

THE FUNDAMENTAL THEOREM OF FINITELY GENERATED ABELIAN GROUPS

In this handout, we give a proof of the fundamental theorem of finitely generated abelian groups.

Theorem 1. *Every finitely generated abelian group is the product of finitely many cyclic groups.*

As a starting point, we will need the following lemma.

Lemma 2. *If A is a subgroup of \mathbb{Z}^n , then A is finitely generated.*

Proof. If we regard \mathbb{Z}^n as a subset of \mathbb{Q}^n , then we can regard elements of A as elements of \mathbb{Q}^n , and in this context it makes sense to speak of a subset of A as being linearly independent (or not). Let v_1, \dots, v_k be any maximal linearly independent subset of A (note that $k \leq n$ since \mathbb{Q}^n is n -dimensional). Let B be the subgroup of A generated by v_1, \dots, v_k . What we want to do is prove that B has finite index in A : to see that this suffices, observe that if $[A : B]$ is finite and w_1, \dots, w_ℓ are coset representatives for B in A , then A is generated by $v_1, \dots, v_k, w_1, \dots, w_\ell$.

Proving that $[A : B]$ is finite is a little bit trickier than one might hope. Here's one argument, not necessarily the shortest. The key is to find an integer N such that $N \cdot A \subset B$. Extend the linearly independent set v_1, \dots, v_k to a basis v_1, \dots, v_n of \mathbb{Q}^n ; clearing the denominators of v_{k+1}, \dots, v_n if necessary, we may assume that v_{k+1}, \dots, v_n also lie in \mathbb{Z}^n . By linear algebra, any element of \mathbb{Q}^n will be a rational linear combination of v_1, \dots, v_n in a unique manner. If $e_i \in \mathbb{Z}^n$ is a standard basis vector, we write

$$e_i = a_{1i}v_1 + \cdots + a_{ni}v_n$$

with each $a_{ji} \in \mathbb{Q}$. Let N be a common denominator for all the a_{ji} ($1 \leq i, j \leq n$). Then Ne_i is an integer linear combination of v_1, \dots, v_n for all i ; it follows that Nw is an integer linear combination of v_1, \dots, v_n for any $w \in \mathbb{Z}^n$.

Now suppose that $w \in A$. By the previous paragraph, there is a unique expression

$$(0.1) \quad Nw = c_1v_1 + \cdots + c_nv_n,$$

and in this expression we have $c_i \in \mathbb{Z}$ for all i . Since v_1, \dots, v_k are linearly independent but w, v_1, \dots, v_k are linearly dependent, we see that w is a linear combination of v_1, \dots, v_k alone. The same must be true of Nw , and since the linear combination (0.1) is unique, we conclude that c_{k+1}, \dots, c_n are all equal to zero and $Nw = c_1v_1 + \cdots + c_kv_k$ with $c_i \in \mathbb{Z}$ for all i . This proves that $Nw \in B$ for all $w \in A$, so that $N \cdot A \subset B$.

We are almost done. Since $B \subset A$ we have $N \cdot B \subset N \cdot A$, and we have the inclusions

$$N \cdot B \subset N \cdot A \subset B$$

and in particular $[(N \cdot A) : (N \cdot B)] \leq [B : (N \cdot B)]$. Since B is generated by k elements, we have $[B : (N \cdot B)]$ finite (in fact it is at most N^k), and therefore $[(N \cdot A) : (N \cdot B)]$ is finite. Note that the multiplication-by- N map $A \mapsto N \cdot A$ is an

isomorphism (because A contains no elements of finite order), and this map carries B to $N \cdot B$. Hence $A/B \cong (N \cdot A)/(N \cdot B)$, and in particular $[A : B] = [(N \cdot A) : (N \cdot B)]$. We have already seen that the latter is finite, and therefore $[A : B]$ is. \square

Now we return to the main theorem.

Proof of Theorem 1. Suppose that A is a finitely generated abelian group, and let v_1, \dots, v_n be generators of A . There is a surjection $\varphi : \mathbb{Z}^n \rightarrow A$ sending the i th standard basis vector of \mathbb{Z}^n to v_i . By Lemma 2 the kernel $B = \ker(\varphi)$ is finitely generated. Let b_1, \dots, b_m be generators of B . There is a map

$$f : \mathbb{Z}^m \rightarrow \mathbb{Z}^n$$

sending the i th standard basis vector in \mathbb{Z}^m to b_i , and $\text{im}(f) = B$. It follows that $A \cong \text{coker}(f)$.

