# MODULES OVER A PID

KEITH CONRAD

Every vector space over a field $K$ that has a finite spanning set has a finite basis: it is isomorphic to $K^n$ for some $n \geq 0$. When we replace the scalar field $K$ with a commutative ring $A$, it is no longer true that every $A$-module with a finite generating set has a basis: not all modules have bases. But when $A$ is a PID, we get something nearly as good as that:

(1) Every submodule of $A^n$ has a basis of size at most $n$.
(2) Every finitely generated torsion-free $A$-module $M$ has a finite basis: $M \cong A^n$ for a unique $n \geq 0$.
(3) Every finitely generated $A$-module $M$ is isomorphic to $A^d \oplus T$, where $d \geq 0$ and $T$ is a finitely generated torsion module.

We will prove this based on how a submodule of a finite free module over a PID sits inside the free module. Then we'll learn how to count with ideals in place of positive integers.

## 1. Preliminary results

We start with two lemmas that have nothing to do with PIDs.

**Lemma 1.1.** *If $A$ is a nonzero commutative ring and $A^m \cong A^n$ as $A$-modules then $m = n$.*

*Proof.* The simplest proof uses a maximal ideal $\mathfrak{m}$ in $A$. Setting $M = A^m$ and $N = A^n$, if $M \cong N$ as $A$-modules then it restricts to an isomorphism $\mathfrak{m}M \cong \mathfrak{m}N$ and we get an induced isomorphism $M/\mathfrak{m}M \cong N/\mathfrak{m}N$. This says $(A/\mathfrak{m})^m \cong (A/\mathfrak{m})^n$ as $A$-modules, hence also as $A/\mathfrak{m}$-vector spaces, so $m = n$ from the well-definedness of dimension for vector spaces. □

Lemma 1.1 says all bases in a finite free module over a nonzero commutative ring have the same size, and we call the size of that basis the *rank* of the free module. Therefore the term rank means dimension when the ring is a field.[1] The proof of Lemma 1.1 remains valid for free modules with a basis of infinite cardinality, so the rank of a free module with an infinite basis is well-defined as a cardinal number. For our purposes, free modules of finite rank will be all we care about.

Commutativity in Lemma 1.1 is important: there are noncommutative rings $A$ such that $A^2 \cong A$ as left $A$-modules.

**Lemma 1.2.** *Every finitely generated torsion-free module $M$ over an integral domain $A$ can be embedded in a finite free $A$-module. More precisely, if $M \neq 0$ there is an embedding $M \hookrightarrow A^d$ for some $d \geq 1$ such that the image of $M$ intersects each standard coordinate axis of $A^d$.*

*Proof.* Let $K$ be the fraction field of $A$ and $x_1, \ldots, x_n$ be a generating set for $M$ as an $A$-module. We will show $n$ is an upper bound on the size of each $A$-linearly independent subset of $M$. Let $f\colon A^n \to M$ be the linear map where $f(e_i) = x_i$ for all $i$. (By $e_1, \ldots, e_n$

[1] The word "rank" means something completely different in linear algebra – the dimension of the image of a linear map.

we mean the standard basis of $A^n$.) Let $y_1, \ldots, y_k$ be linearly independent in $M$, so their $A$-span is isomorphic to $A^k$. Write $y_j = \sum_{i=1}^n a_{ij}x_i$ with $a_{ij} \in A$. We pull the $y_j$'s back to $A^n$ by setting $v_j = (a_{1j}, \ldots, a_{nj})$, so $f(v_j) = y_j$. A linear dependence relation on the $v_j$'s is transformed by $f$ into a linear dependence relation on the $y_j$'s, which is a trivial relation by their linear independence. Therefore $v_1, \ldots, v_k$ is $A$-linearly independent in $A^n$, hence $K$-linearly independent in $K^n$. By linear algebra over fields, $k \leq n$.

From the bound $k \leq n$, there is a linearly independent subset of $M$ with maximal size, say $t_1, \ldots, t_d$. Then $\sum_{j=1}^d At_j \cong A^d$. We will find a scalar multiple of $M$ inside of this. For each $x \in M$, the set $\{x, t_1, \ldots, t_d\}$ is linearly dependent by maximality of $d$, so there is a nontrivial linear relation $ax + \sum_{i=1}^d a_i t_i = 0$, necessarily with $a \neq 0$. Thus $ax \in \sum_{j=1}^d At_j$. Letting $x$ run through the spanning set $x_1, \ldots, x_n$ there is an $a \in A - \{0\}$ such that $ax_i \in \sum_{j=1}^d At_j$ for all $i$, so $aM \subset \sum_{j=1}^d At_j$. Multiplying by $a$ is an isomorphism of $M$ with $aM$, so we have the sequence of $A$-linear maps

$$M \to aM \hookrightarrow \sum_{j=1}^d At_j \to A^d,$$

where the last map is an isomorphism. □

## 2. Submodules of a finite free module

First we will show submodules of a finite free module over a PID are finitely generated, with a natural upper bound on the number of generators.

**Theorem 2.1.** *When $A$ is a* PID*, each submodule of a free $A$-module of rank $n$ is finitely generated with at most $n$ generators.*

*Proof.* A free $A$-module of rank $n$ is isomorphic to $A^n$, so we may assume the free $A$-module is literally $A^n$. We will argue by induction on $n$. The case where $n = 0$ is trivial and the case where $n = 1$ is true since $A$ is a PID: every $A$-submodule of $A$ is an ideal, hence of the form $Aa$ since all ideals in $A$ are principal.

Suppose $n \geqslant 1$ and the theorem is proved for all submodules of $A^n$. Let $M \subset A^{n+1}$ be a submodule. We want to show $M$ has at most $n+1$ generators. View $M \subset A^{n+1} = A^n \oplus A$ and let $\pi\colon A^n \oplus A \twoheadrightarrow A^n$ be projection to the first component of this direct sum. Let's look at the image and kernel of $\pi|_M$, the restriction of $\pi$ to $M$. Its image is $\pi(M)$, which is a submodule of $A^n$ and therefore has at most $n$ generators by the inductive hypothesis, so $\pi(M) = \sum_{i=1}^k Ay_i$ for some $y_1, \ldots, y_k \in A^n$ where $k \leq n$. We can write $y_i = \pi(x_i)$ for some $x_i \in M$, so $\pi(M) = \sum_{i=1}^k A\pi(x_i)$. And $\ker(\pi|_M) = M \cap (0 \oplus A)$, with $0 \oplus A \cong A$ as $A$-modules. Every $A$-submodule of $A$ has a single generator since $A$ is a PID, so $\ker(\pi|_M) = Ax_0$ for some $x_0 \in M$.

We will show $M = \sum_{i=0}^k Ax_i$, so $M$ has at most $k+1$ generators and $k+1 \leqslant n+1$. The containment $\sum_{i=0}^k Ax_i \subset M$ is clear. For the reverse containment, pick an arbitrary $x \in M$ and the previous paragraph tells us $\pi(x) = a_1\pi(x_1) + \cdots + a_k\pi(x_k) = \pi(a_1x_1 + \cdots + a_kx_k)$ for some $a_1, \ldots, a_k$ in $A$. Therefore $x - \sum_{i=1}^k a_ix_i \in \ker(\pi|_M)$, so $x - \sum_{i=1}^k a_ix_i = a_0x_0$ for some $a_0 \in A$. Thus $x = a_0x_0 + a_1x_1 + \cdots + a_kx_k \in \sum_{i=0}^k Ax_i$, so $M \subset \sum_{i=0}^k Ax_i$. □

Next we will refine the previous theorem by showing a submodule of a finite free $A$-module is free (has a basis). The proof will be quite similar to the one we just gave, but it will not logically depend on it.

**Theorem 2.2.** *When $A$ is a* PID*, each submodule of a free $A$-module of rank $n$ is free of rank $\leqslant n$.*

*Proof.* As before, since a free $A$-module of rank $n$ is isomorphic to $A^n$, we can assume the free $A$-module we use is $A^n$. We'll induct on $n$.

The case $n = 0$ is trivial and the case $n = 1$ follows from all submodules of $A$ being (0) or principal with a nonzero generator, and $Aa \cong A$ as $A$-modules when $a$ is nonzero in $A$ since $A$ is an integral domain.

Suppose $n \geqslant 1$ and the theorem is proved for all submodules of $A^n$. For a submodule $M$ of $A^{n+1}$, to show $M$ is free of rank at most $n+1$ write $A^{n+1} = A^n \oplus A$ and let $\pi\colon A^n \oplus A \twoheadrightarrow A^n$ be projection to the first component. Since $\pi(M)$ is a submodule of $A^n$, $\pi(M)$ is free of rank $\leqslant n$ by the inductive hypothesis.

Case 1: $\pi(M) = 0$. Here $M \subset 0 \oplus A$, so $M$ is free of rank at most 1 since $A$ is a PID.

Case 2: $\pi(M) \neq 0$. Here $\pi(M)$ is a nonzero submodule of $A^n$, so $\pi(M)$ is free of positive rank $d \leq n$. Write a basis of $\pi(M)$ as $\pi(e_1), \ldots, \pi(e_d)$ where $e_i \in M$: $\pi(M) = \bigoplus_{i=1}^d A\pi(e_i)$. The elements $e_1, \ldots, e_d$ in $M$ are linearly independent since their images under $\pi$ are: if $\sum a_i e_i = 0$ in $M$ then apply $\pi$ to get $\sum a_i \pi(e_i) = 0$ in $\pi(M)$, so all $a_i$ are 0.

For $m \in M$, $\pi(m) = \sum_{i=1}^d a_i \pi(e_i)$ for unique $a_1, \ldots, a_d \in A$. Then $\pi(m - \sum_{i=1}^d a_i e_i) = 0$, so $m - \sum_{i=1}^d a_i e_i \in \ker(\pi|_M)$. We get inverse maps

$$M \longleftrightarrow A^d \oplus \ker(\pi|_M) \quad \text{by} \quad \begin{cases} m \longmapsto (a_1, \ldots, a_d, m - \sum_{i=1}^d a_i e_i) \\ \sum_{i=1}^d a_i e_i + k \longmapsfrom (a_1, \ldots, a_d, k) \end{cases}$$

and you should check both directions are linear. Therefore $M \cong A^d \oplus \ker(\pi|_M)$ as $A$-modules, so $M$ is a free $A$-module of rank $d$ or $d+1$ (depending on whether or not $\ker(\pi|_M)$ is $\{0\}$), and $d + 1 \leq n + 1$. □

Theorem 2.2 is always false if $A$ is not a PID, even for the $A$-module $A$ itself.

**Non-example 2.3.** If $A$ is not a PID then either it is not an integral domain or it has a nonprincipal ideal. If $A$ is not an integral domain then we have $xy = 0$ for some nonzero $x$ and $y$ in $A$, and the principal ideal $Ax$ is not a free $A$-module. If $A$ has a nonprincipal ideal then that ideal is not a free $A$-module.

**Remark 2.4.** Theorem 2.2 is true for non-finitely generated free modules: every submodule of a free module over a PID is free. The proof allowing infinite bases uses Zorn's lemma. See [5, pp. 650–651].

**Corollary 2.5.** *When $A$ is a* PID*, every finitely generated torsion-free $A$-module is a finite free $A$-module.*

*Proof.* By Lemma 1.2, such a module embeds into a finite free $A$-module, so it is finite free too by Theorem 2.2. □

The term "free" in "torsion-free module" and "free module" means different things: a torsion-free module has no nonzero torsion elements (all elements have annihilator ideal (0) aside from the element 0), while a free module has a basis. So Corollary 2.5 is saying a finitely generated module over a PID that has no torsion elements admits a basis. Corollary 2.5 is *false* without the finite generatedness hypothesis. For example, $\mathbf{Q}$ is a torsion-free abelian group but it has no basis over $\mathbf{Z}$: every (nonzero) free $\mathbf{Z}$-module has proper $\mathbf{Z}$-submodules (that is, proper subgroups) of finite index while $\mathbf{Q}$ does not.

**Corollary 2.6.** *Let $A$ be a* PID*. If we have a tower of $A$-modules $M \supset M' \supset M''$ with $M \cong A^n$ and $M'' \cong A^n$ then $M' \cong A^n$.*

*Proof.* Since $M$ is free of rank $n$ and $M'$ is a submodule, Theorem 2.2 tells us $M' \cong A^m$ with $m \leq n$. Using Theorem 2.2 on $M''$ as a submodule of $M'$, $M'' \cong A^k$ with $k \leq m$. By hypothesis $M'' \cong A^n$, so $k = n$ by Lemma 1.1. Thus $m = n$. □

Corollaries 2.5 and 2.6 are both generally false when $A$ is not a PID.

