Finitely Generated Abelian Groups and Smith Normal Form

Dylan C. Beck

Groups Generated by a Subset of Group Elements

Given a group G and a subset X of G, consider the set

$$\langle X \rangle = \{g_1^{n_1} \cdots g_k^{n_k} \mid k \geq 0,\, n_i \in \mathbb{Z}, \text{ and } g_i \in X\}.$$

Proposition 1. We have that $\langle X \rangle$ is a subgroup of G.

Proof. Given that $k = 0$, we have that $g_1^{n_1} \cdots g_k^{n_k} = e_G$ by definition of the empty product. Consequently, the set $\langle X \rangle$ is nonempty. By the one-step subgroup test, it suffices to prove that if g and h are in $\langle X \rangle$, then gh^{-1} is in $\langle X \rangle$. We leave it to the reader to establish this. □

We refer to the subset $\langle X \rangle$ of G as the subgroup of G **generated** by X; the elements of X are said to be the **generators** of $\langle X \rangle$. Given that $|X|$ is finite, we say that $\langle X \rangle$ is **finitely generated**.

Remark 1. Every finite group $G = \{e_G, g_1, \dots, g_n\}$ is finitely generated by $e_G, g_1, \dots, g_n$.

Proposition 2. We have that $\langle X \rangle = \bigcap_{H \in \mathscr{C}} H$, where $\mathscr{C} = \{H \leq G \mid X \subseteq H\}$ is the collection of all subgroups H of G that contain the set X.

Proof. Consider a subgroup H of G with $X \subseteq H$. Given any element $g_1^{n_1} \cdots g_k^{n_k}$ of $\langle X \rangle$, it follows that $g_1^{n_1} \cdots g_k^{n_k}$ is in H by hypothesis that H is a subgroup of G that contains X. Certainly, this argument holds for all subgroups H of G with $X \subseteq H$, hence we have that $\langle X \rangle \subseteq \bigcap_{H \in \mathscr{C}} H$.

Conversely, observe that $\langle X \rangle$ is a subgroup of G that contains X. Explicitly, by Proposition 1, we have that $\langle X \rangle$ is a subgroup of G, and for each element g in X, we have that $g = g_1^{n_1} \cdots g_k^{n_k}$ for some integer $k \geq 1$, where $g_1 = g$, $n_1 = 1$, and $n_i = 0$ for all $2 \leq i \leq k$. Consequently, we have that $\bigcap_{H \in \mathscr{C}} H = \langle X \rangle \bigcap_{H \in \mathscr{C}} H \subseteq \langle X \rangle$. We conclude that $\langle X \rangle = \bigcap_{H \in \mathscr{C}} H$. □

Given a finitely generated group G with set of generators X, we refer to a **relation** among the generators of G as an equation involving the elements of $X \cup \{e_G\}$. We are already familiar with some relations on G. Given an element g of finite order, we have the relation $g^{\operatorname{ord}(g)} = e_G$. Given an element g in the center $Z(G)$ of G (if it is nontrivial) and any element h of G, we have the relation $gh = hg$ or $g^{-1}h^{-1}gh = e_G$. Further, if we assume that every relation among the generators of G can be deduced from the finitely many relations $\mathscr{R}_1, \dots, \mathscr{R}_n$ of the elements of $X \cup \{e_G\}$, then we refer to the object $G = \langle X \mid \mathscr{R}_1, \dots, \mathscr{R}_n \rangle$ as a (finite) **presentation** of the group G.

Example 1. Consider the group G presented by $G = \langle r, s \mid \operatorname{ord}(r) = 3, \operatorname{ord}(s) = 2, \text{ and } srs = r^{-1}\rangle$. Considering that $\operatorname{ord}(r) = 3$ and $\operatorname{ord}(s) = 2$, the elements of G are given by e_G, r, r^2, s, rs, and $r^2 s$. Of course, one might naturally wonder why these are all of the elements of G. Let us prove this.

By definition, every element of G is of the form $r^i s^j$ for some integers i and j. By hypothesis that $\operatorname{ord}(r) = 3$, every element of G is of the form s^j, rs^j, and $r^2 s^j$ for some integer j. Likewise, by hypothesis that $\operatorname{ord}(s) = 2$, it follows that e_G, s, r, rs, r^2, and $r^2 s$ are all possible elements of G.

Example 2. Certainly, the number of relations can be zero, i.e., the set of relations is $\emptyset$. Consider the group presented by $G = \langle g \mid \emptyset\rangle$. One can easily verify that the map $\varphi : G \to \mathbb{Z}$ defined by $\varphi(g^k) = k$ is a group isomorphism, hence up to isomorphism, the unique group with this presentation is $\mathbb{Z}$.

Example 3. Construct a group presentation for the direct product $\mathbb{Z} \times \mathbb{Z}$.

