5. Abelian groups and semi-direct products

Direct products

If $G_1, \ldots, G_n$ are groups, the direct product $G = G_1 \times \cdots \times G_n$ is the group whose elements are n-tuples $(g_1, \ldots, g_n)$, with $g_i \in G_i$, and all operations done componentwise.

Definition: If G is a group and H and K are normal subgroups of G with $HK = G$ and $H \cap K$ trivial, then the map $(h, k) \to hk$ from $H \times K \to HK = G$ is an isomorphism. G is called the internal direct product of H and K.

Fundamental theorem of finitely generated abelian groups

Definition: A group is *finitely generated* if it has a finite generating set.

Finitely generated groups can be finite or infinite. For example $\mathbb{Z}^n$ is finitely generated.

Proposition: An abelian group G is finitely generated if and only if there is an integer k and a surjective homomorphism

$$f : \mathbb{Z}^k \to G.$$

Proof: If f exists, then G is generated by $f(e_i)$ for $i = 1, \ldots, k$, where e_i is the element of $\mathbb{Z}^k$ with a 1 in position i and zeroes elsewhere.

Conversely, if G is generated by $g_1, \ldots, g_k$, define $f : \mathbb{Z}^k \to G$ by $f(e_i) = g_i$.

Theorem: Let G be a finitely generated abelian group. Then there are integers

$$r \geq 0$$

and $n_1, \ldots, n_s$, all at least 2, such that

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

and such that $n_{i+1} | n_i$ for $i = 1, \ldots, s - 1$.

The integer r is called the *free rank* of G, and the n_i are called the *invariant factors*. Two finitely generated abelian groups are isomorphic if and only if they have the same rank and the same invariant factors.

Example: If G has order 20, then its possible invariant factors are:

1. 20, in which case it's cyclic and also isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
2. 10 and 2 in which case it's $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Alternatively, suppose that G is finite of order n and $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of n. Then G is a product of its Sylow p-subgroups A_i which have orders $p_i^{a_i}$. Each abelian p-group A_i is a product of cyclic p-groups of order $p^{a_{ij}}$ for $j = 1, \ldots, t$ where $a_{i1} + a_{i2} + \cdots + a_{is} = a_{ij}$. If you arrange the a_{ij} so that the primes are in increasing order and the exponents are in decreasing (or increasing) order then the $p_i^{a_{ij}}$ determine the group up to isomorphism. The powers $p^{a_{ij}}$ are called the *elementary divisors* of G.

Example: If G has order 20, then the elementary divisors are either $5, 4$ (if the group is cyclic) or $5, 2, 2$ if not.

Semidirect products

Definition: Let H and K be groups and let $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. Write ϕ_k for the map $H \to H$ associated by ϕ to $k \in K$. The *semidirect product* $P = H \rtimes_\phi K$ of H and K by ϕ is defined as follows:

1. As a set, it consists of pairs (h, k).
2. The group law is $(h_1, k_1)(h_2, k_2) = (h_1 \phi_{k_1}(h_2), k_1 k_2)$.
3. The groups $H = \{(h, 1) : h \in H\}$ and $K = \{(1, k) : k \in K\}$ are included in P as subgroups.
4. P has $|H||K|$ elements.
5. H is a normal subgroup of P. In fact $(1, k)(h, 1)(1, k^{-1}) = (\phi_k(h), 1)$. So the conjugation action of K on H is given by the automorphism ϕ.
6. The quotient group P/H is isomorphic to K.

Example: Let $R = \mathbb{Z}/n\mathbb{Z}$, where n is odd, and let $S = \mathbb{Z}/2\mathbb{Z}$. The cyclic group $\mathbb{Z}/n\mathbb{Z}$ (written multiplicatively) has an automorphism $\phi(x) = x^{-1}$ of order 2. Let s be the generator of S and define $\phi_s(x) = x^{-1}$ for $x \in R$. Then $R \rtimes_\phi S$ is a group of order $2n$. Writing $(x, 1) = x$ and $(1, s) = s$, the computation above shows that $sx = (1, s)(x, 1) = (x^{-1}, s) = (x^{-1}, 1)(1, s)x^{-1}s$ or, in other words, the group P we have constructed is the dihedral group with $2n$ elements.

Example: Let $R = \mathbb{Z}/11\mathbb{Z}$. The automorphism group of R is cyclic of order 10 generated by 2. Let U be the cyclic group of order 10 generated by y, with $\phi_y(x) = x^2$ for $x \in R$.
Then $P = R \rtimes_\phi U$ is a group of order 110 generated by $x = (1, 0)$ and $y = (0, 1)$ satisfying $x^{11} = y^{10} = 1$ and $yx = x^2 y$.