Definition 7.8. Let N, H be two groups and let $\varphi : H \longrightarrow \mathrm{Aut}(N)$ be a homomorphism. Write $\varphi(h)$ as φ_h. Define a new group with elements $N \times H$ and multiplication defined by

$$(n_1, h_1) * (n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1, h_2)$$

This is the *(external) semi-direct product* of N and H defined by φ and is written $N \rtimes_\varphi H$.

We usually just write the elements as nh and the product is $n_1h_1n_2h_2 = n_1\varphi_{h_1}(n_2)h_1h_2$.

Problems 7.9.

(1) Show that each element does indeed have an inverse, and that the associative law holds. Thus this operation does indeed define a group.

(2) Show that the multiplication is complete determined by the relation $hn = \varphi_h(n)h$.

(3) In $\mathrm{Gl}(n, F)$, for F a field, let T be the upper triangular matrices with nonzeros on the diagonal; let U be the upper triangular matrices with 1's on the diagonal and let D be the diagonal matrices with nonzero elements on the diagonal. Show that $T = U \rtimes D$. Describe the map $\varphi : D \longrightarrow \mathrm{Aut}(U)$.

Example 7.10. $D_n \cong C_n \rtimes_\varphi C_2$ where $\varphi : C_2 \longrightarrow \mathrm{Aut}(C_n)$ takes the non-identity element of C_2 to the automorphism of C_n taking n to n^{-1}.
$S_n = A_n \rtimes \langle(1, 2)\rangle$.
$S_4 = V \rtimes S_3$ where V is Klein-4 subgroup with elements of the form $(a, b)(c, d)$. What is the map φ?
$\mathrm{Gl}(n, F) \cong \mathrm{Sl}(2, F) \rtimes F*$.

Proposition 7.11. *Suppose there is a short exact sequence*

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\theta} H \longrightarrow 1$$

and there is a map $\alpha : H \longrightarrow G$ such that $\theta \circ \alpha$ is the identity on H. Then G is the internal direct product $N \rtimes \alpha(H)$.

Proof. We have $\alpha(H)$ is a subgroup of G. Suppose $g \in \alpha(H) \cap N$. Then $g = \alpha(h)$ and $\theta(g) = e_H$. Consequently $h = \theta \circ \alpha(h) = \theta(g) = e_H$. Thus $\alpha(H) \cap N = \alpha(e_H) = e_G$.

We next show that $\alpha(H)N = G$. Let $g \in G$ and let $g' = \alpha(\theta(g))$. Then $g' \in \alpha(H)$. We also have

$$\theta(g^{-1}g') = \theta(g)^{-1}\theta(\alpha(\theta(g))) = \theta(g)^{-1}\theta(g) = e_H$$

Then $g^{-1}g' \in N$. Setting $g^{-1}g' = n \in N$, we get $g = g'n^{-1}$. Thus an arbitrary element of G is in $\alpha(H)N$ as was to be shown. $\square$

Here is another problem, I haven't checked whether it is a semi-direct product.

Problems 7.12.

(1) Let $H = H(F)$ be the set of 3 by 3 upper triangular matrices over a field F with 1s on the diagonal. Show that this is indeed a subgroup of $\mathrm{Gl}(3, F)$.

(2) Show that $Z(H)$ consists of all matrices of the form $\begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Furthermore $Z(H) \cong (F, +)$.

(3) Show that the following 3 types of matrices generate this group.

$$\begin{bmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$$

(4) Show that $H(\mathbb{F}_p)$ is generated by 3 matrices, those in the form above with $a = b = c = 1$.

(5) Show that $H(\mathbb{F}_2) \cong D_4$.

8 Finitely Generated Abelian Groups

We will write the group operation additively. For A an abelian group, $a \in A$, and m an integer, $mA = a + \cdots + a$ with m summands. The order of a is the smallest positive integer m such that $ma = 0$. One can check that $ma + na = (m+n)a$ and $(mn)a = m(na)$.

Let's start with abelian groups that we understand well.