The Commutator Subgroup

Until now, we have only studied abelian groups; however, non-abelian groups exist.

Proposition 3. $G = \langle r, s \mid \operatorname{ord}(r) = 3, \operatorname{ord}(s) = 2, \text{ and } srs = r^{-1}\rangle$ is a non-abelian group.

Proof. On the contrary, we will assume that $rs = sr$. We have therefore that $srs = s^2 r = r$. On the other hand, we have that $srs = r^{-1}$ so that $r = r^{-1}$ and $r^2 = e_G$, contradicting that $\operatorname{ord}(r) = 3$. □

Consequently, given a non-abelian group G, we might wish to quantify just "how far" G is from being abelian. Considering that G is non-abelian, we must have that $|G| \geq 6$, hence there exist elements g and h of G such that $gh \neq hg$. Consider the element $[g, h] = g^{-1}h^{-1}gh$ of G. We refer to $[g, h]$ as the **commutator** of g and h. Given nonempty subsets X and Y of G, we define the group

$$[X, Y] = \langle [x, y] \mid x \in X \text{ and } y \in Y\rangle$$

generated by all the commutators of an element in X and an element in Y. Ultimately, we may define the **commutator subgroup** $[G, G] = \langle [g, h] \mid g, h \in G\rangle$ of G.

Proposition 4. Consider a group G and a subgroup H of G.

(i.) We have that $gh = hg[g, h]$. Particularly, we have that $gh = hg$ if and only if $[g, h] = e_G$.

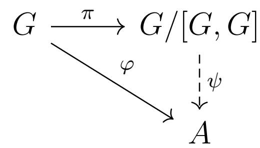
(ii.) We have that $H \trianglelefteq G$ if and only if $[H, G] \leq H$.

(iii.) $[G, G]$ is a normal subgroup of G.

(iv.) $G/[G, G]$ is abelian.

(v.) Given that $H \trianglelefteq G$ and G/H is abelian, we must have $[G, G] \leq H$. Conversely, if $[G, G] \leq H$, then $H \trianglelefteq G$ and G/H is abelian. Put another way, $G/[G, G]$ is the largest abelian quotient of G; thus, the larger $[G, G]$ is (with respect to inclusion), the "less abelian" G is.

(vi.) Every group homomorphism $\varphi : G \to A$ from G into an abelian group A "factors through" the commutator subgroup of G, i.e., $[G, G] \leq \ker \varphi$, and there exists a group homomorphism $\psi : G/[G, G] \to A$ such that $\varphi = \psi \circ \pi$, where $\pi : G \to G/[G, G]$ is the natural surjection. Put another way, the following diagram exists and is commutative (i.e., $\varphi = \psi \circ \pi$).



Proof. (i.) By definition, we have that $[g, h] = g^{-1}h^{-1}gh$, from which it follows that $g[g, h] = h^{-1}gh$ so that $hg[g, h] = gh$. Further, we have that $gh = hg$ if and only if $[g, h] = g^{-1}h^{-1}gh = e_G$.

(ii.) By definition, we have that $H \trianglelefteq G$ if and only if $g^{-1}Hg \subseteq H$ for all elements g in G. Consequently, if $H \trianglelefteq G$, then for any element $[h, g] = h^{-1}g^{-1}hg$ of $[H, G]$, we have that $g^{-1}hg$ is in H so that $[h, g] = h^{-1}g^{-1}hg$ is in H and $[H, G] \leq H$. Conversely, if $[H, G] \leq H$, then every element $[h, g]$ of $[H, G]$ can be written as $[h, g] = k$ for some element k of H. But this implies that $hk = h[h, g] = g^{-1}hg$ is in H for all h in H and g in G, i.e., $g^{-1}Hg \subseteq H$ for all elements g in G.

(iii.) We must establish that $g^{-1}[G, G]g \subseteq [G, G]$ for all elements g in G. Consider an element g of G and an element $[h, k]$ of $[G, G]$. Observe that $(g^{-1}hg)^{-1} = g^{-1}h^{-1}g$, hence we have that

$$g^{-1}[h, k]g = g^{-1}h^{-1}k^{-1}hkg = (g^{-1}h^{-1}g)(g^{-1}k^{-1}g)(g^{-1}hg)(g^{-1}kg) = [g^{-1}hg, g^{-1}kg]$$

is in $[G, G]$. We conclude therefore that $g^{-1}[G, G]g \subseteq [G, G]$ for all elements g in G.

(iv.) By part (iii.) above, we have that $G/[G, G]$ is a group with respect to the operation of G. Given any elements $g[G, G]$ and $h[G, G]$ of $G/[G, G]$, we have therefore that

$$(g[G, G])^{-1}(h[G, G])^{-1}(g[G, G])(h[G, G]) = g^{-1}h^{-1}gh[G, G] = e_G[G, G].$$

We conclude that $(g[G, G])(h[G, G]) = (h[G, G])(g[G, G])$ so that $G/[G, G]$ is abelian.

