3.10 Finitely Generated Abelian Groups

Last updated: 2020–11–22

Specializing the structure theorem for finitely generated modules over a principal ideal domain, we obtain a structure theorem for finitely generated abelian groups.

3.10.1 Theorem (Structure). *For any finitely generated abelian group G, there exists unique nonnegative integers r, ℓ and unique positive integers $q_1, q_2, \dots, q_\ell$ such that $q_1 > 1$, q_j divides q_{j+1} for all $1 \leqslant j < \ell$, and*

$$G \cong \frac{\mathbb{Z}}{\langle q_1 \rangle} \oplus \frac{\mathbb{Z}}{\langle q_2 \rangle} \oplus \cdots \oplus \frac{\mathbb{Z}}{\langle q_\ell \rangle} \oplus \mathbb{Z}^r .$$

The history of Theorem 3.10.1 is complicated because it was first proven when group theory was not well-established. Carl Friedrick Gauss (1801) proves an early form for finite groups and Leopold Kronecker (1870) provides a complete proof. The finitely presented case is solved by Henry Smith (1861), however the finitely generated case is sometimes credited to Henri Poincaré (1900). Emmy Noether (1926) generalizes the Kronecker argument to finitely generated abelian groups.

Proof. Since the ring $\mathbb{Z}$ of integers is a principal ideal domain, this theorem follows immediately from Theorem 3.9.1. □

3.10.2 Corollary. *Let G be a finite abelian group. Assuming that, for any positive integer n, the number of elements $g \in G$ such that $n\,g = 0$ is at most n, the groups G is cyclic.*

Proof. By Theorem 3.10.1, there exists a nonnegative integers ℓ and positive integers $q_1, q_2, \dots, q_\ell$ such that $q_1 > 1$, q_j divides q_{j+1} for all $1 \leqslant j < \ell$, and

$$G \cong \frac{\mathbb{Z}}{\langle q_1 \rangle} \oplus \frac{\mathbb{Z}}{\langle q_2 \rangle} \oplus \cdots \oplus \frac{\mathbb{Z}}{\langle q_\ell \rangle} .$$

However, if $\ell > 1$, then $|G| > q_\ell$ and $q_\ell\, g = 0$ for all $g \in G$ contradicting the hypothesis. Therefore, we conclude that $\ell = 1$ and G is cyclic. □

3.10.3 Corollary. *Let K be a field. Any finite subgroup the multiplicative group $K^\times$ is cyclic.*

Proof. Let n be a positive integer. A polynomial $K[x]$ of degree n has at most n linear factors. Since the polynomial ring $K[x]$ is a unique factorization domain, it follows any polynomial of degree n has at most n roots. In particular, there are at most n elements $a \in K$ such that $a^n - 1 = 0$. Applying Corollary 3.10.2, we deduce that any finite subgroup the multiplicative group $K^\times$ is cyclic. □

There is a second form of Theorem 3.10.1 involving prime powers which is often more convenient to use in applications.

3.10.4 Corollary. *For any finitely generated abelian group G, there exists unique nonnegative integers r, k, prime integers $p_1, p_2, \dots, p_k$ and positive integers $e_1, e_2, \dots, e_k$ such that*

$$G \cong \frac{\mathbb{Z}}{\langle p_1^{e_1} \rangle} \oplus \frac{\mathbb{Z}}{\langle p_2^{e_2} \rangle} \oplus \cdots \oplus \frac{\mathbb{Z}}{\langle p_k^{e_k} \rangle} \oplus \mathbb{Z}^r .$$

Sketch of Proof. The prime factorization $q = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ combined with Theorem 2.3.11 imply that

$$\frac{\mathbb{Z}}{\langle q \rangle} \cong \frac{\mathbb{Z}}{\langle p_1^{e_1} \rangle} \oplus \frac{\mathbb{Z}}{\langle p_2^{e_2} \rangle} \oplus \cdots \oplus \frac{\mathbb{Z}}{\langle p_k^{e_k} \rangle}. \qquad \square$$

3.10.5 Problem. Find, up to isomorphism, all of the abelian groups of order 8. Identify the isomorphism class of each of the following

$$(\mathbb{Z}/\langle 15 \rangle)^\times, \qquad (\mathbb{F}_{17})^\times/\langle -1 \rangle, \qquad \mathbb{F}_8^+, \qquad (\mathbb{Z}/\langle 16 \rangle)^\times, \qquad \mu_8.$$

Solution. Corollary 3.10.4 implies that the abelian groups of order $8 = 2^3$ are isomorphic to

$$\frac{\mathbb{Z}}{\langle 2^3 \rangle}, \qquad \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle}, \qquad \text{or} \qquad \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle}.$$