**Non-example 2.7.** Let $A = \mathbf{Z}[\sqrt{-5}]$ and consider the tower of ideals

$$3\mathbf{Z}[\sqrt{-5}] \subset (3, 1+\sqrt{-5}) \subset \mathbf{Z}[\sqrt{-5}].$$

The bottom and top are principal ideals, so they are free $A$-modules of rank 1. The middle ideal $(3, 1+\sqrt{-5})$ is finitely generated and torsion-free, but is not principal and therefore is not a free $A$-module. (A nonzero ideal is a free module only when it is principal, since all pairs of elements in an ideal are linearly related.)

There is a convenient way of picturing a submodule of a finite free module over a PID: bases can be chosen for the module and submodule that are aligned nicely, as follows.

**Definition 2.8.** If $A$ is a PID, $M$ is a finite free $A$-module, and $M'$ is a submodule of $M$, then a basis $\{v_1, \ldots, v_n\}$ of $M$ and a basis $\{a_1 v_1, \ldots, a_m v_m\}$ of $M'$ with $a_i \in A - \{0\}$ and $m \leq n$ is called a pair of *aligned* bases.

Pictures will explain what alignment of bases means before we give the main theorem about them.

**Example 2.9.** Let $A = \mathbf{Z}$, $M = \mathbf{Z}[i]$ and take $M' = (1+2i)\mathbf{Z}[i]$. So $M = \mathbf{Z} + \mathbf{Z}i$ and

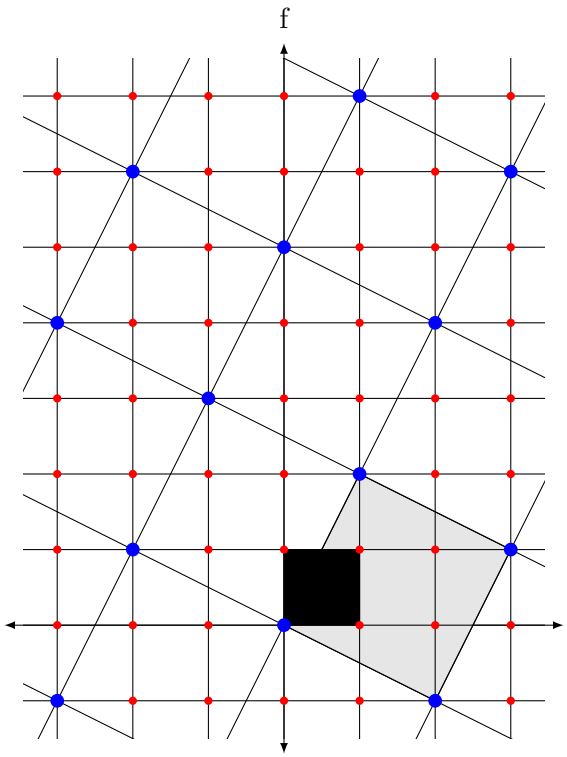
$$M' = (1+2i)\mathbf{Z}[i] = (1+2i)\mathbf{Z} + (1+2i)\mathbf{Z}i = \mathbf{Z}(1+2i) + \mathbf{Z}(-2+i).$$

The obvious $\mathbf{Z}$-bases for $M$ and $M'$ are $\{1, i\}$ and $\{1+2i, -2+i\}$. In Figure 1, we shade a box having each basis as a pair of edges and translate each box across the plane. The modules $M$ and $M'$ are the intersection points of the networks of lines formed by the small and large boxes, respectively. The modules do not know about the lines, which only show us how a choice of basis gives a specific way to picture how the module is generated by the basis.

To see a completely different picture of the same two modules $M$ and $M'$, we use new bases: $\{1+2i, i\}$ for $M$ and $\{1+2i, 5i\}$ for $M'$. These are bases because of the relations

$$\begin{pmatrix} 1+2i \\ i \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad \begin{pmatrix} 1+2i \\ 5i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1+2i \\ -2+i \end{pmatrix},$$

where the two matrices are integral with determinant 1, so the elements of $\mathbf{Z}[i]$ in the vector components on both sides have the same $\mathbf{Z}$-span. These new bases lead to Figure 2, where the parallelograms with each basis as a pair of edges is shaded and looks quite unlike the shaded boxes of Figure 1. Translating the parallelograms across the plane produces two new networks of lines (both sharing all the vertical lines) The intersection points are *the same* as before; make sure you can see the vertices of the large box from Figure 1 as intersection points of lines in Figure 2. In Figure 2 five of the parallelograms for $M$ fill up of the parallelograms for $M'$. These bases are aligned.




$$\mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i, \quad (1+2i) = \mathbf{Z}(1+2i) + \mathbf{Z}(-2+i)$$

FIGURE 1. Nonaligned bases for a modules and submodule

**Theorem 2.10.** *Each finite free $A$-module $M$ of rank $n \geqslant 1$ and nonzero submodule $M'$ of rank $m \leqslant n$ admit a pair of aligned bases: there is a basis $v_1, \ldots, v_n$ of $M$ and nonzero $a_1, \ldots, a_m \in A$ such that*

$$M = \bigoplus_{i=1}^{n} Av_i \qquad \text{and} \qquad M' = \bigoplus_{j=1}^{m} Aa_j v_j.$$

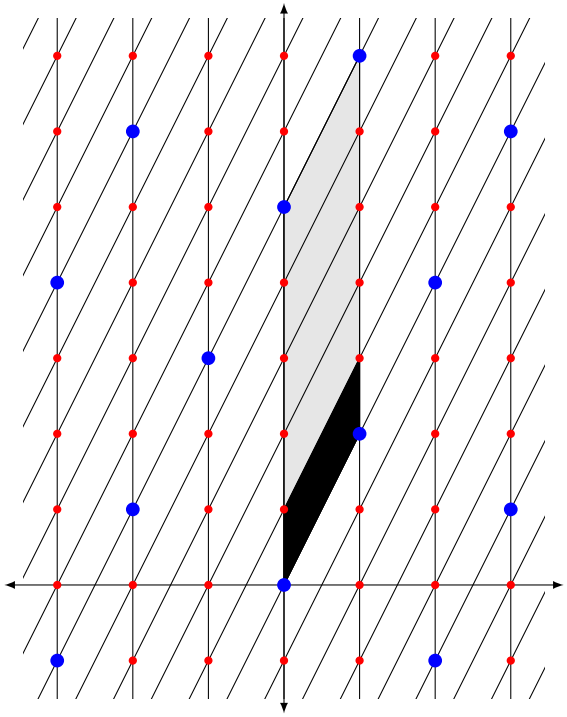
*We can also arrange that $a_1 \mid a_2 \mid \cdots \mid a_m$.*

The condition $a_1 \mid a_2 \mid \cdots \mid a_m$ at the end of the theorem plays an important role in the proof of the theorem, but it is not used in any applications presented later except for Theorem 3.6, so you can largely ignore it.

*Proof.* Our argument is based on [6, Sect. 1.5]. An $A$-basis of $M$ gives us coordinate functions for that basis, which are $A$-linear maps $M \to A$: for an $A$-basis $v_1, \ldots, v_n$ of $M$, its dual basis is the $A$-linear maps $v_j^\vee : M \to A$ where $v_j^\vee(x_1v_1 + \cdots + x_dv_d) = x_j$ for $x_1, \ldots, x_d \in A$. Bases for $M$ and $M'$ as in the theorem are "aligned" coordinate systems on $M$ and $M'$.

Motivation. To explain the main idea in the proof, we'll first suppose the conclusion of the theorem is true and derive an important consequence about the images of all $A$-linear maps $\varphi\colon M \to A$ (the dual module of $M$) when they are restricted to $M'$: there is a nonzero $A$-linear map $\psi\colon M \to A$ such that

$$\varphi(M') \subset \psi(M') \quad \text{for all} \quad \varphi.$$



$$\mathbf{Z}[i] = \mathbf{Z}(1+2i) + \mathbf{Z}i, \quad (1+2i) = \mathbf{Z}(1+2i) + \mathbf{Z} \cdot 5i$$

FIGURE 2. Aligned bases for a module and submodule

To show this, by the formula for $M'$ in the conclusion of the theorem we get for all $\varphi$ that

$$\varphi(M') = \varphi\Big(\sum_{j=1}^{m} Aa_j v_j\Big) = \sum_{j=1}^{m} Aa_j \varphi(v_j) \in Aa_1 + \cdots + Aa_m.$$

Since $A$ is a PID, $Aa_1 + \cdots + Aa_m = (a)$ for some nonzero $a \in A$, so $\varphi(M') \subset (a)$ for all $\varphi$.[2]

Write $a = c_1a_1 + \cdots + c_ma_m$ with $c_j \in A$ (the choice of $c_j$'s may not be unique, but fix such a representation for $a$) and define $\psi = \sum_{j=1}^{m} c_j e_j^\vee$ as a linear map $M \to A$. Then $\psi(\sum_{j=1}^{m} a_j e_j) = \sum_{j=1}^{m} c_j a_j = a$ and $\sum_{j=1}^{m} a_j e_j \in M'$, so

$$(a) \subset \psi(M') \subset (a).$$

Thus $\psi(M') = (a)$ and this ideal is the unique maximal member with respect to inclusion among all ideals $\varphi(M')$ as $\varphi$ varies over all linear maps $M \to A$. (This is not saying $(a)$ is a maximal ideal!). This ends the motivation.

Step 1. The set of ideals $S := \{\varphi(M') : \varphi\colon M \to A \text{ is linear}\}$ is not $\{(0)\}$ and has a maximal member $(a)$.

Let $\{v_1, \ldots, v_n\}$ be a basis of $M$. Since $M' \neq \{0\}$, at least one coordinate function $v_j^\vee$ for this basis of $M$ is not identically 0 on $M'$, which makes $v_j^\vee(M')$ a nonzero ideal in $S$.

Each nonzero ideal of $A$ is contained in only finitely many ideals of $A$ since $A$ is a PID: if $(x)$ is a nonzero ideal then we have $(x) \subset (y)$ if and only if $y \mid x$. Up to unit multiples, there

[2]If $a_1 \mid a_2 \mid \cdots \mid a_m$, which we don't want to assume, then we can let $a = a_1$ since $(a_m) \subset \cdots \subset (a_2) \subset (a_1)$.

are only finitely many possible $y$ since $x$ has only finitely many factors up to unit multiples. Applying this to $(x) = \varphi(M')$ for some $\varphi$ where $\varphi(M') \neq (0)$ and looking at the finitely many ideals containing $(x)$, $S$ contains a maximal member with respect to inclusion, say

$$(a) = \psi(M').$$

Then $a \neq 0$, and maximality means that if $(a) \subset \varphi(M')$ for some $\varphi$, then $\varphi(M') = (a)$.[3] Since $a \in \psi(M')$, there's some $v' \in M'$ such that $\boxed{a = \psi(v')}$.

Step 2: For the ideal $(a)$ in Step 1 and each $A$-linear map $\varphi\colon M \to A$, $a \mid \varphi(v')$ in $A$.

Write the ideal $(a, \varphi(v'))$ as $(b)$, where $b \in A - \{0\}$. For some $x$ and $y$ in $A$,

$$b = ax + \varphi(v')y = x\psi(v') + y\varphi(v') = (x\psi + y\varphi)(v').$$

Since $x\psi + y\varphi$ is a linear map $M \to A$,

$$(a) \subset (a, \varphi(v')) = (b) \subset (x\psi + y\varphi)(M'),$$

so the maximality of $(a)$ in Step 1 implies $(a) = (b) = (a, \varphi(v'))$. Therefore $a \mid \varphi(v')$.

Step 3: There is an $e_1 \in M$ such that $\psi(e_1) = 1$.

Write $v'$ in the basis $\{v_1, \ldots, v_n\}$ as $v' = \sum_{i=1}^n c_i v_i$. Then $c_i = v_i^\vee(v') \in (a)$ by Step 2, so $c_i = ab_i$ where $b_i \in A$. Thus

$$v' = a(b_1 v_1 + \cdots + b_n v_n).$$

Set $e_1 := b_1 v_1 + \cdots + b_n v_n$ in $M$, so $a = \psi(v') = a\psi(e_1)$ in $A$. Since $a \neq 0$, $\psi(e_1) = 1$.

Step 4: We have direct sum decompositions

$$M = Ae_1 \oplus \ker \psi, \qquad M' = Aae_1 \oplus (M' \cap \ker \psi).$$

First we show $M = Ae_1 + \ker \psi$. For each $v \in M$, $\psi(v - \psi(v)e_1) = \psi(v) - \psi(v)\psi(e_1) = \psi(v) - \psi(v) = 0$, so $v - \psi(v)e_1 \in \ker \psi$. Therefore $M \subset Ae_1 + \ker \psi$ and the reverse containment is obvious.