(v.) Given that G/H is abelian, we have that $(xH)(yH) = (yH)(xH)$ for all elements xH and yH in G/H, from which it follows that $x^{-1}y^{-1}xy$ is in H for all elements x and y of G. By definition of $[G, G]$, we conclude that $[G, G] \leq H$. Conversely, if $[G, G] \leq H$, then for any elements g in G and h in H, we have that $h^{-1}g^{-1}hg$ is in H, from which it follows that $g^{-1}hg$ is in H and $g^{-1}Hg \subseteq H$ for all elements g in G. For any elements x and y of G, we have that $x^{-1}y^{-1}xy$ is in H so that

$$e_G H = x^{-1}y^{-1}xyH = (xH)^{-1}(yH)^{-1}(xH)(yH),$$

and we conclude as desired that $(yH)(xH) = (xH)(yH)$ so that G/H is abelian.

(vi.) Given any element $[g, h] = g^{-1}h^{-1}gh$ of $[G, G]$, we have that

$$\varphi([g, h]) = \varphi(g^{-1}h^{-1}gh) = \varphi(g^{-1})\varphi(h^{-1})\varphi(g)\varphi(h) = \varphi(g)^{-1}\varphi(g)\varphi(h)^{-1}\varphi(h) = e_A$$

by hypothesis that φ is a group homomorphism and A is abelian. We conclude therefore that $[G, G] \leq \ker \varphi$. Consider the map $\psi : G/[G, G] \to A$ defined by $\psi(g[G, G]) = \varphi(g)$. Given that $g[G, G] = h[G, G]$, we have that $h^{-1}g[G, G] = e_G[G, G]$ so that $h^{-1}g$ is in $[G, G]$. Considering that $[G, G] \leq \ker \varphi$, it follows that $e_A = \varphi(h^{-1}g) = \varphi(h^{-1})\varphi(g) = \varphi(h)^{-1}\varphi(g)$ so that $\varphi(g) = \varphi(h)$, hence ψ is well-defined. By hypothesis that φ is a group homomorphism, it follows that ψ is a group homomorphism, and it is easy to verify that $\varphi = \psi \circ \pi$. Our proof is complete. □

Finitely Generated Abelian Groups

Consider the **free abelian group of rank** r given by the direct product $\mathbb{Z}^r = \prod_{i=1}^r \mathbb{Z}$ with $\mathbb{Z}^0 \overset{\text{def}}{=} \{0\}$. Using additive notation, it follows that $\mathbb{Z}$ is finitely generated by 1, hence $\mathbb{Z}^r$ is finitely generated by the vectors $\mathbf{e}_i$ whose jth entry is the Kronecker delta δ_{ij} for each integer $1 \leq j \leq r$.

Theorem 1. (The Fundamental Theorem of Finitely Generated Abelian Groups) Every finitely generated abelian group G can be written uniquely as $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_\ell}$ for some integer $r \geq 0$, where the integers $n_i \geq 2$ are the invariant factors of G that satisfy $n_1 \mid n_2 \mid \cdots \mid n_\ell$.

Ultimately, we will find that the Fundamental Theorem of Finitely Generated Abelian Groups is a consequence of the more general and powerful fact known as the Fundamental Theorem of Finitely Generated Modules over a Principal Ideal Domain, so for now, let us continue without proof.

Q2b, January 2018. Consider the abelian group $G = \mathbb{Z} \times \mathbb{Z}$. Given nonzero integers a and b, let $H_1 = \langle (a, 0) \rangle$ and $H_2 = \langle (0, b) \rangle$. Prove that we have $G/(H_1 \times H_2) \cong \mathbb{Z}/\langle \gcd(a, b) \rangle \times \mathbb{Z}/\langle \operatorname{lcm}(a, b) \rangle$. (**Hint:** use the fact that $ab = \gcd(a, b) \operatorname{lcm}(a, b)$ for any pair of integers a and b.)

One of the most fundamental properties of finitely generated abelian groups is the following.

Proposition 5. Every subgroup of a finitely generated abelian group is finitely generated.

Proof. Consider a finitely generated abelian group G with a subgroup H. We proceed by induction on the number n of generators of G. Given that $n = 1$, we have that $G = \langle g \rangle$ is cyclic. Considering that every subgroup of a cyclic group is cyclic (and therefore finitely generated), the claim holds for $n = 1$. We will assume inductively that the claim holds for some integer $n \geq 2$.

