

NOTES ON THE FUNDAMENTAL THEOREM ON FINITELY  
GENERATED ABELIAN GROUPS

**Theorem 1.** *Let  $G$  be a free abelian group of rank  $n$ , and let  $H$  be a subgroup of  $G$ . Then:*

- (a)  $H$  is free of rank  $m \leq n$ .
- (b) There exists a basis  $u_1, \dots, u_n$  for  $G$  and positive integers  $c_1, \dots, c_m$  such that  $c_1u_1, \dots, c_mu_m$  forms a basis for  $H$ .
- (c) The index  $[G : H]$  is finite if and only if  $m = n$ . In this case, let  $x_1, \dots, x_n$  (resp.  $y_1, \dots, y_n$ ) be any basis for  $G$  (resp.  $H$ ), and write

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

with  $A \in M_n(\mathbf{Z})$ . Then  $[G : H] = |\det(A)|$ .

*Proof.* (Sketch)

We proceed by induction on  $n$ . If  $n = 1$  then  $H = a\mathbf{Z}$  for some  $a \in \mathbf{Z}$  and therefore  $H$  is free of rank 1 (if  $a \neq 0$ ) or 0 (if  $a = 0$ ). In general, we identify  $G$  with  $\mathbf{Z}^n$  and let  $\pi : \mathbf{Z}^n \rightarrow \mathbf{Z}$  be projection onto the last coordinate. Let  $H' = \ker(\pi) \cap H$  and let  $H'' = \pi(H)$ . Then by induction  $H'$  is free of rank  $\leq n-1$  (since  $H'$  is isomorphic to a subgroup of  $\mathbf{Z}^{n-1}$ ) and  $H''$  is free of rank at most 1. If  $H'' = (0)$  then  $H = H'$  and we are done. Otherwise,  $H'' = a\mathbf{Z}$  is free of rank 1. Choose  $x \in H$  such that  $\pi(x) = a$ . Then  $\pi$  maps  $G'' := x\mathbf{Z}$  isomorphically onto  $H''$ , so to prove (a) it suffices to prove that  $H = H' \oplus G''$ . This is straightforward and we leave it to the reader.

We assume  $m = n$  and prove (b) and (c) at the same time. (We leave the case  $m < n$  to the reader). Let  $x = [x_1, \dots, x_n]^t$  (resp.  $y = [y_1, \dots, y_n]^t$ ) be a basis for  $G$  (resp.  $H$ ), and write  $y = Ax$  with  $A \in M_n(\mathbf{Z})$ . The reader can verify that performing an elementary column operation on  $A$  corresponds to replacing  $x$  by another basis  $x'$ . Similarly, performing an elementary row operation on  $A$  corresponds to replacing  $y$  by another basis  $y'$ . Therefore, it is enough to prove that by performing elementary row and column operations on  $A$ , we can obtain a diagonal matrix. (Convince yourself that this is enough).

For this, it is enough by symmetry and induction to use elementary row operations to obtain a matrix  $A'$  with  $a'_{i1} = 0$  for all  $i > 1$ . This can be done using the division algorithm and induction on  $M :=$

$\max\{|a_{i1}| : i > 1\}$ : Swap rows if necessary so that  $|a_{11}| \leq |a_{i1}|$  for  $i > 1$ . Then add a suitable integer multiple of row 1 to row  $i$  for each  $i > 1$  so that  $M$  is decreased.  $\square$

**Theorem 2** (Fund. Thm. on F.G. Abelian Groups). (a) *If  $G$  is a finitely generated abelian group, then  $G$  is isomorphic to the direct product of finitely many cyclic groups.*

(b) *More specifically, there is an integer  $r \geq 0$ , prime numbers  $p_1, \dots, p_k$  (not necessarily distinct), and positive integers  $\alpha_1, \dots, \alpha_k$  such that*

$$(1) \quad G \cong \mathbf{Z}^r \times (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z}) \times \cdots \times (\mathbf{Z}/p_k^{\alpha_k}\mathbf{Z}).$$

*Moreover, the integer  $r$  (called the rank of  $G$ ) and the integers  $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$  (called the elementary divisors of  $G$ ) are uniquely determined (up to re-ordering the invariant factors).*

*Proof.* (Sketch) Part (a) follows easily from the previous theorem, since  $(\langle u_1 \rangle \times \cdots \times \langle u_n \rangle) / (\langle c_1 u_1 \rangle \times \cdots \times \langle c_m u_m \rangle) \cong (\mathbf{Z}/c_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/c_m\mathbf{Z}) \times \mathbf{Z}^{n-m}$ .

The existence of the elementary divisor decomposition in part (b) follows from the Chinese Remainder Theorem, which says that if  $\gcd(a, b) = 1$  then  $\mathbf{Z}/ab\mathbf{Z} \cong \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$ . The fact that  $r$  is uniquely determined by  $G$  follows from the fact that  $G' = G/G_{\text{tor}} \cong \mathbf{Z}^r$ , and  $G'/2G' \cong (\mathbf{Z}/2\mathbf{Z})^r$ , so  $|G'/2G'| = 2^r$ . We leave the uniqueness of the elementary divisors as an exercise for the reader (consider the groups  $pG_{\text{tor}}$  and  $G/pG_{\text{tor}}$  and use induction).  $\square$