Abelian Groups

Commutative groups are also called abelian groups in honour of Nils Henrik Abel who did some pioneering work in algebra, number theory and geometry.

We will write the binary operation for an abelian group M using the symbol $+$ as our intuition about addition will be in handy while thinking about this operation. Similarly, we will use $-m$ to denote the inverse of the element m of M. This will fit in nicely with our intuition about subtraction. Finally, we will use 0 for the identity element of the group M as this will fit in with our usual use of 0 for additive identity.

The underlying additive structure of a ring is an abelian group. Moreover, if M is an abelian group, then the collection $\mathrm{End}(M)$ of endomorphisms of M is a ring as follows. If $f : M \to M$ and $g : M \to M$ are endomorphism we define $f + g$ by

$$(f + g)(m) = f(m) + g(m)$$

Exercise: Check that $f + g$ is an endomorphism of the abelian group M.

We define the product as composition $(f \circ g)(m) = f(g(m))$.

Exercise: Check that the composition of endomorphisms is also an endomorphism of M.

The $\underline{0}$ endomorphism of M is the one that sends every element of M to 0. The $\underline{1}$ endomorphism of M is the identity map with sends every element of M to itself.

Exercise: With the above definitions, check that $\mathrm{End}(M)$ is a ring.

In particular, we see that we have the natural ring homomorphism $\mathbb{Z} \to \mathrm{End}(M)$.

Exercise: This homomorphism sends a positive integer k to the endomorphism that sends m to the sum of k copies of itself. Similarly, this homomorphism sends a negative integer $-k$ to the endomorphism that sends m to the sum of k copies of $-m$.

In order to simplify notation we will use $k \cdot m$ for the result of applying the endomorphism associated with an integer k to the element m of the abelian group M. Again, this will fit in nicely with our intuition for multiplication.

Conversely, given a ring R, we can give a natural map $\ell : R \to \mathrm{End}((R, +))$ where the symbol $(R, +)$ is used to denote the underlying additive group of R. We define $\ell(a)$ to be the endomorphism that sends b to $a \cdot b$ for every b in R.

Exercise: Use the (left) distributive law in R to show that $\ell(a)$ is an endomorphism of $(R, +)$.

In other words, the map ℓ sends an element a of R to the endomorphism of $(R, +)$ given by left multiplication by a.

Exercise: Use associativity of multiplication in R to show that $\ell(a) \circ \ell(b) = \ell(a \cdot b)$.

Thus, the map ℓ preserves multiplication. Similarly,

Exercise: Use the right distributive law in R to show that $\ell(a+b) = \ell(a) + \ell(b)$ where the right-hand side is addition of endomorphisms of $(R, +)$.

Hence, the map ℓ preserves multiplication.

Exercise: Use the additive identity law to show that $\ell(1)$ is $\underline{1}$, the identity endomorphism of $(R, +)$.

Similarly, we can see that $\ell(0) = \underline{0}$. Combining all these results we see that ℓ is a ring homomorphism.

In other words, *any* ring can be seen as a subring of the ring of endomorphisms of *some* abelian group.

This can be seen as the justification for studying abelian groups as a preliminary to studying rings!

Orders of Elements

Given an element a in an abelian group M, let us assume that its order m is finite.

Exercise: If p is any integer, then show that the order of $p \cdot a$ divides m.

Exercise: If p and m have no common factor, then show that the order of $p \cdot a$ is m.

On the other suppose that k is a divisor of m, i.e. $k|m$.

Exercise: Show that the element $k \cdot a$ has order *exactly* m/k.

Exercise: Combine the above two exercises to show that if the order of $p \cdot a$ is m/k where k the greatest common divisor of p and m.

Now suppose that we are given another element b of M which has order n which is also finite.

Exercise: If m and n have no common factor then show that if some multiple $p \cdot a$ *equals* some multiple $q \cdot b$ then both of these are the 0 element of M. (Hint: The order of $p \cdot a$ is a divisor of m and that of $q \cdot b$ is a divisor of n.)

As a consequence, we can show

Exercise: If m and n have no common factor then the order of $a + b$ is $m \cdot n$.

On the other hand, if m and n do have a common factor, then we cannot expect to “create” an element of order $m \cdot n$. For example, a and b could be equal! In that case, any combination of a and b is a multiple of a, and so its order *divides* m. However, we can show

Exercise: Given positive integers m and n there is a divisor k of m and a divisor l of n so that:

- k and l have no common factor.
- The least common multiple of m and n is $k \cdot l$.