Given that $G = \langle g_1, \dots, g_{n+1} \rangle$, consider the canonical projection $\pi : G \to G/\langle g_{n+1} \rangle$ defined by $\pi(g) = g + \langle g_{n+1} \rangle$. By hypothesis that G is a finitely generated abelian group, every element of g is of the form $m_1 g_1 + \cdots + m_{n+1} g_{n+1}$ for some integers m_i, hence every element of $G/\langle g_{n+1} \rangle$ is of the form $m_1 g_1 + \cdots + m_n g_n + \langle g_{n+1} \rangle$ so that $G/\langle g_{n+1} \rangle = \langle g_1 + \langle g_{n+1} \rangle, \dots, g_n + \langle g_{n+1} \rangle \rangle$. By our induction hypothesis, every subgroup $H/\langle g_{n+1} \rangle$ of $G/\langle g_{n+1} \rangle$ is finitely generated. Explicitly, we may assume that the elements $h_1, \dots, h_k$ of H satisfy $H/\langle g_{n+1} \rangle = \langle h_1 + \langle g_{n+1} \rangle, \dots, h_k + \langle g_{n+1} \rangle \rangle$. Considering that every subgroup of a cyclic group is cyclic, it follows that $H \cap \langle g_{n+1} \rangle = \langle h_{k+1} \rangle$ for some element h_{k+1} of H. We claim that $H = \langle h_1, \dots, h_{k+1} \rangle$. Given any element h of H, we have that

$$\pi(h) = m_1 h_1 + \cdots + m_k h_k + \langle g_{n+1} \rangle = \pi(m_1 h_1 + \cdots + m_k h_k)$$

for some element $m_1 h_1 + \cdots + m_k h_k$ of $\langle h_1, \dots, h_k \rangle$. But this implies that

$$\pi(h - m_1 h_1 - \cdots - m_k h_k) = 0 + \langle g_{n+1} \rangle$$

so that $h - m_1 h_1 - \cdots - m_k h_k$ is in $\langle g_{n+1} \rangle$. Evidently, it is also in H (as it is a linear combination of elements of H), hence it is in $H \cap \langle g_{n+1} \rangle = \langle h_{n+1} \rangle$ so that $h - m_1 h_1 - \cdots m_k h_k = m_{k+1} h_{k+1}$ for some integer m_{k+1}. We conclude that $h = m_1 h_1 + \cdots + m_{k+1} h_{k+1}$ so that $H = \langle h_1, \dots, h_{k+1} \rangle$. $\square$

Smith Normal Form

Given positive integers $m, n \geq 1$, consider the set $\mathbb{Z}^{m \times n}$ of $m \times n$ matrices with integer entries.

Proposition 6. We have that $\mathbb{Z}^{m \times n}$ is an abelian group with respect to matrix addition. Further, there exists a map $\cdot : \mathbb{Z} \times \mathbb{Z}^{m \times n} \to \mathbb{Z}^{m \times n}$ that sends $(r, A) \mapsto r \cdot A$ with the properties that

(i.) $r \cdot (A + B) = r \cdot A + r \cdot B$,

(ii.) $(r + s) \cdot A = r \cdot A + s \cdot A$,

(iii.) $r \cdot (s \cdot A) = (rs) \cdot A$, and

(iv.) $1 \cdot A = A$

for all integers r and s and all matrices A and B in $\mathbb{Z}^{m \times n}$.

Proof. Observe that the multiplication map $\mathbb{Z} \times \mathbb{Z}^{m \times n} \to \mathbb{Z}^{m \times n}$ that sends $(r, A) \mapsto rA$ works. $\square$

Consequently, we refer to $\mathbb{Z}^{m \times n}$ as a $\mathbb{Z}$-**module**. We note that $\mathbb{Z}$-modules are quite common.

Proposition 7. Every abelian group G can be viewed as a $\mathbb{Z}$-module via the action $r \cdot g = g^r$.

Proof. Given any two elements g and h in G and any integers r and s, we have that

(i.) $r \cdot (gh) = (gh)^r = g^r h^r = (r \cdot g)(r \cdot h)$ by hypothesis that G is abelian;

(ii.) $(r + s) \cdot g = g^{r+s} = g^r g^s = (r \cdot g)(s \cdot g)$;

(iii.) $r \cdot (s \cdot g) = r \cdot (g^s) = (g^s)^r = g^{rs} = (rs) \cdot g$; and

(iv.) $1 \cdot g = g^1 = g$, as desired. $\square$

Later, we will define the notion of an R-module over any commutative ring R, and we will understand an R-module as a generalization of a vector space; for now, we are ready for the main theorem.

Theorem 2. (The Smith Normal Form) Given a nonzero matrix A in $\mathbb{Z}^{m \times n}$, there exists an invertible matrix P in $\mathbb{Z}^{m \times m}$ and an invertible matrix Q in $\mathbb{Z}^{n \times n}$ such that

$$PAQ = \begin{pmatrix} n_1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & n_2 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & n_3 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n_\ell & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

where the integers $n_i \geq 1$ are unique (up to sign) and satisfy $n_1 \mid n_2 \mid n_3 \mid \cdots \mid n_\ell$. Further, one can compute the integers n_i by the recursive formula $n_i = d_i / d_{i-1}$, where d_i is the greatest common divisor of all $i \times i$-minors of the matrix A and d_0 is defined to be 1.