Theorem 8.1. *Let $m_1, \ldots, m_t$ be positive integers and $A = \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_t$. Let $P = \{p_1, \ldots, p_s\}$ be the set of all primes dividing $m_1 m_2 \cdots m_t$ and let the m_j have factorizations $m_j = \prod_{i=1}^{s} p_i^{e_{ij}}$ (allowing some $e_{ij} = 0$). Then*

$$A \cong A_1 \times \cdots \times A_s$$

where $A_i = \mathbb{Z}/p_i^{e_{i1}} \times \mathbb{Z}/p_i^{e_{i2}} \times \cdots \mathbb{Z}/p_i^{e_{it}}$

Proof. We know that $\mathbb{Z}/m_j \cong \mathbb{Z}/p_1^{e_{1j}} \times \cdots \times \mathbb{Z}/p_s^{e_{sj}}$. Thus

$$\begin{aligned}
A &= \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_t \\
&\cong \mathbb{Z}/p_1^{e_{11}} \times \cdots \times \mathbb{Z}/p_s^{e_{s1}} \\
&\quad \times \mathbb{Z}/p_1^{e_{12}} \times \cdots \times \mathbb{Z}/p_s^{e_{s2}} \\
&\qquad \cdots \\
&\quad \times \mathbb{Z}/p_1^{e_{1t}} \times \cdots \times \mathbb{Z}/p_s^{e_{st}} \\
&\cong \mathbb{Z}/p_1^{e_{11}} \times \cdots \times \mathbb{Z}/p_1^{e_{1t}} \\
&\quad \times \mathbb{Z}/p_2^{e_{21}} \times \cdots \times \mathbb{Z}/p_2^{e_{2t}} \\
&\qquad \cdots \\
&\quad \times \mathbb{Z}/p_s^{e_{s1}} \times \cdots \times \mathbb{Z}/p_s^{e_{st}} \\
&\cong \times A_1 \times \cdots \times A_s
\end{aligned}$$

□

Definition 8.2. The multiset $\left\{p_i^{e_{ij}} : i = 1, \ldots, s; \text{ and } j = 1, \ldots t\right\}$ is the set of *elementary divisors* of A.

Theorem 8.3. *With the notation of the previous theorem, for each i let $f_{i1} \geq f_{i2} \cdots \geq f_{it}$ be a permutation of the exponents $e_{i1}, \ldots e_{it}$ putting them in decreasing order. Let $n_j = \prod_{i=1}^{t} p_i^{f_{ij}}$. Then $n_t \mid n_{t-1} \mid \cdots \mid n_1$ and $A \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$.*

Proof. The fact that $n_j \mid n_{j-1}$ follows from $f_{ij} \leq f_{i,j-1}$. Stepping into the previous proof, by permuting the lines with the e_{ij} we have

$$\begin{aligned}
A &\cong \mathbb{Z}/p_1^{f_{11}} \times \cdots \times \mathbb{Z}/p_1^{f_{1t}} \\
&\quad \times \mathbb{Z}/p_2^{f_{21}} \times \cdots \times \mathbb{Z}/p_2^{f_{2t}} \\
&\qquad \cdots \\
&\quad \times \mathbb{Z}/p_s^{f_{s1}} \times \cdots \times \mathbb{Z}/p_1^{f_{st}} \\
&\cong \mathbb{Z}/p_1^{f_{11}} \times \cdots \times \mathbb{Z}/p_s^{f_{s1}} \\
&\quad \times \mathbb{Z}/p_1^{f_{12}} \times \cdots \times \mathbb{Z}/p_s^{f_{s2}} \\
&\qquad \cdots \\
&\quad \times \mathbb{Z}/p_1^{f_{1t}} \times \cdots \times \mathbb{Z}/p_s^{f_{st}} \\
&\cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t
\end{aligned}$$

□

Definition 8.4. The n_j (that are not 1) in the previous theorem are called the *invariant factors* of A.