Since $\big(\mathbb{Z}/\langle 15 \rangle\big)^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$, every element has order 1, 2, or 4, so we see that $\big(\mathbb{Z}/\langle 15 \rangle\big)^\times \cong \mathbb{Z}/\langle 2^2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$. Similarly, we have

$$(\mathbb{F}_{17})^\times = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8\}$$

and $(\mathbb{F}_{17})^\times/\langle -1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8\}$ which is generated by 3, so $(\mathbb{F}_{17})^\times/\langle -1 \rangle \cong \mathbb{Z}/\langle 2^3 \rangle$. The field $\mathbb{F}_8$ has characteristic 2, so every element added to itself is 0, whence $\mathbb{F}_8^+ \cong \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$. Because we have $(\mathbb{Z}/\langle 16 \rangle)^\times = \{1, 3, 5, 7, 9, 11, 13, 15\}$, every element has order 1, 2, or 4, so $(\mathbb{Z}/\langle 16 \rangle)^\times \cong \mathbb{Z}/\langle 2^2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$. Finally, the group μ_8 is cyclic so $\mu_8 \cong \mathbb{Z}/\langle 2^3 \rangle$. $\square$

3.10.6 Problem. Determine the number of abelian groups of order 720 up to isomorphism.

Solution. Since $720 = 2^4 \cdot 3^2 \cdot 5$, the Corollary 3.10.4 implies that the abelian groups of order 720 are isomorphic to

$$\begin{array}{ll}
\frac{\mathbb{Z}}{\langle 2^4 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^4 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\
\frac{\mathbb{Z}}{\langle 2^3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\
\frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\
\frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} \\
\frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3^2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle} & \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 2 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 3 \rangle} \oplus \frac{\mathbb{Z}}{\langle 5 \rangle}.
\end{array}$$

There are 10 isomorphic classes of abelian groups of order 720. $\square$

3.10.7 Remark. For any prime integer p, Corollary 3.10.4 implies that the number of abelian groups of order p^k, up to isomorphism, is the number of integer partitions of k.

3.11 Jordan Canonical Form

The structure theorem for all finitely generated modules over a principal ideal domain has a striking application to linear algebra.

3.11.1 Proposition. *Let K be a field and let V be a finite-dimensional K-vector space. Choosing a linear operator $T : V \to V$ is equivalent to endowing V with structure of a module over the polynomial ring $K[t]$.*

Sketch of Proof.
($\Rightarrow$) Fix a linear operator $T : V \to V$. To equip V with the structure of a $K[t]$-module, we must define the product of a polynomial $f := a_0 + a_1 t + \cdots + a_n t^n \in K[t]$ and a vector $v \in V$. We set $f v := a_0 V + a_1 T(v) + a_2 T^2(v) + \cdots + a_n T^n(v)$. The right side is $[f(T)](v)$ where $f(T) = a_0 I + a_1 T + a_2 T^2 + \cdots + a_n T^n \in \operatorname{End}_K(V)$. One verifies that this makes V into a $K[t]$-module.

In particular, multiplying by t is the same as acting by T. Multiplying by a polynomial of degree 0 is just scalar multiplication by an element in K.

($\Leftarrow$) Multiplication by t defines a map $T : V \to V$. For all $a \in K$ and all $v, w \in V$, the $K[t]$-module structure demonstrates that $T(a v + w) = t(a v + w) = a t v + t w = a T(v) + T(w)$, so T is a linear operator on V. Identifying elements in K with constant polynomials, we see that V is a K-vector space. □

3.11.2 Theorem. *Let V be a nonzero finite-dimensional K-vector space. For any linear operator $T : V \to V$, there exists a positive integer ℓ and unique monic polynomials $q_1, q_2, \ldots, q_\ell \in K[t]$ of positive degree such that q_j divides q_{j+1} for all $1 \leqslant j < \ell$ and*

$$V \cong \frac{K[t]}{\langle q_1 \rangle} \oplus \frac{K[t]}{\langle q_2 \rangle} \oplus \cdots \oplus \frac{K[t]}{\langle q_\ell \rangle}.$$

Proof. Proposition 3.11.1 shows that V is a $K[t]$-module. Since $K[t]$ is a principal ideal domain, Theorem 3.9.1 expresses V as a direct sum of cyclic $K[t]$-modules. There are no free summands, because V is finite-dimensional. □

3.11.3 Definition. The polynomial $q_\ell(t)$ in Theorem 3.11.2 is called the ***minimal polynomial*** of the linear operator T. It is the unique monic polynomial $m_T \in K[t]$ of lowest degree such that $m_T(T) = 0$. The ***characteristic polynomial*** of T is the product $\chi_T(t) := \prod_{i=1}^{\ell} q_i(t)$.

3.11.4 Remark. Suppose that $q = b_0 + b_1 t + \cdots + b_{m-1} t^{m-1} + t^m \in K[t]$. Relative to the basis $1, t, t^2, \ldots, t^{m-1}$ for $K[t]/\langle q \rangle$, we have

$$M(T) := \begin{bmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & 1 & \cdots & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -b_{m-1} \end{bmatrix}.$$

This is called the ***companion*** matrix of q.

Every square matrix over a field is similar to a matrix in rational canonical form.

3.11.5 Theorem (Rational canonical form). *Let K be a field and let V be a finite-dimensional K-vector space. For any linear operator $T : V \to V$, there exists a basis of V such that the matrix $\mathbf{M}(T)$ is block diagonal and each block is a companion matrix.* □

The Jordan canonical form is named after Camille Jordan, who first stated it in 1870.