Generally, the Smith Normal Form holds for any matrix with entries in a principal ideal domain, e.g., the integers $\mathbb{Z}$ and any polynomial ring $k[x]$, where k is a field (such as $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$). We shall soon see that the Smith Normal Form functions as an incredibly powerful tool in linear algebra to compute the Rational Canonical Form of a matrix over a field k or the Jordan Canonical Form of a matrix over an algebraically closed field (often $\mathbb{C}$). Let us investigate how this works.

Example 4. Compute the Smith Normal Form of the matrix $xI - A$ given that

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

to find the invariant factors, elementary divisors, and minimal and characteristic polynomials of A.

Quite generally, the minimal polynomial of a matrix A (or linear operator represented by A) is the largest invariant factor of the matrix $xI - A$, and the characteristic polynomial of A is the product of all of the invariant factors of A. Later, we will see that the invariant factors of A give rise to the Rational Canonical Form of A, and the elementary divisors lead us to the Jordan Canonical Form.

Q3, January 2017. Consider the free abelian group $\mathbb{Z}^n$ of rank n whose elements are row vectors. Given a matrix A in $\mathbb{Z}^{r \times n}$, let K_A denote the subgroup of $\mathbb{Z}^n$ generated by the rows of A.

(a.) Given a matrix $B = PAQ$, where P is an invertible $r \times r$ matrix over $\mathbb{Z}$ and Q is an invertible $n \times n$ matrix over $\mathbb{Z}$, prove that $\mathbb{Z}^n / K_A$ and $\mathbb{Z}^n / K_B$ are isomorphic as abelian groups.

(b.) Given that $A = \begin{pmatrix} 4 & -2 & 4 \\ 2 & 4 & 4 \end{pmatrix}$, express $\mathbb{Z}^3 / K_A$ as a direct sum of cyclic groups.

Before we prove part (a.) (as it is rather nontrivial at first glance), we need a technical lemma.

Lemma 1. Given a group G with a normal subgroup K and a group H, if there exists a group isomorphism $\varphi : G \to H$, then $\varphi(K)$ is a normal subgroup of H and $G/K \cong H/\varphi(K)$.

Proof. Given any element h of H, we have that $h = \varphi(g)$ for some element g in G. Consequently, it follows that $h\varphi(K)h^{-1} = \varphi(g)\varphi(K)\varphi(g)^{-1} = \varphi(gKg^{-1}) = \varphi(K)$ so that $\varphi(K)$ is normal in H.

Consider the group homomorphism $\psi : G \to H/\varphi(K)$ defined by $\psi(g) = \varphi(g)\varphi(K)$. By hypothesis that φ is surjective, for every element g of G, there exists a unique element g' of G such that $g = \varphi(g')$. Consequently, we have that $g\varphi(K) = \varphi(g')\varphi(K) = \psi(g')$ so that ψ is surjective. Further, we have that g is in $\ker \psi$ if and only if $\varphi(g)\varphi(K) = \psi(g) = e_G\varphi(K)$ if and only if $\varphi(g)$ is in $\varphi(K)$ if and only if $\varphi(g) = \varphi(k)$ for some k in K if and only if $g = k$ by assumption that φ is injective. We conclude that $\ker \psi = K$, hence $G/K \cong H/\varphi(K)$ by the First Isomorphism Theorem. □

Corollary 1. Given a group G with a normal subgroup K, if there exists a group isomorphism $\varphi : G \to G$, then $G/K \cong G/\varphi(K)$.

Proof. (a.) Consider the ith row $\mathbf{v}_i = \langle a_{i1}, \dots, a_{in} \rangle$ of the matrix A. By definition, we have that

$$K_A = \{m_1\mathbf{v}_1 + \cdots m_r\mathbf{v}_r \mid m_i \in \mathbb{Z}\}.$$

Crucially, we make the following observation: for any vector $\langle m_1, \dots, m_r \rangle$ in $\mathbb{Z}^r$, we have that

$$\langle m_1, \dots, m_r \rangle A = m_1 \mathbf{v}_1 + \cdots + m_r \mathbf{v}_r.$$