We are now reduced to the statement: if G is a free abelian group on a basis of size n and $f : \mathbb{Z}^m \rightarrow G$ is a homomorphism, then $\text{coker}(f)$ is a product of cyclic groups. Recall that once we have chosen a basis of \mathbb{Z}^m and a basis of G , then the map f is given by an n -by- m matrix, as follows. Let e_1, \dots, e_m be our basis of \mathbb{Z}^m , and x_1, \dots, x_n our basis of G ; if $f(e_j) = \sum_{i=1}^n m_{ij}x_i$ then $M = (m_{ij})$. That is, the j th column of M gives the image of e_j .

Suppose we replace M with another matrix M' obtained by performing any one of the following three column operations on M :

- (1) interchange any two columns;
- (2) replace a column with its negative;
- (3) add an integer multiple of one column to a different column.

If we form the map $f' : \mathbb{Z}^m \rightarrow G$ corresponding to this new matrix M' , observe that $\text{im}(f') = \text{im}(f)$. For instance, if we add c times the j th column to the k th column then $f'(e_k) = cf(e_j) + f(e_k)$, and the subspace of G generated by $f(e_1), \dots, f(e_m)$ is the same as the subspace of G generated by $f(e_1), \dots, cf(e_j) + f(e_k), \dots, f(e_m)$. Since $\text{im}(f') = \text{im}(f)$, we also have $\text{coker}(f) = \text{coker}(f')$, and therefore we can perform column operations on M without changing the isomorphism type of the cokernel.

Next we want to prove the same statement for row operations, which is a bit more complicated. One checks that any of the following operations yield another basis of G :

- (1) interchange x_i and x_j for some i, j ;
- (2) replace x_i with $-x_i$ for some i ;
- (3) replace x_i with $x_i - cx_j$ for some $j \neq i$ and $c \in \mathbb{Z}$.

Suppose we interchange x_i and x_j ; in terms of this new basis, the matrix of the map f becomes the matrix M' obtained by swapping rows i, j of M . The other operations are similar (note that if we replace x_i with $x_i - cx_j$, the effect is to add c times row j from row i). Since the map f is unchanged, the cokernel is unchanged. Thus we may perform the following row operations on M without changing the cokernel of f :

- (1) interchange any two rows;
- (2) replace a row with its negative;
- (3) add an integer multiple of one row to a different row.

We have shown that if we begin with a map $f : \mathbb{Z}^n \rightarrow G$ given by the matrix M , then we can perform any combination of row and column operations on M without changing the cokernel.

Suppose M has a nonzero entry in either the first row or the first column; then it is possible (through swaps and sign changes) to put a positive integer in the 1, 1-entry. Let M'_1 be a matrix that can be obtained from M by these operations that has the smallest possible positive integer in the 1, 1-entry. Let a_{11} denote this entry. I claim that a_{11} divides all other entries in the first row and column. Suppose, e.g., that a is an entry in the first row; the division algorithm gives $a = qa_{11} + r$ with $0 \leq r < a_{11}$. Subtracting q times the first column from the column containing a puts an r in the first row, and swapping this column with the first column puts r in the 1, 1-entry. By choice of M'_1 , we have $r = 0$.

Now subtract the appropriate multiple of the first row from other rows, and the appropriate multiple of the first column from other columns, so that all other entries in the first row and column become zero.

At the end of this procedure, we obtain a matrix M_1 in which the 1, 1-entry is a nonnegative integer m_{11} , and all other entries in the first row and column are zero. (Note that $a_{11} = 0$ if and only if the entire first row and column were zero to begin with.)

Repeating this procedure with the second row/column, and so forth, we can use these row and column operation to transform M into a matrix M' in which the only nonzero entries are along the diagonal. Denote these diagonal elements by a_{ii} for $1 \leq i \leq \min(i, j)$. Let $a_{ii} = 0$ for $\min(i, j) < i \leq \max(i, j)$. We are now reduced to considering maps $f : \mathbb{Z}^n \rightarrow G$, where G is a free abelian group on the basis x_1, \dots, x_n , and in which f (given by the matrix M') send $e_i \mapsto a_{ii}x_i$ for $1 \leq i \leq n$. The cokernel of G is evidently isomorphic to

$$\mathbb{Z}/a_{11}\mathbb{Z} \times \cdots \times \mathbb{Z}/a_{nn}\mathbb{Z}$$

and we are done. □

Corollary 3. *If A is a subgroup of \mathbb{Z}^n , then A is a free abelian group of rank m for some $m \leq n$.*

(Contrast this with the behavior of free (nonabelian) groups, in which a subgroup of a free group may be free of larger rank.)

Proof. By Lemma 2, the group A is finitely generated. The group A contains no elements of finite order (since the same is true by \mathbb{Z}^n), and so by Theorem 1, the group A is free abelian of rank m for some m . Since the generators of $A \subset \mathbb{Z}^n$ are linearly independent in \mathbb{Z}^n , hence in \mathbb{Q}^n , we get $m \leq n$. □