The sum in $Ae_1 + \ker \psi$ is direct since if $v \in Ae_1 \cap \ker \psi$ then $v = \alpha e_1$ and $\psi(v) = \alpha\psi(e_1) = \alpha$, so if $\psi(v) = 0$ then $\alpha = 0$.

Next we show $M' = Aae_1 + (M' \cap \ker \psi)$. For each $v \in M'$, $\psi(v - \psi(v)e_1) = 0$ as before, and $\psi(v) \in \psi(M') = (a)$, so $M \subset Aae_1 + \ker \psi$ and the reverse containment is obvious. This sum is direct for the same reason as above. This completes Step 4.

Step 5: Extend the direct sum decompositions in Step 4 to bases of $M$ and $M'$.

If $M' \cap \ker \psi = \{0\}$ then $M' = Aae_1$, so $m = 1$ and the theorem is proved in this case by using any basis of $\ker \psi$ as $e_2, \ldots, e_n$.

Now suppose $M' \cap \ker \psi \neq \{0\}$. Then $\ker \psi$ is free of rank $n - 1$ and $M' \cap \ker \psi$ is free of rank $m - 1 \geq 1$ by the direct sum decompositions of $M$ and $M'$ in Step 4.

Rename $a$ as $a_1$. By induction on $n$ (and $m$), there is a basis $e_2, \ldots, e_n$ of $\ker \psi$ and nonzero $a_2, \ldots, a_m$ in $A$ such that $a_2 e_2, \ldots, a_m e_m$ is a basis of $M' \cap \ker \psi$. Then the direct sums in Step 4 take the form

$$M = Ae_1 \oplus (Ae_2 \oplus \cdots \oplus Ae_n), \qquad M' = Aa_1 e_1 \oplus (Aa_2 e_2 \oplus \cdots \oplus Aa_m e_m).$$

If we are not interested in a relation like $a_1 \mid a_2 \mid \cdots \mid a_m$ then we are done with the proof. If instead we want to prove $a_1 \mid a_2 \mid \cdots \mid a_m$ then we can bring in $a_2 \mid \cdots \mid a_m$ by the inductive hypothesis. Why does $a_1 \mid a_2$? Do we need to go back and prove stronger forms of

[3] We anticipate $(a)$ will be the unique maximal member of $S$ by the argument in the motivational section at the start of this proof, but at the moment $(a)$ is just some maximal member of $S$.

earlier steps? That isn't necessary. Consider how $\varphi = e_1^\vee + e_2^\vee$ behaves on $v' = ae_1 = a_1e_1$: $a_1 = a = \varphi(v') \in \varphi(M')$, so $(a) \subset \varphi(M')$. By the maximality of $(a)$ in Step 1, $(a) = \varphi(M')$. Then $a_2 = \varphi(a_2e_2) \in \varphi(M') = (a) = (a_1)$, so $a_1 \mid a_2$. □

In this theorem, an aligned basis for $M$ and $M'$ depends on both modules: there need not be an aligned basis that uses an arbitrary basis for $M$ or an arbitrary basis for $M'$.

**Example 2.11.** Let $M = \mathbf{Z}^2$ and $M' = \{\binom{x}{y} \in \mathbf{Z}^2 : x \equiv y \bmod p\} = \mathbf{Z}\binom{1}{1} + \mathbf{Z}\binom{p}{0}$ for prime $p$. An example of aligned $\mathbf{Z}$-bases here is $\{\binom{1}{1}, \binom{1}{0}\}$ for $M$ and $\{\binom{1}{1}, p\binom{1}{0}\}$ for $M'$, so $[M : M'] = p$. (Another way to see $[M : M'] = p$ is that the mapping $M \to \mathbf{Z}/(p)$ where $\binom{x}{y} \mapsto x - y \bmod p$ is additive and surjective with kernel $M'$, so $M/M' \cong \mathbf{Z}/(p)$.) A general pair of aligned bases for $M$ and $M'$ has the form $\{v_1, v_2\}$ for $M$ and $\{a_1v_1, a_2v_2\}$ for $M'$, so $M/M' \cong \mathbf{Z}/(a_1) \times \mathbf{Z}/(a_2)$ as abelian groups. Then $[M : M'] = p = |a_1a_2|$, so $\{a_1, a_2\} = \{\pm 1, \pm p\}$. That means $v_1$ or $v_2$ (depending on whether $a_1$ or $a_2$ is $\pm 1$) has to be in $M'$, so the basis $\{\binom{1}{0}, \binom{0}{1}\}$ of $M$ isn't part of an aligned basis with $M'$ since neither element of that basis is in $M'$. Conversely, a vector in $\mathbf{Z}^2$ multiplied by $p$ has both of its coordinates divisible by $p$, so the basis $\{\binom{1}{1}, \binom{p+1}{1}\}$ of $M'$ is not part of an aligned basis with $M$.

**Corollary 2.12.** *Let $A$ be a* PID*, $M$ be finite free $A$-module, and $M'$ be a submodule of $M$. Then $M$ and $M'$ have the same rank if and only if $M/M'$ is a torsion module.*

*Proof.* Let $M$ have rank $n$. The module $M'$ is free of some rank $m \leq n$. Using aligned bases for $M$ and $M'$, we can write

$$M = \bigoplus_{i=1}^{n} Av_i \qquad \text{and} \qquad M' = \bigoplus_{j=1}^{m} Aa_jv_j$$

with nonzero $a_j$'s. Then $M/M' \cong \bigoplus_{j=1}^m A/(a_j) \oplus A^{n-m}$. This is a torsion module if and only if $m = n$. □

## 3. Applications to matrix groups

In this section we give applications of Corollary 2.6 and Theorem 2.10 to matrix groups.

A matrix in $\mathrm{GL}_n(\mathbf{Q})$ that has finite order does not have to have entries in $\mathbf{Z}$. For example, $\left(\begin{smallmatrix} -1 & x \\ 0 & 1 \end{smallmatrix}\right)$ has order 2 for all $x \in \mathbf{Q}$. But this matrix is conjugate to a matrix with entries in $\mathbf{Z}$: $\left(\begin{smallmatrix} 1 & -x/2 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & x \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -x/2 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. More generally, it turns out that every finite subgroup of $\mathrm{GL}_n(\mathbf{Q})$ is conjugate to a subgroup with entries in $\mathbf{Z}$. This is a special case of a result we prove below about subgroups of $\mathrm{GL}_n(K)$ where $K$ is the fraction field of a PID.

**Definition 3.1.** Let $A$ be a PID and $K$ be its fraction field. A subset $S$ of $K$ has a *common denominator in $A$* when there is a nonzero $a \in A$ such that $aS \subset A$.

**Example 3.2.** Every finite subset $S$ of $K$ has a common denominator in $A$: use the product of the denominators of the elements of $S$ when they are written as ratios of numbers in $A$.

**Example 3.3.** Let $S = \sum_{j=1}^n Ax_i$ be a finitely generated $A$-submodule of $K$. It has a common denominator in $A$, such as a common denominator of the numbers $x_1, \ldots, x_n$.

**Non-example 3.4.** In $\mathbf{Q}$, the set of reciprocal powers $\{1/2, 1/4, 1/8, \ldots, 1/2^n, \ldots\}$ has no common denominator in $\mathbf{Z}$.

**Theorem 3.5.** *Let $A$ be a* PID *and $K$ be its fraction field. Every subgroup $G$ of $\mathrm{GL}_n(K)$ whose matrix entries have a common denominator in $A$ is conjugate to a subgroup with matrix entries in $A$: there is a matrix $L \in \mathrm{GL}_n(K)$ such that all matrices in $LGL^{-1}$ have entries in $A$. In particular, every finite subgroup of $\mathrm{GL}_n(K)$ is conjugate to a subgroup with matrix entries in $A$.*

The common denominator hypothesis of this theorem means for some nonzero $a \in A$, $ag$ has matrix entries in $A$ for all $g \in G$.

*Proof.* For each $g \in G$, $g(A^n)$ is a finite free $A$-submodule of $K^n$. Let $M$ be the $A$-module $\sum_{g\in G} g(A^n)$, which is the set of finite sums of vectors in $K^n$ that belong to $g(A^n)$ for some $g \in G$. This is an $A$-module in $K^n$ that contains $A^n$ (use $g = I_n$). Note $M$ is $G$-stable (carried back to itself when acting on it by elements of $G$).

The common denominator hypothesis says there is a nonzero $a \in A$ such that each matrix $ag$ for $g \in G$ has all of its entries in $A$. Therefore $aM = \sum_{g\in G}(ag)(A^n) \subset A^n$, so $M \subset (1/a)A^n$ in $K^n$. Thus $A^n \subset M \subset (1/a)A^n$. By Corollary 2.6, $M \cong A^n$ as $A$-modules.

Let $\varphi\colon A^n \to M$ be an $A$-module isomorphism. Then $M = \varphi(A^n)$ is the $A$-linear span of $\varphi(e_1), \ldots, \varphi(e_n)$. These vectors are $A$-linearly independent since they span a free $A$-module of rank $n$, so they are also $K$-linearly independent: a nontrivial $K$-linear relation would become a nontrivial $A$-linear relation. Therefore the matrix $\Phi = [\varphi(e_1) \cdots \varphi(e_n)]$ is invertible, so $\Phi \in \mathrm{GL}_n(K)$ and $\Phi = \varphi$ on $A^n$.

For each $g \in G$, $gM \subset M$ since $M$ is $G$-stable, so $g\varphi(A^n) \in \varphi(A^n)$. Therefore $g(\Phi(A^n)) \subset \Phi(A^n)$, so $\Phi^{-1}g\Phi(A^n) \subset A^n$. This means the matrix $\Phi^{-1}g\Phi$ has entries in $A$ (its columns are $(\Phi^{-1}g\Phi)(e_i)$ for $i = 1, \ldots, n$). Letting $g$ run over $G$, the group $\Phi^{-1}G\Phi$ is conjugate to $G$ and its elements have matrix entries in $A$. □

Our second application to matrix groups will be the computation of normalizers. For a group $G$ and subgroup $H$ of $G$, the normalizer of $H$ is $\mathrm{N}_G(H) = \{g \in G : gHg^{-1} = H\} = \{g \in G : g^{-1}Hg = H\}$: this is the largest subgroup of $G$ in which $H$ is a normal subgroup.

**Theorem 3.6.** *Let $A$ be a* PID *and $K$ be its fraction field. In the group $\mathrm{GL}_n(K)$, both $\mathrm{GL}_n(A)$ and $\mathrm{SL}_n(A)$ have normalizer $K^\times \mathrm{GL}_n(A)$.*

We view $K^\times$ inside $\mathrm{GL}_n(K)$ as the nonzero scalar diagonal matrices $\{cI_n : c \in K^\times\}$. This is the center of $\mathrm{GL}_n(K)$.

*Proof.* The result is trivial when $n = 1$, since $\mathrm{GL}_1(K) = K^\times$ is commutative, so from now on we can assume $n \geq 2$. Set $G = \mathrm{GL}_n(K)$. We will show $\mathrm{N}_G(\mathrm{GL}_n(A)) = K^\times \mathrm{GL}_n(A)$ and then indicate how that argument can be modified to show $\mathrm{N}_G(\mathrm{SL}_n(A)) = K^\times \mathrm{GL}_n(A)$.

That $K^\times \mathrm{GL}_n(A) \subset \mathrm{N}_G(\mathrm{GL}_n(A))$ is obvious. To prove $\mathrm{N}_G(\mathrm{GL}_n(A)) \subset K^\times \mathrm{GL}_n(A)$, pick $g \in \mathrm{N}_G(\mathrm{GL}_n(A))$. We will find $c \in K^\times$ such that $cg \in \mathrm{GL}_n(A)$. The proof is based on an answer to the Mathoverflow question https://mathoverflow.net/questions/80667. Set $M = g(A^n)$.

Step 1: $M$ is a free $A$-module of rank $n$ and is $\mathrm{GL}_n(A)$-stable: $L(M) \subset M$ for all $L \in \mathrm{GL}_n(A)$.

The $A$-module $M$ is spanned by $g(e_1), \ldots, g(e_n)$ where $e_1, \ldots, e_n$ is the standard basis of $A^n$, and $g(e_1), \ldots, g(e_n)$ is $A$-linearly independent since $g$ is an invertible matrix over $A$. Thus $M \cong A^n$ as $A$-modules.

