mG}| = \frac{|\mathbb{Z}p^{m-1}b_1| \cdots |\mathbb{Z}p^{m-1}b_s|}{|\mathbb{Z}p^m b_1| \cdots |\mathbb{Z}p^m b_s|} = \frac{o(p^{m-1}b_1)}{o(p^m b_1)} \cdots \frac{o(p^{m-1}b_s)}{o(p^m b_s)}.$$

Notice that, in a finite abelian p-group, we have that if $a \neq 0$ then $o(pa) = \frac{1}{p}o(a)$ (If p^l is the order of a then p^{l-1} is the order of pa). The formula above thus implies that

$$|\frac{p^{m-1}G}{p^mG}| = p^s$$

and thus the number of summands of order at least p^m is $\log_p |\frac{p^{m-1}G}{p^mG}|$. Similarly the number of summands of order at least p^{m+1} is $\log_p |\frac{p^mG}{p^{m+1}G}|$. The number of summands of order exactly p^m is thus the difference

$$\log_p |\frac{p^{m-1}G}{p^mG}| - \log_p |\frac{p^mG}{p^{m+1}G}|.$$

This shows that the number of summands of order exactly p^m is an invariant that does not depend on what the decomposition is. □

3 Composition series and solvable groups

I. Simple groups. The primes of group theory.

We now introduce an important notion, namely that of a simple group. These can be thought of as the atoms or the primes of group theory.

Definition. A group G is simple if $G \neq \{1\}$ and the only normal subgroups of G are $\{1\}$ and G.

Example. The abelian simple groups are the cyclic groups of prime order. See exercise sheet 6.

Remark. Look at Exercise 5 on sheet 4. According to this exercise we have that if G is a direct product of non-abelian simple groups, then the simple factors are unique up to order (and not only up to isomorphism!). Thus we had here something analogous to a unique prime factorisation of a number. When we also allow for abelian simple factors the result would be similar and we get that the factors are unique (this time up to isomorphism). The problem is that not all finite groups can be written as direct products of simple groups. Example is S_3 and $\mathbb{Z}_4$. It turns out that any finite group can still in a different sense been built out of simple groups. To describe what this means we need to talk first about composition series.

Definition. Let G be a group.

(1) A *subnormal series* of G is a series

$$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_n = G$$

where $H_{i-1} \trianglelefteq H_i$, $i = 1, \ldots, n$. The quotient groups

$$H_1/H_0, H_2/H_1, \ldots, H_n/H_{n-1}$$

are called the *factors* of the series.

(2) A subnormal series is called a *composition series* if

$$H_1/H_0, H_2/H_1, \ldots, H_n/H_{n-1}$$

are simple groups, called the *composition factors*.

Example. Let $G = \mathbb{Z}a$ be a cyclic group of order 6. Then the subgroup $3G$ is of order 2 and index 3 and we get a subnormal series

$$\{0\} \leq 3G \leq G$$

with factors $3G/\{0\} \cong \mathbb{Z}_2$ and $G/3G \cong \mathbb{Z}_3$. Similarly the subgroup $2G$ is a subgroup of order 3 and index 2 that gives us another subnormal series

$$\{0\} \leq 2G \leq G$$

with factors $2G/\{0\} \cong \mathbb{Z}_3$ and $G/2G \cong \mathbb{Z}_2$. In fact these are both composition series as the factors are simple. Notice that the composition factors turn out to be the same (up to order). In fact this is always true.

The Jordan-Hölder Theorem. *Suppose that a group G has composition series*

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

and

$$\{1\} = K_0 < K_1 < \ldots < K_m = G.$$

Then $n = m$ and the composition factors $H_1/H_0, \ldots, H_n/H_{n-1}$ are the same (up to order) as $K_1/K_0, \ldots, K_n/K_{n-1}$.

Remarks. (1) Let G be a group with a normal subgroup N. It follows from the correspondence theorem that G/N is simple iff $G \neq N$ and there is no normal subgroup M in G such that $N < M < G$.

(2) Suppose that for some group G we have a subnormal series

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

that is not a composition series. Then some quotient H_m/H_{m-1} is not simple and by remark (1) there exists some subgroup K of G such that $H_{m-1} < K < H_m$ where K is normal in H_m. Notice also that (as H_{m-1} is normal in H_m) H_{m-1} is normal in K. By adding K, we thus get a subnormal series that is longer.

(3) Let G be a finite group. It has a subnormal series (for example $\{1\} < G$). Applying remark (2) we can continue adding terms while the series is not a composition series. Each time we get a longer series and as G is finite, this procedure must terminate in a composition series for G. Hence every finite group has a composition series.

Examples (1) G be an internal direct product of $S_1, \ldots, S_n$ where S_i is simple. The map

$$\phi : S_1 \cdots S_n \to S_n,\ a_1 a_1 \cdots a_n \mapsto a_n$$

is a group homomorphism with kernel $S_1 \cdots S_{n-1}$. By the first Isomorphism Theorem we have

$$\frac{S_1 \cdots S_n}{S_1 \cdots S_{n-1}} \cong S_n$$

we thus get a compostion series

$$\{0\} < S_1 < S_1S_2 < \ldots < S_1 \cdots S_n = G$$

with composition factors $\frac{S_1 \cdots S_i}{S_1 \cdots S_{i-1}} \cong S_i$. This shows that there exists at least one group with $S_1, \ldots, S_n$ as composition factors. (We can take $S_1 \times S_2 \times \cdots \times S_n$).

(2) Let n be a positive intger. All finite abelian groups of order n have the same composition factors (Sheet 6). So normally there are a number of different groups that have some given composition factors $S_1, \ldots, S_n$.

The Jordan Hölder theorem suggests the following possible strategy for finding all finite groups.

(a) Find all the simple groups.
(b) For any given choice $S_1, \ldots, S_r$ of simple groups find all the possible groups G whose composition factors are $S_1, \ldots, S_r$.

Remarks. (1) Classifying all finite groups is generally concidered too hard. These are too rich and for a given choice of simple groups $S_1, \ldots, S_n$ there is a great variety of ways of obtaining a group G with these as composition factors. As the number, n, of simple factors increases this becomes more and more complicated.

(2) On the other hand (a) is done! This is one of the real triumphs of 20th century mathematics. The classification result was announced in 1981. The proof is a collection of a number of journal articles by many different mathematicians and runs over 10000 journal pages!

According to the classification of finite simple groups, these are

(1) The cyclic groups of prime order, $\mathbb{Z}_p$,
(2) The alternating groups, $A_n, n \geq 5$,
(3) The simple groups of Lie type (a number of infinite families that crop up in a geometrical context)
(4) Twenty six exceptional groups that do not belong to any of the infinite families above.

The groups in (1) are dealt with on sheet 6. In the next chapter we deal with (2).

II. Solvable groups

Definition. We say that a group is solvable if it has a subnormal series with abelian factors.

Examples (1) Every abelian group is solvable.
(2) We have that S_3 has a composition series

$$\{1\} < A_3 < S_3$$

with factors $A_3/\{1\} \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$. As the factors are abelian S_3 is solvable.

Remark. We will see on sheet 6 that S_4 is solvable. In next chapter we will however see that S_n is not solvable for $n \geq 5$. This is the underlying reason for the fact that we can't solve the quintic by radicals.

Proposition 3.1 *A finite group G is solvable if and only its composition factors are cyclic of prime order.*

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. □