We want to show that any finite abelian group is the product of cyclic groups, as in the previous theorem, so it has a set of elementary divisors and invariant factors.

Definition 8.5. Let A be an abelian group. For $m \in \mathbb{N}$ let

$$\begin{aligned} mA &= \{ma : a \in A\} \\ A[m] &= \{a : ma = 0\} \\ A(p) &= \left\{a \in A : \operatorname{ord}(a) = p^k \text{ for some } k\right\} \end{aligned}$$

We leave it as an exercise to prove that mA, $A[n]$ and $A(p)$ are all subgroups of A. Also that $A(p) = \cup_{i=0}^{\infty} A[p^i]$, and for A finite $A(p) = A[p^k]$ for some large enough k. The fact that $A[m]$ and $A(p)$ are group follows from the basic result that if a and b commute, then the order of $a+b$ divides $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$.

Problems 8.6.

(1) Find the elementary divisors and the invariant factors for $\mathbb{Z}/50 \times \mathbb{Z}/75 \times \mathbb{Z}/136 \times \mathbb{Z}/21000$.

(2) How many abelian groups are there of order $p^6 q^5 r^4$ where p, q, r are distinct primes? How many have k invariant factors, for $k = 1, 2, 3, 4, 5, 6$? Check your answer against the response to the previous question.

Example 8.7. $\mathbb{Q}/\mathbb{Z}$ is an interesting example. Every element has finite order, but $\mathbb{Q}/\mathbb{Z}$ cannot be written as a direct product of $\langle a \rangle$ and another group H for any nonzero $a \in \mathbb{Q}/\mathbb{Z}$.

Proposition 8.8. *Suppose that A is abelian with $|A| = mn$ and m, n coprime.*

(1) $mA = A[n]$

(2) A is the internal direct product of $A[m]$ and $A[n]$

Proof. Let $u, v \in \mathbb{Z}$ be such that $um + nv = 1$. Let $a \in A[n]$. Then $a = (mu + vn)a = m(ua) + v(na) = m(ua)$, since we assume $na = 0$. This shows that $A[n] \subseteq mA$. On the other hand, an arbitrary element of mA is ma for $a \in A$. Since $|A| = mn$, $m(na) = (mn)a = 0$, and this shows $mA \subseteq A[n]$.

For the second claim of the theorem, we note that $A[m] \cap A[n] = 0$ and $a = (um+nv)a = u(ma)+v(na) = m(ua)+n(va)$ shows that any $a \in A$ can be written as an element of $mA = A[n]$ plus an element of $nA = A[m]$. Thus $A[m]+A[n] = A$. This shows A is the internal direct product of $A[m]$ and $A[n]$. $\square$

Proposition 8.9. *Suppose that $A_1 \times B_1 \cong A_2 \times B_2$ where everything in A_i has order dividing m and everything in B_i has order dividing n, and m, n coprime. Then $A_1 \cong A_2$ and $B_1 \cong B_2$.*

Proof. Assume $A_1 \times B_1 \cong A_2 \times B_2$.

$$\begin{aligned} m(A_i \times B_i) &= mA_i \times mB_i \\ &= \{(0, mb) : b \in B_i\} \\ &= \{0\} \times B_i \end{aligned}$$

The first step because $m(a, b) = (ma, mb)$ and the last step because multiplication by m (coprime to n) gives an automorphism of B_i. Since $m(A_1 \times B_1) \cong m(A_2 \times B_2)$ we get $B_1 \cong B_2$. Similarly we show $A_1 \cong A_2$. □

Corollary 8.10. *Let $|A| = p_1^{e_1} \dots p_s^{e_2}$ then*

$$A \cong A[p_1^{e_1}] \times \cdots \times A[p_s^{e_s}] = A(p_1) \times \cdots \times A(p_s)$$

This factorization is unique up to reordering.

Proof. Apply induction using the previous propositons. □

The previous theorem is the first step in the classification of finite abelian groups. The next step is to classify p-groups. The key lemma follows. Its proof is quite technical and not very illuminating, so I sketch the proof in [Hungerford Sec 8.2].