3.11.6 Corollary. *Let K be an algebraic closed field and let V be a nonzero finite-dimensional K-vector space. For any linear operator $T : V \to V$, there exists a positive integer k, elements $\lambda_1, \lambda_2, \dots, \lambda_k \in K$, and positive integers $e_1, e_2, \dots, e_k$ such that*

$$V \cong \frac{K[t]}{\langle (t-\lambda_1)^{e_1} \rangle} \oplus \frac{K[t]}{\langle (t-\lambda_2)^{e_2} \rangle} \oplus \cdots \oplus \frac{K[t]}{\langle (t-\lambda_k)^{e_k} \rangle}.$$

Sketch of Proof. Over an algebraically closed field, every polynomial factors into a product of linear ones. Combining the factorization of the polynomials q_j and Theorem 2.3.11 yield the decomposition. □

3.11.7 Remark. Relative to the basis $1, t-\lambda, (t-\lambda)^2, \dots, (t-\lambda)^{e-1}$ for the K-vector space $K[t]/\langle (t-\lambda)^e \rangle$, we have

For all nonnegative j, observe that
$t\,(t-\lambda)^j = 1\,(t-\lambda)^{j+1} + \lambda\,(t-\lambda)^j$.

$$M(T) := \begin{bmatrix} \lambda & 0 & \cdots & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & \cdots & 1 & \lambda \end{bmatrix}.$$

This is called the ***Jordan*** matrix of $(t-\lambda)^e$.

Over an algebraically closed field, every square matrix is similar to a matrix in Jordan canonical form.

3.11.8 Theorem (Jordan canonical form). *Let K be algebraically closed and let V be a finite-dimensional nonzero K-vector space. For any linear operator $T : V \to V$, there exists a basis of V such that the matrix $\mathbf{M}(T)$ is block diagonal and each block is a Jordan matrix.* □

3.11.9 Problem. Construct all linear operators $T : K^6 \to K^6$ with minimal polynomial $(t-5)^2\,(t-6)^2$ up to similarity.

Solution. The minimal polynomial of T divides the characteristic polynomial of T and these polynomials have the same irreducible factors. Thus, Corollary 3.11.6 implies that K^6 is isomorphic to one of the following:

$$\begin{array}{l} \frac{K[t]}{\langle (t-5)^2 \rangle} \oplus \frac{K[t]}{\langle (t-6)^2 \rangle} \oplus \frac{K[t]}{\langle (t-6)^2 \rangle} \\ \frac{K[t]}{\langle (t-5)^2 \rangle} \oplus \frac{K[t]}{\langle (t-6)^2 \rangle} \oplus \frac{K[t]}{\langle t-6 \rangle} \oplus \frac{K[t]}{\langle t-6 \rangle} \\ \frac{K[t]}{\langle (t-5)^2 \rangle} \oplus \frac{K[t]}{\langle t-5 \rangle} \oplus \frac{K[t]}{\langle (t-6)^2 \rangle} \oplus \frac{K[t]}{\langle t-6 \rangle} \\ \frac{K[t]}{\langle (t-5)^2 \rangle} \oplus \frac{K[t]}{\langle t-5 \rangle} \oplus \frac{K[t]}{\langle t-5 \rangle} \oplus \frac{K[t]}{\langle (t-6)^2 \rangle} \\ \frac{K[t]}{\langle (t-5)^2 \rangle} \oplus \frac{K[t]}{\langle (t-5)^2 \rangle} \oplus \frac{K[t]}{\langle (t-6)^2 \rangle}. \end{array}$$

□

The Jordan canonical form for the matrix of the desired linear operators is one of the following:

$$\begin{bmatrix} 5&0&0&0&0&0 \\ 1&5&0&0&0&0 \\ 0&0&6&0&0&0 \\ 0&0&1&6&0&0 \\ 0&0&0&0&6&0 \\ 0&0&0&0&1&6 \end{bmatrix}, \quad \begin{bmatrix} 5&0&0&0&0&0 \\ 1&5&0&0&0&0 \\ 0&0&6&0&0&0 \\ 0&0&1&6&0&0 \\ 0&0&0&0&6&0 \\ 0&0&0&0&0&6 \end{bmatrix},$$

$$\begin{bmatrix} 5&0&0&0&0&0 \\ 1&5&0&0&0&0 \\ 0&0&5&0&0&0 \\ 0&0&0&6&0&0 \\ 0&0&0&1&6&0 \\ 0&0&0&0&0&6 \end{bmatrix}, \quad \begin{bmatrix} 5&0&0&0&0&0 \\ 1&5&0&0&0&0 \\ 0&0&5&0&0&0 \\ 0&0&0&5&0&0 \\ 0&0&0&0&6&0 \\ 0&0&0&0&1&6 \end{bmatrix},$$

$$\begin{bmatrix} 5&0&0&0&0&0 \\ 1&5&0&0&0&0 \\ 0&0&5&0&0&0 \\ 0&0&1&5&0&0 \\ 0&0&0&0&6&0 \\ 0&0&0&0&1&6 \end{bmatrix}.$$