To show $M$ is $\mathrm{GL}_n(A)$-stable, we use the property $g^{-1}\,\mathrm{GL}_n(A)g = \mathrm{GL}_n(A)$, which is the condition of $g$ normalizing $\mathrm{GL}_n(A)$. For $L \in \mathrm{GL}_n(A)$, $L' := g^{-1}Lg$ is in $\mathrm{GL}_n(A)$ too, so

$Lg = gL'$. Therefore

$$L(M) = Lg(A^n) = gL'(A^n) = g(A^n) = M.$$

Step 2: There is $d \in A - \{0\}$ such that $dM \subset A^n$.

Let $d \in A - \{0\}$ be a common denominator for the coordinates of $g(e_1), \ldots, g(e_n)$ in $K^n$. Then $dg(e_i) \in A^n$ for $i = 1, \ldots, n$, so $dM \subset A^n$.

Step 3: There is $c \in K^\times$ such that $cg \in \mathrm{GL}_n(A)$.

By Steps 1 and 2, $dM$ is a submodule of $A^n$ with rank $n$, so by Theorem 2.10 we can find a basis $\{f_1, \ldots, f_n\}$ of $A^n$ and nonzero $a_1, \ldots, a_n$ in $A$ such that $\{a_1 f_1, \ldots, a_n f_n\}$ is a basis of $dM$ and $a_1 \mid a_2 \mid \cdots \mid a_n$. We won't use the full strength of that divisibility condition, but just $a_1 \mid a_i$ for $i = 1, \ldots, n$.

In the direct sum decomposition

$$dM = \bigoplus_{i=1}^n A a_i f_i,$$

divide through by $a_1$:

$$\frac{d}{a_1} M = \bigoplus_{i=1}^n A \frac{a_i}{a_1} f_i = A f_1 \oplus \bigoplus_{i=2}^n A \frac{a_i}{a_1} f_i.$$

Set $M' = (d/a_1)M$, so $M'$ is a submodule of $A^n$ (each $a_i/a_1$ is in $A$) and $M'$ contains the vector $f_1$ that's part of a basis $\{f_1, \ldots, f_n\}$ of $A^n$. Since $M$ is $\mathrm{GL}_n(A)$-stable by Step 1, so is $M'$.

The matrix $L$ with columns $f_1, \ldots, f_n$ (in that order) is in $\mathrm{GL}_n(A)$ since the columns are a basis of $A^n$, and $L(e_1) = f_1$. Then $e_1 = L^{-1}(f_1) \in M'$ because $L^{-1} \in \mathrm{GL}_n(A)$ and $M'$ is $\mathrm{GL}_n(A)$-stable. By a similar argument, if we permute the columns of $L$ to place $f_1$ in the $j$th column for $j = 2, \ldots, n$ then we get $e_j \in M'$. Thus $M'$ is a submodule of $A^n$ that contains $e_1, \ldots, e_n$, so $\boxed{M' = A^n}$. Rewriting that as $(d/a_1)g(A^n) = A^n$ tells us the matrix $(d/a_1)g$ is in $\mathrm{GL}_n(A)$, so $cg \in \mathrm{GL}_n(A)$ where $c = d/a_1 \in K^\times$. This completes the proof that $\mathrm{N}_G(\mathrm{GL}_n(A)) = K^\times \mathrm{GL}_n(A)$.

To show $\mathrm{N}_G(\mathrm{SL}_n(A)) = K^\times \mathrm{GL}_n(A)$, we have $K^\times \mathrm{GL}_n(A) \subset \mathrm{N}_G(\mathrm{SL}_n(A))$ since $\mathrm{SL}_n(A) \lhd \mathrm{GL}_n(A)$. For the reverse containment, if $g \in \mathrm{N}_G(\mathrm{SL}_n(A))$ then we want $c \in K^\times$ such that $cg(A^n) = A^n$, so $cg \in \mathrm{GL}_n(A)$. The procedure used above for $\mathrm{N}_G(\mathrm{GL}_n(A))$ can be applied to $\mathrm{N}_G(\mathrm{SL}_n(A))$, with the following changes: $M = g(A^n)$ is $\mathrm{SL}_n(A)$-stable rather than $\mathrm{GL}_n(A)$-stable in Step 1, and in Step 3 modify the matrix $L$ with columns $f_1, \ldots, f_n$ so that its last column is $u^{-1} f_n$ where $u = \det(f_1 \cdots f_n) \in A^\times$, as that makes $\det(L) = uu^{-1} = 1$, so $L \in \mathrm{SL}_n(A)$. □

## 4. Finitely generated modules

As an application of aligned bases for a submodule of a finite free module, we describe the structure of every finitely generated module over a PID.

**Theorem 4.1.** *Let $A$ be a* PID*. Every finitely generated $A$-module has the form $F \oplus T$ where $F$ is a finite free $A$-module and $T$ is a finitely generated torsion $A$-module. Moreover, $T \cong \bigoplus_{j=1}^m A/(a_j)$ for some $m$ with nonzero $a_i$.*

*Proof.* Let $M$ be a finitely generated $A$-module, with generators $x_1, \ldots, x_n$. Define $f\colon A^n \twoheadrightarrow M$ by $f(e_i) = x_i$. Then there is a surjective linear map $A^n \twoheadrightarrow M$, so $M$ is isomorphic to

a quotient $A^n/N$. As in the proof of Corollary 2.12, $A^n/N \cong \left(\bigoplus_{j=1}^m A/(a_j)\right) \oplus A^{n-m}$ for some $m \leq n$ and nonzero $a_j$'s. The direct sum of the $A/(a_j)$'s is a torsion module and $A^{n-m}$ is a finite free $A$-module. □

**Example 4.2.** Taking $A = \mathbf{Z}$, every finitely generated abelian group is isomorphic to $\mathbf{Z}^n \oplus G$ where $n \geq 0$ and $G$ is a finite abelian group (a finitely generated torsion abelian group must be finite).

**Corollary 4.3.** *Every finitely generated torsion module over a* PID $A$ *is a direct sum of cyclic torsion modules: it is isomorphic to* $A/(a_1) \oplus \cdots \oplus A/(a_k)$*, where the* $a_i$*'s are nonzero.*

Some $a_i$'s might be units, making $A/(a_i) = 0$.

*Proof.* A finitely generated module in Theorem 4.1 is a torsion module if and only if $F = 0$. The description of $T$ in Theorem 4.1 gives the desired cyclic decomposition for finitely generated torsion modules. □

Corollary 2.5 could be regarded as a consequence of Theorem 4.1: a finitely generated module is $F \oplus T$ where $F$ is finite free and $T$ is torsion, and being torsion-free forces $T = 0$, so the module is free.

When a finitely generated $A$-module is written as $F \oplus T$, where $F$ is a finite free submodule and $T$ is a torsion submodule, the choice of $F$ is not unique but $T$ is unique: $T$ is the set of all elements in $F \oplus T$ with nonzero annihilator ideal, which is a description that makes no reference to the direct sum decomposition. The best way to see $F$ is not unique is by examples.

**Example 4.4.** Using $A = \mathbf{Z}$, $\mathbf{Z} \times \mathbf{Z}/(2)$ has generating set $\{(1, \overline{0}), (0, \overline{1})\}$ and $\{(1, \overline{1}), (0, \overline{1})\}$. Therefore it can be written as $F_1 \oplus T_1$, where $F_1 = \langle (1, \overline{0}) \rangle \cong \mathbf{Z}$ and $T_1 = 0 \oplus \mathbf{Z}/(2)$, and also as $F_2 \oplus T_2$ where $F_2 = \langle (1, \overline{1}) \rangle \cong \mathbf{Z}$ and $T_2 = 0 \oplus \mathbf{Z}/(2) = T_1$.

**Example 4.5.** It can be shown that every unit in $\mathbf{Z}[\sqrt{2}]$ has the form $\pm(1 + \sqrt{2})^k$ some choice of sign $\pm 1$ and some integer $k$, so $\mathbf{Z}[\sqrt{2}]^\times$ is a finitely generated abelian group. The torsion subgroup of $\mathbf{Z}[\sqrt{2}]^\times$ is $\{\pm 1\}$, while $1 + \sqrt{2}$ and $-(1 + \sqrt{2})$ each generate different free subgroups that complement $\{\pm 1\}$:

$$\mathbf{Z}[\sqrt{2}]^\times = \{\pm 1\} \times (1 + \sqrt{2})^{\mathbf{Z}} = \{\pm 1\} \times (-(1 + \sqrt{2}))^{\mathbf{Z}}$$

This leads to two isomorphisms of $\mathbf{Z}[\sqrt{2}]^\times$ with $\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, which identify different subgroups with $\mathbf{Z}$ (the powers of $1 + \sqrt{2}$ and the powers of $-(1 + \sqrt{2})$) but both identify the same subgroup $\{\pm 1\}$ with $\mathbf{Z}/(2)$.

**Example 4.6.** It can be shown that $\mathbf{Z}[\sqrt{2}, \sqrt{3}]^\times = \pm(1 + \sqrt{2})^{\mathbf{Z}}(2 + \sqrt{3})^{\mathbf{Z}}(\sqrt{2} + \sqrt{3})^{\mathbf{Z}}$, where the units $1 + \sqrt{2}$, $2 + \sqrt{3}$, and $\sqrt{2} + \sqrt{3}$ (with respective inverses $\sqrt{2} - 1, 2 + \sqrt{3}$, and $\sqrt{3} - \sqrt{2}$) have no multiplicative relations over $\mathbf{Z}$: if $(1 + \sqrt{2})^a(2 + \sqrt{3})^b(\sqrt{2} + \sqrt{3})^c = 1$ for integer exponents $a$, $b$, and $c$, then $a = b = c = 0$. Therefore $\mathbf{Z}[\sqrt{2}, \sqrt{3}]^\times \cong \mathbf{Z}^3 \times \mathbf{Z}/2\mathbf{Z}$. Two examples of complements to $\pm 1$ in $\mathbf{Z}[\sqrt{2}, \sqrt{3}]^\times$ are $\langle 1 + \sqrt{2}, 2 + \sqrt{3}, \sqrt{2} + \sqrt{3} \rangle$ and $\langle 1 + \sqrt{2}, -(2 + \sqrt{3}), -(\sqrt{2} + \sqrt{3}) \rangle$.

While the free part of a direct sum decomposition is not unique, the rank of the free part is unique: writing $M = F \oplus T$ with $F$ finite free and $T$ necessarily being the torsion submodule $M_{\text{tor}}$ of $M$, we have $F \cong M/T = M/M_{\text{tor}}$ so the rank of $F$ is the rank of the finite free module $M/M_{\text{tor}}$. The *rank* of a finitely generated module over a PID $A$ is defined

to be the rank of its free part, which is well-defined even though the free part itself is not. In down-to-earth terms, the rank is the largest number of linearly independent torsion-free elements (over $\mathbf{Z}$, it is the largest number of independent elements of infinite order).

Our focus in this section was on describing the abstract structure of a finitely generated module over a PID, *not* proving a module over a PID arising somewhere in mathematics is finitely generated. The fact that certain abelian groups ($\mathbf{Z}$-modules) are finitely generated can be a major theorem (look up the Mordell–Weil theorem) and a formula for the rank can be a major theorem or conjecture (look up Dirichlet's unit theorem or the Birch and Swinnerton-Dyer conjecture).

Theorem 4.1 says for a finitely generated module $M$ over a PID $A$, $M = M_{\mathrm{tor}} \oplus F$ where $F$ is a free $A$-module. In particular, $M_{\mathrm{tor}}$ is a direct summand of $M$. That conclusion can become false if (i) $A$ is a PID and $M$ is *not* finitely generated or (ii) $M$ is finitely generated and $A$ is *not* a PID. We'll give examples of this using $A = \mathbf{Z}$ for (i) and $A = \mathbf{Z}[x]$ for (ii).

**Example 4.7.** Set $M = \prod_p \mathbf{Z}/(p)$, which is a $\mathbf{Z}$-module in a natural way. We will show the torsion submodule $T$ of $M$ is not a direct summand: $M \neq T \oplus N$ for a submodule $N$. The argument is based on [4, Theorem 10.2].

Step 1: $T = \bigoplus_p \mathbf{Z}/(p)$ and $T \neq M$.

To prove the claim, one containment is immediate: since elements in the direct sum have only finitely many nonzero coordinates and each $\mathbf{Z}/(p)$ is killed off by a single prime $p$, each element of the direct sum is killed off by a product of finitely many primes and thus is in $T$. Conversely, if $\mathbf{m} := (a_p \bmod p)_p$ is an element of $T$ and $k\mathbf{m} = 0$ where $k \in \mathbf{Z} - \{0\}$, then $ka_p \equiv 0 \bmod p$ for each prime $p$. When $p \nmid k$, $a_p \equiv 0 \bmod p$, so $\mathbf{m}$ has only finitely many possible nonzero coordinates (its $p$-coordinates where $p$ is a prime factor of $k$). Therefore $\mathbf{m} \in \bigoplus_p \mathbf{Z}/(p)$, which finishes Step 1. Because there are infinitely many primes, $T \neq M$.

