A Crash "Course" In Finitely Generated Abelian Groups

An abelian group is **finitely generated** if every member is formed by taking sums from a finite subset called a **generating set**. A finitely generated abelian group G is **free** if for some generating set, $\{g_1, \ldots, g_n\}$, $\Sigma_{i=1}^{n} k_i g_i = 0$ iff all $k_i = 0$. In this case the generating set is called a **basis** and n is called the **rank** of G. Any subgroup of a finitely generated free abelian group is also a finitely generated free abelian group with rank less than or equal to the original group. Every nontrivial finitely generated free abelian group is isomorphic to $\mathbb{Z}^n$ for some integer $n \geq 1$ and these are all distinct.

Note that $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$ is not free. (The brackets denote equivalence classes.) The set $\{[1]\}$ generates it, but is not a basis. For example, $[2] = 2\cdot[1] = 4\cdot[1]$, so we do not have uniqueness. You can show this happens for any generating subset.

Let A be an $m \times n$ integer matrix. Then $A : \mathbb{Z}^n \to \mathbb{Z}^m$ is a homomorphism. The image, denoted $A\mathbb{Z}^n$, is a subgroup of $\mathbb{Z}^m$. Thus the quotient group $\mathbb{Z}^m/A\mathbb{Z}^n$ is well defined. It can be shown that every finitely generated abelian group is isomorphic to $\mathbb{Z}^m/A\mathbb{Z}^n$ for some (non-unique) integer matrix A.

There is a well known algorithm for deciding whether $\mathbb{Z}^m/A\mathbb{Z}^n$ and $\mathbb{Z}^k/B\mathbb{Z}^p$ are isomorphic. It involves applying row and column operations to place each matrix into a canonical form. The allowed operations are as follows.

(1) Switch two rows (or two columns).
(2) Multiply a row (or a column) by -1.
(3) Add a multiple of one row (or column) to another row (or column).

These are sufficient if A and B are square matrices of the same size. Assume this for now.

The motivation for allowing the row operations should be clear. They are the exact analog of the row operations that are allowed when solving systems of equations over a field like $\mathbb{R}$. However, we cannot multiple through by integers other than ± 1 since this could effect the outcome. For example, $\mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/3\mathbb{Z}$, but is equal to $\mathbb{Z}/(-2)\mathbb{Z}$. (Notice that the units of the ring $\mathbb{Z}$ are just ± 1, while the units of $\mathbb{R}$ are all nonzero real numbers.) Each column operation corresponds to a change of generators. When you were solving systems of equations over $\mathbb{R}$ the variable names might have had physical significance like time or pressure. Thus, switching them would change the solution space. But our generating elements have no special significance, thus the three column operations are allowed.

It can be shown that, using (1), (2) & (3), any square integer matrix can be placed into a diagonal form

$$\begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix}$$

such that $d_1|d_2$, $d_2|d_3$ and so on. This is called the **Smith normal form**. Your book gives a standard algorithm for doing this. I'll use $A \rightsquigarrow B$ to indicate that B can be derived from A by the allowed moves. Once we have a matrix in Smith normal form, it is easy to understand the structure of the corresponding group.

Examples.

1. Let $A = \begin{bmatrix} 2 & -2 & -4 \\ 4 & 0 & -8 \\ 4 & 20 & 12 \end{bmatrix}$. Then, $A \rightsquigarrow \begin{bmatrix} 2 & -2 & -4 \\ 0 & 4 & 0 \\ 0 & 24 & 20 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 20 \end{bmatrix}$.

Therefore, $\dfrac{\mathbb{Z}^3}{A\mathbb{Z}^3} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$.

2. Let $B = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 0 & -1 \\ 0 & 0 & 0 \end{bmatrix}$. Then, as you can check, $B \rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Therefore, $\dfrac{\mathbb{Z}^3}{B\mathbb{Z}^3} \cong \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.

3. Let $C = \begin{bmatrix} 1 & -6 & 8 & 6 & 2 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 3 & 1 \\ 0 & 0 & 2 & 3 & 1 \\ 1 & 3 & 4 & 6 & 2 \end{bmatrix}$. A bit of work shows that the Smith normal form is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Therefore, $\dfrac{\mathbb{Z}^5}{C\mathbb{Z}^5} \cong \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}$.

You should be able to see that a 1 in the Smith normal form yields a trivial factor, a 0 yields a $\mathbb{Z}$ factor, and an integer $d > 1$ yields a $\mathbb{Z}/d\mathbb{Z}$ factor.

