18. Finitely generated abelian groups (Chapter 21.3)

Aim: apply the structure theorem for finitely generated modules over a PID to $\mathbb{Z}$.

Theorem 18.1 (Structure theorem for finitely generated abelian groups). Let G be a finitely generated abelian group. Then there exist integers $s \geq 0$ and $a_1, \ldots, a_u > 1$ with $a_1 | a_2 | \cdots | a_u$ such that

$$G \cong \mathbb{Z}^s \oplus \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_u}.$$

Moreover, such a decomposition is unique.

Proof. G is a finitely generated $\mathbb{Z}$-module and $\mathbb{Z}$ is a PID. Hence Theorem 17.6 gives the existence of an integer $s \geq 0$ and nonzero nonunits $a_1, \ldots, a_u \in \mathbb{Z}$ with $a_1 | a_2 | \cdots | a_u$ such that

$$G \cong \mathbb{Z}^s \oplus \mathbb{Z}/\mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}a_u. \qquad (*)$$

Since the only units of $\mathbb{Z}$ are ± 1, we have that $a_i \neq \pm 1$. Since

$$\mathbb{Z}/\mathbb{Z}a_i = \mathbb{Z}/\mathbb{Z}(-a_i) = \mathbb{Z}_{a_i},$$

we may replace any negative a_i in $(*)$ by $-a_i$ to obtain the claim. □

To find the integers s and a_i in Theorem 18.1, we proceed as follows. Let G be a finitely generated abelian group with generators $\{g_1, \ldots, g_n\}$. We find the kernel of the $\mathbb{Z}$-module homomorphism

$$\varphi: \mathbb{Z}^n \longrightarrow G$$
$$e_i \longmapsto g_i.$$

If $(x_1, \ldots, x_n) \in \ker\varphi$, then

$$0 = \varphi(x_1, \dots, x_n) = x_1 g_1 + \dots + x_n g_n.$$

Hence if $\operatorname{Ker}\varphi$ is generated by $\{(x_{11}, \dots, x_{1n}), \dots, (x_{m1}, \dots, x_{mn})\}$, we obtain a system of equations

$$\begin{matrix} x_{11} g_1 + \dots + x_{1n} g_n = 0 \\ \vdots \\ x_{m1} g_1 + \dots + x_{mn} g_n = 0. \end{matrix}$$

Let

$$A = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \text{ and let } \begin{pmatrix} a_1 & & & & \\ & \ddots & & 0 & \\ & & a_r & & \\ & 0 & & 0 & \\ & & & & \ddots \, 0 \end{pmatrix}$$ be the Smith normal form of A. Then

$$G \cong \mathbb{Z}^{m-n} \oplus \mathbb{Z}_{a_1} \oplus \dots \oplus \mathbb{Z}_{a_r}.$$

Some of the first a_i's may be -1 or 1, in which case $\mathbb{Z}_{a_i} = 0$. After removing these, we get the required form.

Example 18.2 Let

$$G = \left\langle g_1, g_2, g_3 \;\middle|\; \begin{matrix} 5g_1 + 9g_2 + 5g_3 = 0 \\ 2g_1 + 4g_2 + 2g_3 = 0 \\ g_1 + g_2 - 3g_3 = 0 \end{matrix} \right\rangle.$$

Let

$$A = \begin{pmatrix} 5 & 9 & 5 \\ 2 & 4 & 2 \\ 1 & 1 & -3 \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_3} \begin{pmatrix} 1 & 1 & -3 \\ 2 & 4 & 2 \\ 5 & 9 & 5 \end{pmatrix} \xrightarrow[R_3 - 5R_1]{R_2 - 2R_1}$$

$$\begin{pmatrix} 1 & 1 & -3 \\ 0 & 2 & 8 \\ 0 & 4 & 20 \end{pmatrix} \xrightarrow[C_3 \to C_3 + 3C_1]{C_2 \to C_2 - C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & 4 & 20 \end{pmatrix} \xrightarrow{R_3 \to R_3 - 2R_2}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 8 \\ 0 & 0 & 4 \end{pmatrix} \xrightarrow{C_3 \to C_3 - 4C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Then

$$\begin{aligned} G &\cong \mathbb{Z}_1 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \\ &= 0 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \\ &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4. \end{aligned}$$