Consequently, every element of K_A is of the form $\langle m_1, \dots, m_r \rangle A$ for some vector $\mathbf{m} = \langle m_1, \dots, m_r \rangle$ of $\mathbb{Z}^r$. Put another way, we have that $K_A = \mathbb{Z}^r A$. By the same argument applied to $B = PAQ$, we have that $K_B = \mathbb{Z}^r B = \mathbb{Z}^r PAQ$. By hypothesis that P is invertible, it follows that the abelian group homomorphism $\rho : \mathbb{Z}^r \to \mathbb{Z}^r$ defined by $\rho(\mathbf{v}) = \mathbf{v}P$ is an isomorphism with inverse $\rho^{-1}(\mathbf{v}P) = \mathbf{v}$. Likewise, the abelian group homomorphism $\sigma : \mathbb{Z}^n \to \mathbb{Z}^n$ defined by $\sigma(\mathbf{v}) = \mathbf{v}Q$ is an isomorphism with inverse $\sigma^{-1}(\mathbf{v}Q) = \mathbf{v}$. We have therefore that $\sigma : \mathbb{Z}^n \to \mathbb{Z}^n Q$ is a group isomorphism with $\mathbb{Z}^n = \sigma(\mathbb{Z}^n) = \mathbb{Z}^n Q$ and $\sigma(\mathbb{Z}^r PA) = \mathbb{Z}^r PAQ$, from which it follows by Lemma 1 that $\mathbb{Z}^n / \mathbb{Z}^r PA \cong \mathbb{Z}^n Q / (\mathbb{Z}^r PAQ)$. We have also that $\rho : \mathbb{Z}^r \to \mathbb{Z}^r$ is a group isomorphism such that $\mathbb{Z}^r = \rho(\mathbb{Z}^r) = \mathbb{Z}^r P$, from which it follows that $\mathbb{Z}^r PA = \mathbb{Z}^r A = K_A$. Ultimately, we conclude as desired that

$$\frac{\mathbb{Z}^n}{K_B} = \frac{\mathbb{Z}^n}{\mathbb{Z}^r B} = \frac{\mathbb{Z}^n}{\mathbb{Z}^r PAQ} = \frac{\mathbb{Z}^n Q}{\mathbb{Z}^r PAQ} \cong \frac{\mathbb{Z}^n}{\mathbb{Z}^r PA} = \frac{\mathbb{Z}^n}{\mathbb{Z}^r A} = \frac{\mathbb{Z}^n}{K_A}. \qquad \square$$

Proof. (Theorem 1) Given an abelian group G with generators $g_1, \dots, g_n$, every element of G can be written as $m_1 g_1 + \cdots + m_n g_n$ for some integers m_i. Consider the map $\varphi : \mathbb{Z}^n \to G$ defined by $\varphi(\langle m_1, \dots, m_n \rangle) = m_1 g_1 + \cdots + m_n g_n$. One can easily verify that φ is a surjective group homomorphism, hence by the First Isomorphism Theorem, we have that $G \cong \mathbb{Z}^n / \ker \varphi$. By Proposition 5, it follows that $\ker \varphi$ is finitely generated, i.e., $\ker \varphi = \langle \langle a_{11}, \dots, a_{1n} \rangle, \dots, \langle a_{r1}, \dots, a_{rn} \rangle \rangle$ for some integers a_{ij} with $r \leq n$. Consequently, the elements of $\ker \varphi$ are $k_1 \langle a_{11}, \dots, a_{1n} \rangle + \cdots + k_r \langle a_{r1}, \dots, a_{rn} \rangle$ for some integers k_i. Put another way, we have that $\ker \varphi = \mathbb{Z}^r A = \psi(\mathbb{Z}^r)$, where A is the matrix whose ith row is $\langle a_{i1}, \dots, a_{in} \rangle$ and $\psi : \mathbb{Z}^r \to \mathbb{Z}^n$ is the map defined by $\psi(\mathbf{v}) = \mathbf{v}A$ (cf. the proof of part (a.) of Q3, January 2017). Given that φ is injective, we have that $G \cong \mathbb{Z}^n$. Otherwise, A is a nonzero matrix in $\mathbb{Z}^{r \times n}$, and by Theorem 2, there exists an invertible matrix P in $\mathbb{Z}^{r \times r}$ and an invertible matrix Q in $\mathbb{Z}^{n \times n}$ such that PAQ is diagonal with ℓ nonzero entries $n_1 \mid n_2 \mid n_3 \mid \cdots \mid n_\ell$ followed by $n - \ell$ zeros along the diagonal. By part (a.) of Q3, January 2017, we conclude that

$$\begin{aligned} G \cong \frac{\mathbb{Z}^n}{\ker \varphi} = \frac{\mathbb{Z}^n}{\mathbb{Z}^r A} \cong \frac{\mathbb{Z}^n}{\mathbb{Z}^r PAQ} \\ &= \frac{\mathbb{Z}^n}{\langle n_1 \rangle \times \langle n_2 \rangle \times \langle n_3 \rangle \times \cdots \times \langle n_\ell \rangle \times \underbrace{\langle 0 \rangle \times \cdots \times \langle 0 \rangle}_{n-\ell \text{ factors}}} \\ &\cong \frac{\mathbb{Z}}{n_1 \mathbb{Z}} \times \frac{\mathbb{Z}}{n_2 \mathbb{Z}} \times \frac{\mathbb{Z}}{n_3 \mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_\ell \mathbb{Z}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n-\ell \text{ factors}} \\ &\cong \mathbb{Z}^{n-\ell} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \mathbb{Z}_{n_3} \times \cdots \times \mathbb{Z}_{n_\ell}. \qquad \square \end{aligned}$$