Step 2: We can't write $M = T \oplus N$ for a $\mathbf{Z}$-submodule $N$ of $M$.

Assume there is such a direct sum decomposition. Then $N \cong M/T$, so $M$ has a submodule isomorphic to $M/T$. We will get a contradiction by showing $M$ and its submodules all share a property that is not true for $M/T$.

The property is this: $\bigcap_p pM = \{\mathbf{0}\}$, where the intersection runs over all primes. Indeed, for each prime $p$ the $p$-coordinate of an element of $pM$ has to be 0, so all coordinates of an element of $\bigcap_p pM$ equal 0. Therefore if $N$ is a submodule of $M$, $\bigcap_p pN = \{\mathbf{0}\}$.

In contrast to that, we will show $\bigcap_p p(M/T) \neq \{\overline{\mathbf{0}}\}$. Specifically, let $\mathbf{v} := (1, 1, 1, \ldots)$ be the element of $M$ with $p$-coordinate 1 mod $p$ for each prime $p$. We'll show

(i) $\mathbf{v} \notin T$, so $\overline{\mathbf{v}} \neq \overline{\mathbf{0}}$ in $M/T$,
(ii) $\overline{\mathbf{v}} \in \bigcap_p p(M/T)$.

Proof of (i): If $\mathbf{v} \in T$, then $k\mathbf{v} = \mathbf{0}$ for some nonzero integer $k$ since $\mathbf{v} \neq \mathbf{0}$. Looking at the coordinates of $k\mathbf{v}$, we get $k \equiv 0 \bmod p$ for each prime $p$, so $k$ has infinitely many prime factors and that forces $k = 0$, a contradiction.

Proof of (ii): Fix a prime $p$. We will find a $\mathbf{w} \in M$ and $\mathbf{t} \in T$ (depending on $p$). such that $\mathbf{v} = p\mathbf{w} + \mathbf{t}$, so $\mathbf{v} \equiv p\mathbf{w} \bmod T$, so $\mathbf{v} \in p(M/T)$.

All the coordinates of $\mathbf{v}$ are 1. For each prime $q$ other than $p$, $p$ is invertible mod $q$ so we can define $w_q \in \mathbf{Z}/(q)$ by the congruence $pw_q \equiv 1 \bmod q$. Define $w_p = 0 \bmod p$. Then $\mathbf{w} = (w_q)_q$ is in $M$ and $p\mathbf{w}$ has $q$-coordinate 1 for each $q \neq p$ and $p\mathbf{w}$ has $p$-coordinate 0. Therefore $\mathbf{v} = p\mathbf{w} + \mathbf{t}$ where $\mathbf{t}$ has $p$-coordinate 1 and every other coordinate 0, which means $\mathbf{t} \in T$. That completes Step 2.

**Remark 4.8.** This construction of a $\mathbf{Z}$-module whose torsion submodule is not a direct summand of it carries over without change to modules over a PID $A$ that has infinitely many non-associate irreducible elements. Let $M$ be the $A$-module $\prod_{(\pi)} A/(\pi)$, where the direct product is taken over all distinct maximal ideals $(\pi)$. It is left to the reader to prove the torsion submodule $T$ of $M$ is $\bigoplus_{(\pi)} A/(\pi)$ and $M \neq T \oplus N$ for an $A$-submodule $N$ of $M$ by an argument similar to the case $A = \mathbf{Z}$ above.

The infinite direct product $\prod_p \mathbf{Z}/(p)$ in Example 4.7 may seem artificial. What about using the abelian group $S^1$, whose torsion submodule is the group $\mu_\infty$ of all roots of unity? It seems plausible that we can't write $S^1 = \mu_\infty \times H$ for a subgroup $H$ of $S^1$, but that *is* possible by the Axiom of Choice since $\mu_\infty$ is a divisible abelian group. See Corollary 2.5 in https://kconrad.math.uconn.edu/blurbs/zorn1.pdf. Note that unlike $\mu_\infty$, the torsion submodule $\bigoplus_p \mathbf{Z}/(p)$ in Example 4.7 is not divisible.

**Example 4.9.** Let $A = \mathbf{Z}[x]$ and $r$ be an integer besides 0 and $\pm 1$, so the ideal $\mathfrak{a} := (r, x)$ in $A$ is not principal. We will show $M := A^2/\mathfrak{a}\binom{r}{x}$, which is a finitely generated $A$-module, does not have $M_{\mathrm{tor}}$ as a direct summand. This example and the argument behind it are from https://math.stackexchange.com/questions/3593455/.

Since $A$ is an integral domain and $\mathfrak{a}$ is a proper ideal in $A$, $\binom{r}{x} \notin \mathfrak{a}\binom{r}{x}$, so $\overline{\binom{r}{x}} \neq \overline{\mathbf{0}}$ in $M$.

Claim: $M_{\mathrm{tor}} = A\overline{\binom{r}{x}}$.

To prove the claim, we have $\overline{\binom{r}{x}} \in M_{\mathrm{tor}}$ since $x\overline{\binom{r}{x}} = \overline{\mathbf{0}}$ and $x \neq 0$. (Also $r\overline{\binom{r}{x}} = \overline{\mathbf{0}}$.) Thus $A\overline{\binom{r}{x}} \subset M_{\mathrm{tor}}$. For the reverse containment, let $\overline{\binom{a}{b}} \in M_{\mathrm{tor}}$ for $a$ and $b$ in $A$, so $c\overline{\binom{a}{b}} = \overline{\mathbf{0}}$ for some nonzero $c \in A$. That means $\binom{ca}{cb}$ is in $\mathfrak{a}\binom{r}{x}$, so $ca = dr$ and $cb = dx$ for some $d \in \mathfrak{a}$. We want to show $\overline{\binom{a}{b}}$ is in $A\overline{\binom{r}{x}}$.

If $d = 0$ then $ca$ and $cb$ are 0, so $a$ and $b$ are 0 since $c$ is nonzero and $\mathbf{Z}[x]$ is an integral domain. Thus $\overline{\binom{a}{b}} = \overline{\mathbf{0}} \in A\overline{\binom{r}{x}}$.

Suppose instead that $d \neq 0$. From $ca = dr$ and $cb = dx$ we have $b(dr) - a(dx) = bca - acb = 0$, so $d(br - ax) = 0$ and thus $br = ax$. Since $x \mid br$ and $x \nmid r$ (note $r$ is nonzero in $\mathbf{Z}$), $x \mid b$. Write $b = xs$ where $s \in A$, so $ax = br = xsr$. Thus $a = sr$, so $\binom{a}{b} = \binom{sr}{sx} = s\binom{r}{x}$, which implies $\overline{\binom{a}{b}} \in A\overline{\binom{r}{x}}$ in $M$. That proves the claim.

To show $M_{\mathrm{tor}}$ is not a direct summand of $M$, suppose $M = M_{\mathrm{tor}} \oplus N$ for some submodule $N$. The projection $M \to M_{\mathrm{tor}}$ associated to that hypothetical direct sum decomposition of $M$ is $A$-linear and fixes each element of $M_{\mathrm{tor}}$. We will show every $A$-linear map $f\colon M \to M_{\mathrm{tor}}$ must be zero on $M_{\mathrm{tor}}$, which is incompatible with $f$ fixing $M_{\mathrm{tor}}$ since $M_{\mathrm{tor}}$ is nonzero. Since $M_{\mathrm{tor}}$ is the $A$-multiples of $\overline{\binom{r}{x}}$, it suffices to show $f\overline{\binom{r}{x}} = \overline{\mathbf{0}}$. Write $f\overline{\binom{1}{0}} = a\overline{\binom{r}{x}}$ and $f\overline{\binom{0}{1}} = b\overline{\binom{r}{x}}$ for some $a$ and $b$ in $A$. Then

$$f\overline{\begin{pmatrix} r \\ x \end{pmatrix}} = f\left(r\overline{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} + x\overline{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}\right) = rf\overline{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} + xf\overline{\begin{pmatrix} 0 \\ 1 \end{pmatrix}} = ra\overline{\begin{pmatrix} r \\ x \end{pmatrix}} + xb\overline{\begin{pmatrix} r \\ x \end{pmatrix}} = \overline{\mathbf{0}}$$

since $\overline{\binom{r}{x}}$ is killed by both $r$ and $x$.

**Remark 4.10.** Example 4.9 works in the same way if we replace $\mathbf{Z}[x]$ by $R[x]$ where $R$ is an integral domain that is not a field and $r$ is a nonzero nonunit in $R$. What we used about $r$ and $x$ in the example is that $(r, x)$ is a proper ideal of $\mathbf{Z}[x]$, $x$ is prime in $\mathbf{Z}[x]$, and $x \nmid r$. It wasn't important that $r$ is an integer. (For instance, we could have used $r = x + 2$). Therefore we could replace $\mathbf{Z}[x]$ by an integral domain $A$ containing a proper ideal of the

form $(r, p)$ where $p$ is prime in $A$ and $p \nmid r$. Such a domain $A$ consisting of numbers rather than polynomials is $\mathbf{Z}[\sqrt{n}]$ where the integer $n$ is not a square and $n \equiv 1 \bmod 4$: the ideal $(1+\sqrt{n}, 2)$ in $\mathbf{Z}[\sqrt{n}]$ is proper (it has index 2), 2 is prime in $\mathbf{Z}[\sqrt{n}]$, and $2 \nmid (1+\sqrt{n})$.

There are some integral domains $A$ that are not a PID but every finitely generated $A$-module $M$ has $M_{\mathrm{tor}}$ as a direct summand. This is true if $A$ is a Dedekind domain, which is a type of generalization of a PID. When we write $M = M_{\mathrm{tor}} \oplus N$, the complementary module $N$ is torsion-free but need not be free (that is, it need not have an $A$-basis). For example, let $A = \mathbf{Z}[\sqrt{-6}]$ and $M = \mathbf{Z}[\sqrt{2}, \frac{1+\sqrt{-3}}{2}]$, so $A \subset M$ since $M$ contains $\sqrt{2}$ and $\sqrt{-3}$. Then $M_{\mathrm{tor}} = \{0\}$ and $M$ is finitely generated as an $A$-module (it is already finitely generated as a $\mathbf{Z}$-module, and $\mathbf{Z} \subset A$), but it can be shown that $M$ is not a free $A$-module. See Example 2.3 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/notfree.pdf.

## 5. Cardinality and Index over a PID

A finite abelian group is the same thing as a finitely generated torsion module over $\mathbf{Z}$, so finitely generated torsion modules over a PID are generalizations of finite abelian groups. Corollary 4.3 provides a method of defining a "size" for finitely generated torsion modules over a PID as an ideal that generalizes the size of a finite abelian group.

**Definition 5.1.** Let $T$ be a finitely generated torsion module over the PID $A$. Writing $T \cong A/(a_1) \oplus \cdots \oplus A/(a_m)$, define the *$A$-cardinality* of $T$ to be the ideal

$$\mathrm{card}_A(T) = (a_1 a_2 \cdots a_m).$$

The term $A$-cardinality is adapted from [2, pp. 35], where they use "$A$-cardinal".[4] When $A = \mathbf{Z}$, so $T$ is a finite abelian group, $\mathrm{card}_{\mathbf{Z}}(T)$ is the size (cardinality) of $T$.

A finitely generated torsion module can be written as a direct sum of cyclic modules in more than one way (including different numbers of cyclic components), *e.g.*,

$$\mathbf{Z}/(3) \times \mathbf{Z}/(4) \times \mathbf{Z}/(5) \times \mathbf{Z}/(5) \cong \mathbf{Z}/(5) \times \mathbf{Z}/(60) \times \cong \mathbf{Z}/(15) \times \mathbf{Z}/(20) \tag{5.1}$$

and

$$\mathbf{R}[X]/(X) \times \mathbf{R}[X]/(X) \times \mathbf{R}[X]/(X-1) \cong \mathbf{R}[X]/(X^2 - X) \times \mathbf{R}[X]/(X), \tag{5.2}$$

so we need to check $A$-cardinality is well-defined. First let's look at a few examples of $A$-cardinality, assuming that it is well-defined.