Using the Smith normal form it can be shown that any finitely generated abelian group can be written in the form

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z} \cong \mathbb{Z}^b \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z},$$

with $d_i|d_{i+1}$, and all $d_i \neq 1$. The integer $b = n - k$ is number of d_i's equal to zero and is called the **Betti number**, $T = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}$ is called the **torsion**

subgroup and the nonzero d_i's are called the **torsion coefficients**. These numbers, $b, d_1, \ldots, d_k$, completely determine the isomorphism class of G.

The following matrix operation is also useful. If row i and column i are all zeros except for a 1 on the diagonal then they can be deleted without changing the group. That is suppose B is obtained from A in this way and A is $n \times n$. Then

$$\frac{\mathbb{Z}^n}{A\mathbb{Z}^n} \cong \frac{\mathbb{Z}^{n-1}}{B\mathbb{Z}^{n-1}}.$$

Thus, square integer matrices A and B can give isomorphic groups even if they they are of different sizes.

For non-square matrices it is easy to convert to an equivalent square matrix. We give two examples of this.

Examples.

4. Notice that

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \end{bmatrix} : \mathbb{Z}^3 \to \mathbb{Z}^2 \qquad \text{and} \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \mathbb{Z}^2 \to \mathbb{Z}^2$$

have the same image in $\mathbb{Z}^2$.

5. Also,

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} : \mathbb{Z} \to \mathbb{Z}^3 \qquad \text{and} \qquad \begin{bmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{bmatrix} : \mathbb{Z}^3 \to \mathbb{Z}^3$$

have the same image in $\mathbb{Z}^3$.

If there are more columns than rows, use column operations to clear the extra columns and then delete them. If there are more rows than columns, add columns of zeros to make the matrix square.

Exercises.

1. Show that $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$ has Smith normal form $\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$. This proves that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. Check this directly.

2. Try to show that $\begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$ is equivalent to $\begin{bmatrix} 1 & 0 \\ 0 & 8 \end{bmatrix}$. You cannot! Show directly that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/8\mathbb{Z}$.

In computing homology groups we will often need to find G/H where G is a free abelian group and H is a subgroup specified by a basis or generating set. For example if $G = \mathbb{Z}^3$ and H has basis $\{(1,0,0)\}$, then modding out by H will produce a group isomorphic to $\mathbb{Z}^2$. But it may not be obvious how H fits into G. The next theorem takes care of this.

Theorem. Let G be a free abelian group with basis $\{g_1, \ldots, g_k\}$. Let H be a subgroup with generating set $\{h_1, \ldots, h_p\}$. Let

$$h_j = \Sigma_{i=1}^{k} n_{ij} g_i \quad \text{for } j = 1, \ldots, p.$$

Let N be the $k \times p$ matrix $[n_{ij}]$; if $p < k$ one can augment N by adding $k - p$ columns of zeros so that N is now a square matrix. Then

$$G/H \cong \frac{\mathbb{Z}^k}{N\mathbb{Z}^k}.$$

Examples.

5. Let $G = \langle g_1, g_2, g_3 \rangle$ and $H = \langle h_1, h_2 \rangle$ where $h_1 = 2g_1 + g_2 - g_3$ and $h_2 = g_1 + 5g_2 + g_3$. Find the isomorphism class of G/H.

We let $N = \begin{bmatrix} 2 & 1 & -1 \\ 1 & 5 & 1 \\ 0 & 0 & 0 \end{bmatrix}$. The Smith normal form is $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Thus $G/H \cong \mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

6. Let $G = \langle a, b, c, d \rangle$ and $H = \langle a + b, 2b + c, a + 3b + c, a - d, b + d \rangle$. Notice that we have specified too many generators for H so we do not have a basis. We could preform column operations and derive a basis by eliminating redundant generators and then find Smith normal form. But, since the column operations needed to get a basis are allowed moves in finding the Smith normal form, we might as well skip the first step as just compute the Smith normal form.

Let $N = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 \end{bmatrix}$. The Smith normal form is $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. Thus $G/H \cong \mathbb{Z}^2$.

The following theorem is also useful to know.

Theorem. Let A be a square integer matrix and $G = \mathbb{Z}^n / A\mathbb{Z}^n$. Let $|G|$ denote the order of G. Then we have

$$|G| = \begin{cases} |\det(A)| & \text{if} \quad \det(A) \neq 0, \\ \infty & \text{if} \quad \det(A) = 0. \end{cases}$$

References.

- *Elements of Algebraic Topology*, Munkres, §§4 & 11.
- *Rings, Modules and Linear Algebra*, Hartley & Hawkes, Chapter 10.
- *Computational Homology*, Kaczynski *et al.*