By the remark immediately following the statement of Theorem 2, the Fundamental Theorem of Finitely Generated Modules over a Principal Ideal Domain (PID) follows by a similar argument applied to a PID R. Consequently, Theorem 1 follows from Theorem 2 by setting $R = \mathbb{Z}$.

Before we conclude this note, let us discuss the algorithm for computing the invertible matrices P and Q such that PAQ is in Smith Normal Form, as guaranteed by Theorem 2. Observe that any matrix A in $\mathbb{Z}^{m \times n}$ determines a $\mathbb{Z}$-linear transformation $\mathbb{Z}^n \to \mathbb{Z}^m$ whose image is generated by the columns of A. Particularly, we have that $A\mathbb{Z}^n = \langle v_1, v_2, \dots, v_n \rangle$, where v_i is the ith column vector of A and the action of A is left-multiplication on an $n \times 1$ column vector. Put another way, $\mathbb{Z}^m / A\mathbb{Z}^n$ is the cokernel of the map $\mathbb{Z}^n \to \mathbb{Z}^m$ that is left-multiplication by A. Consequently, the Smith Normal Form of A induces an isomorphism between $\mathbb{Z}^m / A\mathbb{Z}^n$ and $\mathbb{Z}^m / PAQ\mathbb{Z}^n$. Because PAQ is a diagonal matrix by construction, the latter group is a direct product of cyclic groups.

We obtain the invertible matrices P and Q guaranteed by Theorem 2 as follows.

Proposition 8. (Finding the Change-of-Basis Matrices for the Smith Normal Form) Let A be a nonzero $m \times n$ matrix over $\mathbb{Z}$ (or any other principal ideal domain). The invertible $m \times m$ matrix P and invertible $n \times n$ matrix Q such that PAQ is in Smith Normal Form can be found as follows.

(i.) Compute the Smith Normal Form of A by using elementary row and column operations to obtain a diagonal matrix with positive integers $n_1 \mid n_2 \mid \cdots \mid n_\ell$ along the diagonal. **Be sure to keep track of all row and column operations $R_i \leftrightarrow R_j$ and $\alpha R_i + R_j \mapsto R_j$.**

(ii.) Use the elementary row operations from the previous step on the $m \times m$ identity matrix. If performed correctly, the resulting matrix is the invertible $m \times m$ matrix P.

(iii.) Use the elementary column operations from the first step on the $n \times n$ identity matrix. If performed correctly, the resulting matrix is the invertible $n \times n$ matrix Q.

Considering that Q is an invertible $n \times n$ matrix, it follows that the columns of Q form a basis for $\mathbb{Z}^n$. Likewise, the columns of P^{-1} form a basis for $\mathbb{Z}^m$. Consequently, the map that sends the ith column of P^{-1} to the generator of the ith cyclic group $\mathbb{Z}/n_i\mathbb{Z}$ of $\mathbb{Z}^m / PAQ\mathbb{Z}^n$ is surjective. Even more, we have that $PAQ\mathbb{Z}^n = PA\mathbb{Z}^n$ so that $P^{-1}(PAQ)\mathbb{Z}^n = A\mathbb{Z}^n$, hence the kernel of this map is $A\mathbb{Z}^n$. By the First Isomorphism Theorem, we conclude that P^{-1} induces an isomorphism $\mathbb{Z}^m / A\mathbb{Z}^n \cong \mathbb{Z}^m / PAQ\mathbb{Z}^n$, the latter of which is a direct product of cyclic groups by construction.

Using Gaussian elimination on P, one can obtain the matrix P^{-1}. One can alternatively begin with the standard basis $\mathbf{e}_1, \dots, \mathbf{e}_m$ of $\mathbb{Z}^m$. Using the same order as the elementary row operations were performed, employ the inverse operation to the columns of the $m \times m$ matrix $\begin{pmatrix} \mathbf{e}_1 & \cdots & \mathbf{e}_m \end{pmatrix}$. Explicitly, if the row operation $R_i \leftrightarrow R_j$ was performed, then perform the column operation $C_i \leftrightarrow C_j$; if the row operation $R_i + \alpha R_j \mapsto R_i$ was performed, then perform the column operations $C_j - \alpha C_i \mapsto C_j$. If performed correctly, the resulting matrix is the invertible $m \times m$ matrix P^{-1}.