**Example 5.2.** If $G$ is a finite abelian group and $G \cong \mathbf{Z}/(a_1) \times \cdots \times \mathbf{Z}/(a_m)$, then $\mathrm{card}_{\mathbf{Z}}(G) = (a_1 \cdots a_m)\mathbf{Z}$, whose positive generator is $|a_1 \cdots a_m| = |G|$.

**Example 5.3.** If $T = \{0\}$ then each $(a_i)$ is $(1)$, so $\mathrm{card}_A(T) = (1) = A$. The converse holds too: if $\mathrm{card}_A(T) = (1)$ then $a_1 \cdots a_m$ is a unit, so each $(a_i)$ is $(1)$ and thus $T$ is trivial.

**Example 5.4.** When $A$ is a field, so $A$-modules are vector spaces, the only (finitely generated) torsion module over $A$ is $T = \{0\}$, and each ideal $(a_i)$ has to be $(1)$, so $\mathrm{card}_A(T) = (1)$.

**Example 5.5.** Let $V = \mathbf{R}^2$, viewed as an $\mathbf{R}[X]$-module with $X$ acting on $\mathbf{R}^2$ as the identity matrix. Then $V$ as an $\mathbf{R}[X]$-module is the direct sum of submodules $\mathbf{R}e_1 \oplus \mathbf{R}e_2 \cong \mathbf{R}[X]/(X-1) \oplus \mathbf{R}[X]/(X-1)$, so $\mathrm{card}_{\mathbf{R}[X]}(V) = (X-1)^2$ as an ideal in $\mathbf{R}[X]$.

[4] Aluffi [1, Remark 5.8] uses the term "characteristic ideal," which can be motivated by the result of Exercise 5.

**Example 5.6.** Let $V = \mathbf{R}^2$, viewed as an $\mathbf{R}[X]$-module with $X$ acting on $\mathbf{R}^2$ as $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then $X(e_1) = e_1$ and $X(e_2) = \binom{1}{1} = e_1 + e_2$, so $\{e_2, X(e_2)\}$ is a basis of $\mathbf{R}^2$. Since $X^2(e_2) = 2e_1 + e_2 = 2(e_1 + e_2) - e_2 = 2X(e_2) - e_2$, so $(X^2 - 2X + 1)(e_2) = 0$, as an $\mathbf{R}[X]$-module $V \cong \mathbf{R}[X]/(X^2 - 2X + 1) = \mathbf{R}[X]/(X-1)^2$. Therefore $\mathrm{card}_{\mathbf{R}[X]}(V) = (X-1)^2$, which is the same ideal as in the previous example. The difference between $\mathbf{R}[X]/(X-1) \oplus \mathbf{R}[X]/(X-1)$ and $\mathbf{R}[X]/(X-1)^2$ as $\mathbf{R}[X]$-modules is similar to that between $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ and $\mathbf{Z}/(4)$ as abelian groups, which are nonisomorphic but have the same size.

The ideal $\mathrm{card}_A(T)$ need not equal the annihilator ideal $\mathrm{Ann}_A(T) = \{a \in A : aT = 0\}$, which in terms of the cyclic decomposition of $T$ is $(\mathrm{lcm}(a_1, \ldots, a_m))$ (see Exercise 8). For example, the finite abelian groups in (5.1) have $\mathbf{Z}$-cardinality (300) and annihilator ideal (60), while the $\mathbf{R}[X]$-modules in (5.2) have $\mathbf{R}[X]$-cardinality $(X^3 - X^2)$ and annihilator ideal $(X^2 - X)$.

When $A = \mathbf{Z}$ and $G$ is a finite abelian group, $\mathrm{Ann}_{\mathbf{Z}}(G)$ is generated by the least positive integer whose power (or multiple, in additive notation) kills everything in the group and is traditionally called the exponent of $G$. The size and exponent of $G$ are equal exactly when $G$ is cyclic, and likewise $\mathrm{card}_A(T) = \mathrm{Ann}_A(T)$ exactly when $T$ is a cyclic $A$-module.

Now we show $\mathrm{card}_A(T)$ is well-defined. You may want to skip the proof on a first reading.

**Theorem 5.7.** *If $A/(a_1) \oplus \cdots \oplus A/(a_m) \cong A/(b_1) \oplus \cdots \oplus A/(b_n)$ as $A$-modules, where the $a_i$'s and $b_j$'s are nonzero, then $(a_1 a_2 \cdots a_m) = (b_1 b_2 \cdots b_n)$ as ideals.*

*Proof.* If $A$ is a field then the theorem is obvious since both ideals are (1), so we assume $A$ is not a field: it has irreducible elements. For every irreducible $\pi$ in $A$, we will show the highest power of $\pi$ in $a_1 a_2 \ldots a_m$ and $b_1 b_2 \cdots b_n$ are equal. Therefore by unique factorization (every PID is a UFD) $a_1 a_2 \ldots a_m$ and $b_1 b_2 \cdots b_n$ are equal up to multiplication by a unit, so $(a_1 a_2 \ldots a_m) = (b_1 b_2 \cdots b_n)$.

Set $T = A/(a_1) \oplus \cdots \oplus A/(a_m)$. For each irreducible $\pi$ in $A$ we look at the descending chain of modules

$$T \supset \pi T \supset \pi^2 T \supset \cdots \supset \pi^i T \supset \cdots$$

The quotient of successive modules $\pi^{i-1}T/\pi^i T$ is an $A$-module on which multiplication by $\pi$ is 0, so this is an $A/(\pi)$-vector space. Since $T$ is finitely generated, so is $\pi^{i-1}T$ (multiply the generators of $T$ by $\pi^{i-1}$) and thus so is its quotient $\pi^{i-1}T/\pi^i T$, so $\pi^{i-1}T/\pi^i T$ is a finite-dimensional $A/(\pi)$-vector space. The dimensions $\dim_{A/(\pi)}(\pi^{i-1}T/\pi^i T)$ will be the key. We will show the highest power of $\pi$ in $a_1 a_2 \ldots a_m$ is $\sum_{i \geq 1} \dim_{A/(\pi)}(\pi^{i-1}T/\pi^i T)$.

Step 1: $T = A/(a)$ is a cyclic torsion module.

For $i \geq 1$ we will show when $T = A/(a)$ that

$$\dim_{A/(\pi)}(\pi^{i-1}T/\pi^i T) = \begin{cases} 1, & \text{if } \pi^i \mid a, \\ 0, & \text{otherwise.} \end{cases}$$

Since $T$ is generated as an $A$-module by 1, $\pi^{i-1}T/\pi^i T$ is spanned as an $A/(\pi)$-vector space by $\pi^{i-1}$, so $\pi^{i-1}T/\pi^i T$ has dimension $\leq 1$ over $A/(\pi)$. It is 0-dimensional if and only if $\pi^{i-1}T = \pi^i T$, which is equivalent to $\pi^{i-1} \in \pi^i A + (a) = (\pi^i, a)$. If $\pi^i \mid a$ then $(\pi^i, a) \subset (\pi^i)$, and obviously $\pi^{i-1} \notin (\pi^i)$, so $\pi^{i-1}T/\pi^i T$ is 1-dimensional over $A/(\pi)$. If $\pi^i$ does not divide $a$ then the greatest common divisor of $\pi^i$ and $a$ is $\pi^j$ for some $j \leq i - 1$, and therefore $\pi^{i-1} \in (\pi^j) = (\pi^i, a)$. Thus

$$\sum_{i \geq 1} \dim_{A/(\pi)}(\pi^{i-1}T/\pi^i T) = |\{i \geq 1 : \pi^i \mid a\}|,$$

which is the highest power of $\pi$ dividing $a$. In particular, if $\pi \nmid a$ then the sum is 0.

Step 2: $T$ is a finitely generated torsion module.

Writing $T = A/(a_1) \oplus \cdots \oplus A/(a_m)$, we have an $A/(\pi)$-vector space isomorphism

$$\pi^{i-1}T/\pi^i T \cong \bigoplus_{k=1}^{m} \pi^{i-1}(A/(a_k))/\pi^i(A/(a_k)),$$

so

$$\dim_{A/(\pi)}(\pi^{i-1}T/\pi^i T) = \sum_{k=1}^{m} \dim_{A/(\pi)}(\pi^{i-1}(A/(a_k))/\pi^i(A/(a_k)))$$

so summing over all $i \geq 1$ gives us on the right the sum of the highest powers of $\pi$ in all $a_k$'s, which is the highest power of $\pi$ in $a_1 a_2 \cdots a_m$. In particular, if $\pi \nmid a_1 \cdots a_m$ then the sum is 0.

Step 3: Comparing isomorphic cyclic decompositions.

The number $\dim_{A/(\pi)}(\pi^{i-1}T/\pi^i T)$, which does not depend on a cyclic decomposition, is unchanged if $T$ is replaced by an isomorphic $A$-module because an $A$-module isomorphism $T \to T'$ induces an $A/(\pi)$-vector space isomorphism $\pi^{i-1}T/\pi^i T \to \pi^{i-1}T'/\pi^i T'$ in a natural way. Therefore $a_1 a_2 \dots a_m$ and $b_1 b_2 \cdots b_n$ are divisible by the same highest power of $\pi$, for all $\pi$. □

**Example 5.8.** We have $\mathrm{card}_A(T) = (1)$ if and only if each $a_i$ in a cyclic decomposition is a unit, which means $T = 0$.

**Example 5.9.** For $a \in A - \{0\}$, $\mathrm{card}_A(A/(a)) = (a)$. For nonzero $a$ and $b$, $\mathrm{card}_A(A/(ab)) = (ab) = (a)(b) = \mathrm{card}_A(A/(a))\,\mathrm{card}_A(A/(b))$.

**Example 5.10.** When $A = \mathbf{Z}$ and $G$ is any of the isomorphic groups in (5.1), which have $A$-cardinality $(300) = (2^2 \cdot 3 \cdot 5^2)$, let's recover the multiplicity of 5 in this by looking at $\dim_{\mathbf{Z}/5\mathbf{Z}}(5^{i-1}G/5^i G)$ for $i \geq 1$. We have

$$G \cong \mathbf{Z}/(3) \times \mathbf{Z}/(4) \times \mathbf{Z}/(5) \times \mathbf{Z}/(5) \cong \mathbf{Z}/(5) \times \mathbf{Z}/(60) \times \cong \mathbf{Z}/(15) \times \mathbf{Z}/(20)$$

and

$$5G \cong \mathbf{Z}/(3) \times \mathbf{Z}/(4) \times (0) \times (0) \cong (0) \times 5\mathbf{Z}/(60) \times \cong 5\mathbf{Z}/(15) \times 5\mathbf{Z}/(20)$$

and $5^i G = 5G$ for $i \geq 2$. Then $\dim_{\mathbf{Z}/5\mathbf{Z}}(G/5G) = 2$ and $\dim_{\mathbf{Z}/5\mathbf{Z}}(5^{i-1}G/5^i G) = 0$ for $i \geq 2$, so the sum of these dimensions is 2, which is the multiplicity of 5 in 300.

**Example 5.11.** When $A = \mathbf{R}[X]$ and $T$ is an $\mathbf{R}[X]$-module in (5.2), for which $\mathrm{card}_A(T) = (X^3 - X^2) = (X^2(X-1))$, the multiplicity of $X$ in $T$ is the sum of $\dim_{\mathbf{R}[X]/(X)}(X^{i-1}T/X^i T)$ for $i \geq 1$. We have

$$T \cong \mathbf{R}[X]/(X) \times \mathbf{R}[X]/(X) \times \mathbf{R}[X]/(X-1) \cong \mathbf{R}[X]/(X^2 - X) \times \mathbf{R}[X]/(X)$$

and

$$XT \cong (0) \times (0) \times \mathbf{R}[X]/(X-1) \cong X\mathbf{R}[X]/(X^2 - X) \times (0)$$

and $X^i T = XT$ for $i \geq 2$. Then $\dim_{\mathbf{R}[X]/(X)}(T/XT) = 2$ and $\dim_{\mathbf{R}[X]/(X)}(X^{i-1}T/X^i T) = 0$ for $i \geq 2$, so the sum of the dimensions is 2, which is the multiplicity of $X$ in $X^3 - X^2$.

**Corollary 5.12.** *If $T$ is a finitely generated torsion $A$-module then* $\mathrm{card}_A(T) \subset \mathrm{Ann}_A(T)$.

*Proof.* It is obvious from a cyclic decomposition $T \cong A/(a_1) \oplus \cdots \oplus A/(a_m)$ that multiplication by $a_1 a_2 \cdots a_m$ kills $T$, so $a_1 \cdots a_m \in \mathrm{Ann}_A(T)$, and therefore $\mathrm{card}_A(T) \subset \mathrm{Ann}_A(T)$. □

**Theorem 5.13.** *For two finitely generated torsion $A$-modules $T_1$ and $T_2$,* $\mathrm{card}_A(T_1 \oplus T_2) = \mathrm{card}_A(T_1)\,\mathrm{card}_A(T_2)$.