Lemma 8.11. *Let A be a p-group and let a be an element of maximal order. Then $A = \langle a \rangle + K$ for some subgroup K of A.*

Proof. Let K be as large as possible such that $K \cap \langle a \rangle = \{0\}$. We want to show that $K + \langle a \rangle = A$. Then the internal direct product theorem says that $A \cong K \times \langle a \rangle$.

Suppose $b \in A \setminus (K + \langle a \rangle)$. Do some tricks to show:

(1) Show there is a $c \in A \setminus (K + \langle a \rangle)$ such that $pc \in K + \langle a \rangle$. [Take the minimal r such that $p^r b \in K + \langle a \rangle$, then let $c = p^{r-1} b$.

(2) Show there is a $d \in A \setminus (K + \langle a \rangle)$ such that $pd \in K$. [Let $pc = k + ma$, argue that $m = pm'$, for some integer m' using that a has maximal degree in A and $K \cap \langle a \rangle = \{0\}$. Then set $d = c - m'a$.]

By assumption on K, $(K + \langle d \rangle) \cap \langle a \rangle \neq \{0\}$, so there is some $k \in K$, and nonzero $r, s \in \mathbb{Z}$ such that $k + rd = sa$.

Now we consider two cases: If $p \mid r$ then $rd \in K$ and consequently $sa \in K$. This contradicts $K \cap \langle a \rangle = \{0\}$. If $p \not| r$ then there are u, v such that $up + rv = 1$. Then $d = u(pd) + v(rd)$. The first term is in K and the second in $K + \langle a \rangle$, so $d \in K + \langle a \rangle$, which is a contradiction. □

Theorem 8.12. *Let A be a p-group. Then A is the direct product of cyclic groups each of which has order a power of p. Consequently, the order of A is also a power of p.*

The decomposition is unique (up to reordering). Put another way, two p-groups are isomorphic iff their decompositions have the same number of factors for each power of p.

Proof. The proof is by induction. Using the lemma we can write $A = \langle a \rangle + K$. The subgroup $\langle a \rangle$ is cyclic of order p^k for some k. Applying the induction hypothesis to K gives the result. Since A is the direct product of groups of order a power of p, A itself must have order a power of p.

Clearly, if two groups have the same number of factors for each power of p they are isomorphic. To prove the converse, suppose

$$A \cong (\mathbb{Z}/p)^{k_1} \times (\mathbb{Z}/p^2)^{k_2} \times \cdots \times (\mathbb{Z}/p^r)^{k_r}$$

So some factorization of A has k_i terms equal to $\mathbb{Z}/p^i$. We can recover the k_i iteratively. Since $\log_p(\mathbb{Z}/p^n) = n$, we have $\log_p(|A|) = \sum_{i=1}^r ik_i$. Notice that $p^{n-1}\mathbb{Z}/p^n \cong \mathbb{Z}/p$ and $p^k\mathbb{Z}/p^n$ is trivial for $k \geq n$. Thus the subgroup $p^{r-1}A$ is isomorphic to

$$p^{r-1}A \cong (\mathbb{Z}/p)^{k_r}$$

Thus we have $\log_p(|p^{r-1}A|) = k_r$. Similar computations for p^iA with $i = r-2, r-3, \ldots, 1$ allows one to recover the other k_i. (Try it as an exercise!)

□

From the two previous theorems we obtain the fundamental theorem.

Theorem 8.13 (Fundamental Theorem of Finite Abelian Groups)**.** *Let A be an abelian group of order $p_1^{e_1} \ldots p_r^{e_r}$. Then A is a direct product of cyclic groups, each having order a power of one of the p_i. If we write*

$$A(p_i) \cong \mathbb{Z}/p_i^{a_{i,1}} \times \mathbb{Z}/p_i^{a_{i,2}} \times \ldots \mathbb{Z}/p_i^{a_{i,s_i}}$$

then for each i, $\sum_{\ell=1}^{s_i} a_{i,\ell} = e_i$. The decomposition is unique, up to reordering.