We conclude with the following example to illustrate the above procedure.

Example 5. Find an explicit isomorphism between a direct product of cyclic groups and

$$G = \frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{\langle (0,0,3,1), (0,6,0,0), (0,1,0,1) \rangle}.$$

Solution. By the preceding discussion, it suffices to find the Smith Normal Form of some $4 \times n$ matrix A such that G is the cokernel of the map that is left-multiplication $A\mathbb{Z}^n$. For instance, one can easily verify that G is the cokernel of the map $\mathbb{Z}^3 \to \mathbb{Z}^4$ that is left-multiplication by

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 6 & 1 \\ 3 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Using elementary row and column operations, we convert A into a diagonal matrix whose positive entries are $n_1 \mid n_2 \mid \cdots \mid n_\ell$. One way to accomplish this is to use (1.) $R_1 \leftrightarrow R_4$, (2.) $R_3 - 3R_1 \mapsto R_3$, (3.) $C_3 - C_1 \mapsto C_3$, (4.) $R_3 + 3R_2 \mapsto R_3$, (5.) $C_2 - 6C_3 \mapsto C_2$, and (6.) $C_2 \leftrightarrow C_3$ to obtain

$$A \overset{(1.)}{\sim} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 6 & 1 \\ 3 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \overset{(2.)}{\sim} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 6 & 1 \\ 0 & 0 & -3 \\ 0 & 0 & 0 \end{pmatrix} \overset{(3.)}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 1 \\ 0 & 0 & -3 \\ 0 & 0 & 0 \end{pmatrix} \overset{(4.)}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 1 \\ 0 & 18 & 0 \\ 0 & 0 & 0 \end{pmatrix} \overset{(5.)}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 18 & 0 \\ 0 & 0 & 0 \end{pmatrix} \overset{(6.)}{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 18 \\ 0 & 0 & 0 \end{pmatrix}.$$

By performing these elementary row operations on the 4×4 identity matrix, we find that

$$P = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 3 & 1 & -3 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

By performing these elementary column operations on the 3×3 identity matrix, we find that

$$Q = \begin{pmatrix} 1 & -1 & 6 \\ 0 & 0 & 1 \\ 0 & 1 & -6 \end{pmatrix}.$$

We find P^{-1} by employing the inverse of the row operations on the columns of the 4×4 identity matrix. Explicitly, if we used $R_i + \alpha R_j \mapsto R_i$, then use $C_j - \alpha C_i \mapsto C_j$; swapping is its own inverse. Using the notation $\overline{(i.)}$ to indicate the inverse operation of the ith step above, we find that

$$\begin{bmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 \end{bmatrix} \xrightarrow{\overline{(1.)}} \begin{bmatrix} \mathbf{e}_4 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_1 \end{bmatrix} \xrightarrow{\overline{(2.)}} \begin{bmatrix} 3\mathbf{e}_3 + \mathbf{e}_4 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_1 \end{bmatrix} \xrightarrow{\overline{(4.)}} \begin{bmatrix} 3\mathbf{e}_3 + \mathbf{e}_4 & \mathbf{e}_2 - 3\mathbf{e}_3 & \mathbf{e}_3 & \mathbf{e}_1 \end{bmatrix},$$

where $\mathbf{e}_i$ is the usual standard basis column vector. Put another way, we have that

$$P^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 3 & -3 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Ultimately, the map $\mathbb{Z}^4 \to G$ defined by $(0,0,3,1)^t \mapsto \overline{0}$, $(0,1,-3,0)^t \mapsto \overline{0}$, $(0,0,1,0)^t \mapsto \overline{1}$, and $(1,0,0,0)^t \mapsto 1$ induces a surjection $\mathbb{Z}^4 \to \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}$ with kernel $\langle (0,0,3,1), (0,6,0,0), (0,1,0,1) \rangle$. By the First Isomorphism Theorem, we conclude that $G \cong \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}$. ◇

Q1, August 2012. Consider the (finitely generated) abelian group $G = \mathbb{Z} \times \mathbb{Z}_{30}$ under addition with subgroup $H = \langle (5,3) \rangle$. Describe with proof the factor group G/H.

Q2b, January 2018 (Revisited). Use the Smith Normal Form to prove that

$$\frac{\mathbb{Z}\times\mathbb{Z}}{\langle (a,0),(0,b)\rangle} \cong \frac{\mathbb{Z}}{\langle \gcd(a,b)\rangle} \times \frac{\mathbb{Z}}{\langle \operatorname{lcm}(a,b)\rangle}.$$

Q1, August 2021. Find an explicit isomorphism between the quotient group $(\mathbb{Z}\times\mathbb{Z})/\langle (4,1),(6,3)\rangle$ and a direct product of cyclic groups.