*Proof.* Combine cyclic decompositions of $T_1$ and $T_2$ to get one for $T_1 \oplus T_2$. □

Some properties of $\mathrm{card}_A(T)$ that generalize results about orders of finite abelian groups (*e.g.*, Cauchy's theorem) are in the exercises.

The notion of index, not just cardinality, also generalizes from abelian groups to finitely generated modules over a PID.

**Definition 5.14.** If $M$ is a finitely generated module over the PID $A$ with submodule $M'$ such that $M/M'$ is a torsion module, we set the $A$-*index* of $M'$ in $M$ to be the $A$-cardinality of their quotient:

$$[M : M']_A = \mathrm{card}_A(M/M').$$

**Example 5.15.** If $M' \subset M$ then $M' = M$ if and only if $[M : M']_A = (1)$, since $M/M' = 0$ if and only if $\mathrm{card}_A(M/M') = (1)$.

**Example 5.16.** For nonzero $a$ and $b$ in $A$, $[A^2 : aA \oplus bA]_A = (ab)$ since $A^2/(aA \oplus bA) \cong A/(a) \oplus A/(b)$.

**Example 5.17.** Let $A = \mathbf{Z}[i]$,

$$M = \mathbf{Z}[i]^2 = \mathbf{Z}[i]\begin{pmatrix}1\\0\end{pmatrix} + \mathbf{Z}[i]\begin{pmatrix}0\\1\end{pmatrix},$$

and

$$M' = \mathbf{Z}[i]\begin{pmatrix}3\\0\end{pmatrix} + \mathbf{Z}[i]\begin{pmatrix}0\\1+2i\end{pmatrix} = \mathbf{Z}[i]3\begin{pmatrix}1\\0\end{pmatrix} + \mathbf{Z}[i](1+2i)\begin{pmatrix}0\\1\end{pmatrix}.$$

Since $M/M' \cong \mathbf{Z}[i]/(3) \oplus \mathbf{Z}[i]/(1+2i)$, $[M : M']_{\mathbf{Z}[i]} = (3(1+2i))$.

Using different bases for these two modules,

$$M = \mathbf{Z}[i]\begin{pmatrix}3\\1+2i\end{pmatrix} + \mathbf{Z}[i]\begin{pmatrix}1-2i\\2\end{pmatrix}$$

and

$$M' = \mathbf{Z}[i]\begin{pmatrix}3\\1+2i\end{pmatrix} + \mathbf{Z}[i]3(1+2i)\begin{pmatrix}1-2i\\2\end{pmatrix},$$

so $M/M' \cong \mathbf{Z}[i]/(3(1+2i))$. Thus again we compute $[M : M']_{\mathbf{Z}[i]} = (3(1+2i))$.

If $M$ is a finite free $A$-module and $M'$ is a submodule, by Corollary 2.12 the $A$-index $[M : M']_A$ is defined if and only if $M$ and $M'$ have equal rank. This is also true in the general case (Exercise 6). When $A = \mathbf{Z}$, $[M : M']_{\mathbf{Z}}$ is the subgroup of $\mathbf{Z}$ generated by the positive integer $|M/M'|$, which is the usual index $[M : M']$, so the $A$-index generalizes the index in group theory.

**Theorem 5.18.** *Let $M$ be a finitely generated $A$-module with submodules $M' \supset M''$ and assume $M/M''$ is a torsion module. Then*

$$[M : M'']_A = [M : M']_A[M' : M'']_A.$$

*Proof.* In terms of $A$-cardinalities, this says

$$\mathrm{card}_A(M/M'') = \mathrm{card}_A(M/M')\,\mathrm{card}_A(M'/M'').$$

The ideal $\mathrm{card}_A(M/M'')$ is defined by hypothesis. Since $M'/M''$ is a submodule of $M/M''$ and $M/M'$ is a quotient module of $M/M''$, both are finitely generated torsion modules so $\mathrm{card}_A(M/M')$ and $\mathrm{card}_A(M'/M'')$ are both defined.

Setting $T = M/M''$ and $T' = M'/M''$, the identity we want to prove becomes

$$\mathrm{card}_A(T) = \mathrm{card}_A(T')\,\mathrm{card}_A(T/T'),$$

which is Exercise 7. □

A finite-free $\mathbf{Z}$-module $M$ looks like $\mathbf{Z}^n$, and a submodule $M'$ also of rank $n$ has finite index in $M$. We will prove a determinant formula for the index of $M'$ in $M$ and then generalize to the case of an arbitrary PID in place of $\mathbf{Z}$.

**Theorem 5.19.** *Let $M$ be a finite free $\mathbf{Z}$-module with rank $n$ and $M'$ be a submodule of $M$ with rank $n$. Let $x_1, \ldots, x_n$ be a basis of $M$ and $y_1, \ldots, y_n$ be a basis of $M'$. Writing $y_j = \sum_{i=1}^n c_{ij}x_i$ with $c_{ij} \in \mathbf{Z}$, the index $[M : M']$ equals $|\det(c_{ij})|$.*

*Proof.* Our proof will be an application of aligned bases in a finite free abelian group and finite-index subgroup: Theorem 2.10 with $A = \mathbf{Z}$.

The $n$-tuples $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ do not have the same $\mathbf{Z}$-span (unless $M' = M$), but morally they should have the same $\mathbf{Q}$-span. To make this idea precise, we transfer the data of $M$ and $M'$ into the vector space $\mathbf{Q}^n$. Let $e_1, \ldots, e_n$ be the standard basis of $\mathbf{Q}^n$ and set $f_j = \sum_{i=1}^n c_{ij}e_i$, using the same coefficients that express $y_1, \ldots, y_n$ in terms of $x_1, \ldots, x_n$. Identify $M$ with $\mathbf{Z}^n$ by $x_i \leftrightarrow e_i$ (extended by $\mathbf{Z}$-linearity). This isomorphism identifies $y_j$ with $f_j$ for all $j$, so $M'$ inside $M$ is identified with the $\mathbf{Z}$-span of $f_1, \ldots, f_n$ inside $\mathbf{Z}^n$.

A $\mathbf{Z}$-linear map $\mathbf{Z}^n \to \mathbf{Z}^n$ is determined by its effect on the standard basis $e_1, \ldots, e_n$ of $\mathbf{Z}^n$. Let $\varphi\colon \mathbf{Z}^n \to \mathbf{Z}^n$ be the $\mathbf{Z}$-linear map determined by $\varphi(e_1) = f_1, \ldots, \varphi(e_n) = f_n$. Then $\varphi(e_j) = \sum_{i=1}^n c_{ij}e_i$ for $j = 1, \ldots, n$, so $(c_{ij})$ is the matrix representation of $\varphi$ with respect to the standard basis $e_1, \ldots, e_n$ of $\mathbf{Z}^n$ and

$$\varphi(\mathbf{Z}^n) = \mathbf{Z}\varphi(e_1) \oplus \cdots \oplus \mathbf{Z}\varphi(e_n) = \mathbf{Z}f_1 \oplus \cdots \oplus \mathbf{Z}f_n,$$

so $[M : M'] = [\mathbf{Z}^n : \varphi(\mathbf{Z}^n)]$. We will show $[\mathbf{Z}^n : \varphi(\mathbf{Z}^n)] = |\det(\varphi)| = |\det(c_{ij})|$.

The bases $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ of $\mathbf{Z}^n$ are usually *not* aligned with each other. By Theorem 2.10, there is a set of aligned bases for $\mathbf{Z}^n$ and its submodule $\varphi(\mathbf{Z}^n)$:

$$\mathbf{Z}^n = \mathbf{Z}v_1 \oplus \cdots \oplus \mathbf{Z}v_n, \quad \varphi(\mathbf{Z}^n) = \mathbf{Z}a_1v_1 \oplus \cdots \oplus \mathbf{Z}a_nv_n,$$

where the $a_i$'s are nonzero integers. Then

$$\mathbf{Z}^n/\varphi(\mathbf{Z}^n) \cong \bigoplus_{i=1}^n \mathbf{Z}/a_i\mathbf{Z},$$

which tells us

$$[\mathbf{Z}^n : \varphi(\mathbf{Z}^n)] = |a_1a_2\cdots a_n|. \tag{5.3}$$

We want to prove $|\det(\varphi)| = |a_1a_2\cdots a_n|$ too.

A $\mathbf{Z}$-linearly independent set of size $n$ in $\mathbf{Q}^n$ is a $\mathbf{Q}$-basis of $\mathbf{Q}^n$, so all four sets $\{e_i\}$, $\{\varphi(e_i)\}$, $\{v_i\}$ and $\{a_iv_i\}$ are $\mathbf{Q}$-bases for $\mathbf{Q}^n$. For two $\mathbf{Q}$-bases of $\mathbf{Q}^n$ there is a unique $\mathbf{Q}$-linear map $\mathbf{Q}^n \to \mathbf{Q}^n$ taking one basis to the other. The $\mathbf{Q}$-linear map $\mathbf{Q}^n \to \mathbf{Q}^n$ taking $e_i$ to $\varphi(e_i)$ is the natural extension of $\varphi\colon \mathbf{Z}^n \to \mathbf{Z}^n$ from a $\mathbf{Z}$-linear map to a $\mathbf{Q}$-linear map,

so we will also call it $\varphi$ (its matrix representation with respect to the standard basis of $\mathbf{Q}^n$ is $(c_{ij})$, just like $\varphi$ as a $\mathbf{Z}$-linear map on $\mathbf{Z}^n$). Consider the diagram of $\mathbf{Q}$-linear maps

$$\begin{array}{ccc} \mathbf{Q}^n & \xrightarrow{\varphi} & \mathbf{Q}^n \\ {\scriptstyle\alpha}\downarrow & & \uparrow{\scriptstyle\gamma} \\ \mathbf{Q}^n & \xrightarrow[\beta]{} & \mathbf{Q}^n \end{array} \quad \text{where} \quad \begin{array}{ccc} e_i & \xmapsto{\varphi} & f_i \\ {\scriptstyle\alpha}\downarrow & & \uparrow{\scriptstyle\gamma} \\ v_i & \xmapsto[\beta]{} & a_i v_i \end{array}$$

This diagram commutes: $\varphi = \gamma \circ \beta \circ \alpha$. Taking determinants of these $\mathbf{Q}$-linear maps $\mathbf{Q}^n \to \mathbf{Q}^n$,[5]

$$\det(\varphi) = \det(\gamma)\det(\beta)\det(\alpha). \tag{5.4}$$

Using the $\mathbf{Q}$-basis $\{v_i\}$ of $\mathbf{Q}^n$, the matrix representation $[\beta]$ is diagonal with $a_i$'s along its main diagonal, so

$$\det(\beta\colon \mathbf{Q}^n \to \mathbf{Q}^n) = a_1 a_2 \cdots a_n.$$

What is $\det(\alpha)$? The map $\alpha$ identifies two $\mathbf{Z}$-bases of the *same* $\mathbf{Z}$-module $\mathbf{Z}^n$:

$$\alpha(c_1 e_1 + \cdots + c_n e_n) = c_1 v_1 + \cdots + c_n v_n, \quad c_i \in \mathbf{Z}.$$

Therefore $\alpha$ is invertible as a $\mathbf{Z}$-linear map of $\mathbf{Z}^n$ to itself. Using $\{e_i\}$ as the basis in which a matrix for $\alpha$ is computed, the matrices of $\alpha\colon \mathbf{Q}^n \to \mathbf{Q}^n$ over $\mathbf{Q}$ and $\alpha\colon \mathbf{Z}^n \to \mathbf{Z}^n$ over $\mathbf{Z}$ are the same. Since an invertible $\mathbf{Z}$-linear map $\mathbf{Z}^n \to \mathbf{Z}^n$ has determinant $\pm 1$,

$$\det(\alpha\colon \mathbf{Q}^n \to \mathbf{Q}^n) = \det(\alpha\colon \mathbf{Z}^n \to \mathbf{Z}^n) = \pm 1.$$

A similar argument shows

$$\det(\gamma\colon \mathbf{Q}^n \to \mathbf{Q}^n) = \det(\gamma\colon \varphi(\mathbf{Z}^n) \to \varphi(\mathbf{Z}^n)) = \pm 1$$

since $\gamma$ identifies two $\mathbf{Z}$-bases of $\varphi(\mathbf{Z}^n)$. Feeding these determinant formulas into the right side of (5.4),

$$\det(\varphi) = \pm a_1 a_2 \cdots a_n. \tag{5.5}$$

Comparing (5.3) and (5.5), $|\det(\varphi)| = |a_1 a_2 \cdots a_n| = [\mathbf{Z}^n : \varphi(\mathbf{Z}^n)] = [M : M']$. □

**Example 5.20.** Let $M = \mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i$ and $M' = (1+2i)\mathbf{Z}[i] = \mathbf{Z}(1+2i) + \mathbf{Z}(-2+i)$. We met this in Example 2.9, where where we saw $\mathbf{Z}[i]$ and $(1+2i)$ have aligned bases $\{1+2i, i\}$ and $\{1+2i, 5i\}$, and these aligned bases $\{v_1, v_2\}$ and $\{v_1, 5v_2\}$ show $[M : M'] = 5$. We will compute this index a second way using a determinant for a matrix expressing a $\mathbf{Z}$-basis of $M'$ in terms of a $\mathbf{Z}$-basis of $M$ without requiring the bases to be aligned.