Problems 8.14.

(1) Classify all abelian groups of order 84,000.

(2) Let A be an abelian group and let T be the set of elements with finite order. Show that T is a subgroup of A. Show that A/T has no elements of finite order.

(3) Give an example of a finitely generated group in which the elements of infinite order do *not* form a subgroup. (Compare with the previous problem.)

(4) Let $G \longrightarrow \mathbb{Z}$ be a surjective homomorphism. Show that G has a subgroup H and an element a such that G is the internal direct product $H \times \langle a \rangle$.

(5) Let G be a finite abelian p-group. Use the classification of finite abelian groups to show that $pG < G$. Under what conditions is $pG = 0$?

(6) Show that $pG = G$ is possible for an infinite group.

9 Free groups, generators and relations

Definition 9.1. G is called a cyclic extension of N when $G/N \cong C_r$ where C_r is the cyclic group of order r.

Example 9.2. The quaternions are a 2-cyclic extension of $\mathbb{Z}/4$. The dihedral group D_r is a 2-cyclic extension of $\mathbb{Z}/r$.

Consider the exact sequence for N an r-cyclic extension of N.

$$1 \longrightarrow N \longrightarrow G \longrightarrow C_r \longrightarrow 1$$

Let's probe this a bit. Let $h \in G$ be such that Nh generates C_r. So

$$Ne = (Nh)^r = Nh^r$$

so $h^r \in N$ (and furthermore no lower power of h is in N). We also have the conjugation by h map, φ_h, restricts to N to give an automorphism of N. A priori it is not an inner automorphism of N since $h \notin N$. We do have that $\varphi_h^r = \varphi_{h^r}$ is an inner automorphism of N since $h^r \in N$. Furthermore $\varphi_h(h^r) = h^r$ (check!).

We now "reverse" the discussion above: we show how to create a new group G from N and r and some other information.

Definition 9.3. Let N be a group, r a positive integer, $v \in N$ and $\tau \in \mathrm{Aut}(N)$ satisfy the following two conditions:

(1) $\tau(v) = v$

(2) $\tau^r = \varphi_v$

Define a new group G—the r-cyclic extension of N defined by τ and v—whose elements are na^i with $n \in N$ and $i \in \{0, \dots, r-1\}$ and with multiplication defined by

$$\begin{aligned} a^r &= v \\ an &= \tau(n)a \end{aligned}$$

for any $n \in N$.

Problems 9.4.

(1) Show that

$$n_1 a^i n_2 a^j = \begin{cases} n_1 \tau^i(n_2) a^{i+j} & \text{when } i+j < r \\ n_1 \tau^i(n_2) v a^{i+j} & \text{when } i+j \geq r \end{cases}$$

(2) Show that the axioms of a group are satisfied by the definition above. (non-trivial!)

(3) Let $N = C_4 = \langle n \rangle$. Then τ must be either the identity map or the map taking n to n^{-1}. Show that in the latter case v must be e or n^2.

(4) Let $\tau : n \mapsto n^{-1}$. Show that $v = e$ and $v = n^2$ give the groups Q and D_4, but which is which?!

(5) Investigate the groups obtained by taking τ the identity map.

(6) Show that when N is abelian and τ is the identity the construction gives an abelian group.

Definition 9.5. Define the group Dic_r via generators and relations by

$$\mathrm{Dic}_r = \langle n, a \mid n^{2r} = e; a^2 = n^r; an = n^{-1}a \rangle$$

Problems 9.6.

(1) Show that Dic_r is a 2-cyclic extension of C_{2r} and identify an appropriate τ and v from the definition.

(2) Show that any element of Dic_r may be written uniquely in the form $n^i a^j$ for $i \in \{0, \dots, 2r-1\}$ and $j \in \{0, 1\}$.

(3) Find a general formula for the product of two elements in Dic_r.

(4) Find the order of each element of Dic_r. [Square $n^i a$.]