(Hint: Let k be product of those prime powers dividing m that are the same as the prime powers dividing the least common multiple of m and n. Let l be the product of the remaining prime powers dividing the l.c.m. of m and n.)

Exercise: With a, b in M as above and m, n, k and l positive integers as above show that $(m/k) \cdot a + (n/l) \cdot b$ has order equal to the least common multiple of the m and n.

Conversely, this is the largest possible order of an additive combination of a and b:

Exercise: (Starred) Given a and b in M of order m and n respectively, show that the order of any element of the form $p \cdot a + q \cdot b$ divides the least common multiple of m and n.

Finite Abelian Groups

We will now apply the above results to the study of finite abelian groups. The "model" for such groups is the additive group $\mathbb{Z}/n$. (We use the same notation for the ring and the underlying additive group!)

Every element of a finite abelian group M is finite and there are finitely many such elements. Repeatedly applying the results of the previous section, we can produce an element a whose order is the least common multiple of the orders of all elements of M. It follows that:

Exercise: The maximum of all orders of elements of finite abelian group M is the least common multiple of these orders.

Exercise: Check that the order of every non-zero element of $\mathbb{Z}/2 \times \mathbb{Z}/2$ is 2.

It follows that least common multiple *could* be smaller than the size of the group. (Recall that the order of an element divides the order of the group.)

Exercise: Check that the order of the element $(1, 1)$ of $\mathbb{Z}/2 \times \mathbb{Z}/3$ is 6.

Given an element a in M of order n, we get a group homomorphism $\mathbb{Z}/n \to M$ which sends k to $k \cdot a$ and this homomorphism is one-to-one. Let us denote the image as $(\mathbb{Z}/n) \cdot a$.

Now, let b be another element of M and suppose that $\bar{b} = b + (\mathbb{Z}/n) \cdot a$. Suppose $s \cdot b$ lies in $(\mathbb{Z}/n) \cdot a$. Now, if u is the order of b in M then $u \cdot b = 0$ also lies in the subgroup $(\mathbb{Z}/n) \cdot a$ of M.

Exercise: Let p be the greatest common divisor of s and u, then $p \cdot b$ also lies in $(\mathbb{Z}/n) \cdot a$. (Hint: The integer p can be written as an additive combination of s and u.)

Hence, if s is the smallest with the property that $s \cdot b$ lies in $(\mathbb{Z}/n) \cdot a$, then s divides the order u of b. Then the order of $s \cdot b$ is u/s. On the other hand, since $s \cdot b = t \cdot a$, its order is n/k where k is the greatest common divisor of n and t. Hence, we get $n/k = u/s$.

Exercise: Suppose that u divides n and s divides u. Now if k is a divisor of n so that $n/k = u/s$, show that s divides k.

Hence, if u divides n, we have s divides k and hence s divides t; we write $t = sq$. If we put $b' = b - q \cdot a$, then $s \cdot b' = s \cdot b - t \cdot a = 0$. So the order of b' is s.

We will now combine the above results to prove the following result.

Theorem: A finite abelian group is isomorphic to

$$(\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_r)$$

where n_1 divides n_2, and so on upto n_r.

Proof: We will show this by induction on the size of the finite abelian group M.

As seen above, we have an element a_r in M whose order is the least common multiple n_r of the orders of all elements of M. We put $M_1 = M/(\mathbb{Z}/n_r) \cdot a_r$. By induction we have

$$M_1 = (\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_{r-1})$$

Given any element $\underline{b}$ of M_1, we have shown above that there is an element b of M so that $b + (\mathbb{Z}/n_r) \cdot a_r$ is $\underline{b}$ and the order of b is the same as the order of $\underline{b}$. (Since this order divides the order of a_r.)

It follows that (for each i) we can pick an element a_i of M that sof order n_i whose image in $(\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_{r-1})$ is the image $(0, \ldots, 1, \ldots, 0)$ which has 1 in the i-th place and 0 elsewhere.

The map that sends $(k_1, \ldots, k_r)$ to $k_1 \cdot a_1 + \cdots + k_r a_r$ then gives the required isomorphism between $(\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_r)$ and M.