From Example 2.9, a $\mathbf{Z}$-basis for $\mathbf{Z}[i]$ is $\{1, i\}$ and a $\mathbf{Z}$-basis for $(1+2i)$ is $\{1+2i, -2+i\}$. Under the isomorphism $\mathbf{Z}[i] \to \mathbf{Z}^2$ as abelian groups ($\mathbf{Z}$-modules) by $a+bi \mapsto \binom{a}{b}$, the ideal $(1+2i)$ is identified with $\mathbf{Z}\binom{1}{2} + \mathbf{Z}\binom{-2}{1} = \left(\begin{smallmatrix} 1 & -2 \\ 2 & 1 \end{smallmatrix}\right)(\mathbf{Z}^2)$, so Theorem 5.19 tells us $[M : M']$ equals $\left|\det\left(\begin{smallmatrix} 1 & -2 \\ 2 & 1 \end{smallmatrix}\right)\right| = |5| = 5$.

**Example 5.21.** In the ring $\mathbf{Z}[\sqrt{10}]$ let $\mathfrak{a}$ be the ideal $(2+5\sqrt{10}, 4+7\sqrt{10})$. We will compute the index of $\mathfrak{a}$ in $\mathbf{Z}[\sqrt{10}]$ as abelian groups using (unaligned) $\mathbf{Z}$-bases for $\mathbf{Z}[\sqrt{10}]$ and $\mathfrak{a}$.

[5]We are using $\mathbf{Q}$-linear maps throughout because it is nonsense to talk about the determinant of a $\mathbf{Z}$-linear map $\mathbf{Z}^n \to \varphi(\mathbf{Z}^n)$ when $\varphi(\mathbf{Z}^n) \neq \mathbf{Z}^n$: the different bases don't all have the same $\mathbf{Z}$-span but they do all have the same $\mathbf{Q}$-span.

A $\mathbf{Z}$-basis for $\mathbf{Z}[\sqrt{10}]$ is $\{1, \sqrt{10}\}$. A $\mathbf{Z}$-basis for $\mathfrak{a}$ is $\{2+5\sqrt{10}, 4+7\sqrt{10}\}$, but this requires verification because it is a stronger condition to generate $\mathfrak{a}$ as a $\mathbf{Z}$-module than to generate it as an ideal[6]: the initial definition of $\mathfrak{a}$ tells us that

$$\begin{aligned}\mathfrak{a} &= \mathbf{Z}[\sqrt{10}](2+5\sqrt{10}) + \mathbf{Z}[\sqrt{10}](4+7\sqrt{10}) \\ &= (\mathbf{Z}+\mathbf{Z}\sqrt{10})(2+5\sqrt{10}) + (\mathbf{Z}+\mathbf{Z}\sqrt{10})(4+7\sqrt{10}) \\ &= \mathbf{Z}(2+5\sqrt{10}) + \mathbf{Z}(50+2\sqrt{10}) + \mathbf{Z}(4+7\sqrt{10}) + \mathbf{Z}(70+4\sqrt{10}).\end{aligned}$$

For $\mathfrak{a}$ to be spanned over $\mathbf{Z}$ by $2+5\sqrt{10}$ and $4+7\sqrt{10}$, we need to write the other two $\mathbf{Z}$-module generators in terms of them. After some linear algebra, we can do this:

$$\begin{aligned}50+2\sqrt{10} &= -57(2+5\sqrt{10}) + 41(4+7\sqrt{10}), \\ 70+4\sqrt{10} &= -79(2+5\sqrt{10}) + 57(4+7\sqrt{10}).\end{aligned}$$

Therefore $\mathfrak{a} = \mathbf{Z}(2+5\sqrt{10}) + \mathbf{Z}(4+7\sqrt{10})$ and the numbers $2+5\sqrt{10}$ and $4+7\sqrt{10}$ are obviously $\mathbf{Z}$-linearly independent, so they are a $\mathbf{Z}$-basis of $\mathfrak{a}$. The isomorphism $\mathbf{Z}[\sqrt{10}] \to \mathbf{Z}^2$ where $a+b\sqrt{10} \mapsto \binom{a}{b}$ identifies the ideal $\mathfrak{a}$ with $\mathbf{Z}\binom{2}{5} + \mathbf{Z}\binom{4}{7} = \left(\begin{smallmatrix} 2 & 4 \\ 5 & 7 \end{smallmatrix}\right)(\mathbf{Z}^2)$, so Theorem 5.19 tells us that the index of $\mathfrak{a}$ in $\mathbf{Z}[\sqrt{10}]$ is $|\det\left(\begin{smallmatrix} 2 & 4 \\ 5 & 7 \end{smallmatrix}\right)| = |-6| = 6$. The absolute value is important: the index is not $-6$.

**Theorem 5.22.** *Let $M$ be a finite free module over the* PID *$A$ with rank $n$ and $M'$ be a submodule with rank $n$. Let $x_1, \ldots, x_n$ be a basis of $M$ and $y_1, \ldots, y_n$ be a basis of $M'$. Writing $y_j = \sum_{i=1}^n c_{ij}x_i$ with $c_{ij} \in A$, $(\det(c_{ij})) = [M : M']_A$. In particular, $\det(c_{ij}) \neq 0$.*

*Proof.* Let $K$ be the fraction field of $A$. If we run through the proof of Theorem 5.19 with $A$ in place of $\mathbf{Z}$, $K$ in place of $\mathbf{Q}$, and use aligned bases $v_1, \ldots, v_n$ and $a_1v_1, \ldots, a_nv_n$ for $M$ and $M'$, with all $a_i$ nonzero in $A$, so $M/M' \cong \bigoplus_{i=1}^n A/(a_i)$, then the proof of Theorem 5.19 shows $\det(c_{ij}) = \det\varphi = ua_1 \cdots a_n$, where $u = \det\alpha \det\gamma$ is a unit in $A$. The $K$-linear operators $\alpha$ and $\gamma$ on $K^n$ have unit determinant since they are also $A$-linear operators on $A^n$ and $\varphi(A^n)$ sending a basis to a basis.

By the definition of $A$-index, $[M : M']_A = \mathrm{card}_A(M/M') = (a_1a_2 \cdots a_n)$. □

**Corollary 5.23.** *Let $M$ be a finite free $A$-module with rank $n$ and basis $x_1, \ldots, x_n$. For $y_1, \ldots, y_n$ in $M$, write $y_j = \sum_{i=1}^n c_{ij}x_i$ with $c_{ij} \in A$. Then $y_1, \ldots, y_n$ is linearly independent if and only if $\det(c_{ij}) \neq 0$.*

*Proof.* If $y_1, \ldots, y_n$ is a linearly independent set, then its $A$-span in $M$ is a free $A$-submodule of rank $n$, so $\det(c_{ij}) \neq 0$ by Theorem 5.22.

Conversely, if $\det(c_{ij}) \neq 0$, then we want to show an $A$-linear relation $\sum_{j=1}^n c_jy_j = 0$ with $c_j \in A$ must have all $c_j$ equal to 0. Writing $y_j$ in terms of the $x_i$'s,

$$0 = \sum_{j=1}^n c_jy_j = \sum_{j=1}^n c_j\left(\sum_{i=1}^n c_{ij}x_i\right) = \sum_{i=1}^n \left(\sum_{j=1}^n c_{ij}c_i\right)x_i,$$

[6]For example, in $\mathbf{Z}[i]$, $(17, 3+5i) \neq \mathbf{Z}17 + \mathbf{Z}(3+5i)$ since the ideal contains $4+i = 17i - (3+5i)(2+2i)$ but $4+i \neq 17a + (3+5i)b$ for integers $a$ and $b$: look at the imaginary parts.

so looking at the coefficients of $x_1, \ldots, x_n$ tells us $\sum_{j=1}^n c_{ij}c_i = 0$ for all $i$. As a matrix equation this says

$$\begin{pmatrix} c_{11} & c_{21} & \cdots & c_{n1} \\ c_{12} & c_{22} & \cdots & c_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1n} & c_{2n} & \cdots & c_{nn} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This is an equation in $A^n \subset K^n$, where $K$ is the fraction field of $A$. The matrix is the transpose of $(c_{ij})$. Since $\det((c_{ji})^\top) = \det(c_{ij}) \neq 0$ the vector vanishes, so all $c_i$ are 0. □

**Corollary 5.24.** *If $M$ is a finite free module over the* PID *$A$ with basis $x_1, \ldots, x_n$, a set of $n$ elements $y_1, \ldots, y_n$ in $M$ is a basis of $M$ if and only if the matrix $(c_{ij})$ expressing the $y$'s in terms of the $x$'s has unit determinant.*

*Proof.* If $y_1, \ldots, y_n$ is a basis of $M$ then $(\det(c_{ij})) = [M : M]_A = (1)$ by Theorem 5.22, so $\det(c_{ij}) \in A^\times$. Conversely, if $\det(c_{ij}) \in A^\times$ then $y_1, \ldots, y_n$ is linearly independent by Corollary 5.23 and the $A$-index of $\sum Ay_j$ in $M$ is $(\det(c_{ij})) = (1)$, so $\sum Ay_j = M$. □

**Example 5.25.** A set of $n$ vectors $v_1, \ldots, v_n$ in $\mathbf{Z}^n$ is a basis of $\mathbf{Z}^n$ if and only if the matrix $(v_1\ v_2\ \cdots\ v_n)$ with the $v$'s as the columns has determinant $\pm 1$, since this matrix expresses $v_1, \ldots, v_n$ in terms of the standard basis of $\mathbf{Z}^n$.

The definition of the ideal $\mathrm{card}_A(T)$ for a torsion module $T$ was based on a decomposition of $T$ as a direct sum of cyclic $A$-modules. To prove $\mathrm{card}_A(T)$ is well-defined (*i.e.*, it is independent of the choice of cyclic decomposition of $T$), the proof in Theorem 5.7 gave a formula for the multiplicity of each prime $\pi$ in $\mathrm{card}_A(T)$ that makes no reference to a cyclic decomposition of $T$: that multiplicity is

$$\sum_{i \geq 1} \dim_{A/(\pi)}(\pi^{i-1}T/\pi^i T),$$

where each quotient module $\pi^{i-1}T/\pi^i T$ is a vector space over the field $A/(\pi)$, and the sum is finite since the $i$th term is 0 for large enough $i$ (depending on $T$). This suggests the following weaker notion of size for finitely generated torsion modules.

**Definition 5.26.** For a finitely generated torsion module $T$ over the PID $A$, set the *primary cardinality* of $T$ to be

$$\omega_A(T) = \sum_{(\pi)} \dim_{A/(\pi)}(T/\pi T) \in \{0, 1, 2, 3, \ldots\}$$

where the sum runs over all nonzero prime ideals $(\pi)$ of $A$.

**Example 5.27.** Let $A = \mathbf{Z}$ and $T = \mathbf{Z}/100\mathbf{Z} \cong \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/25\mathbf{Z}$. If $p$ is 2 or 5 then $T/pT = (\mathbf{Z}/100\mathbf{Z})/(p\mathbf{Z}/100\mathbf{Z}) \cong \mathbf{Z}/p\mathbf{Z}$, so $\dim_{\mathbf{Z}/(p)}(T/pT) = 1$. If $p$ is a prime other than 2 or 5 then $pT = T$ ($p$ is invertible modulo 100), so $T/pT = 0$ and $\dim_{\mathbf{Z}/(p)}(T/pT) = 0$. Thus

$$\omega_{\mathbf{Z}}(\mathbf{Z}/100\mathbf{Z}) = \sum_{\text{prime } p} \dim_{\mathbf{Z}/(p)}(T/pT) = \dim_{\mathbf{Z}/(2)}(T/2T) + \dim_{\mathbf{Z}/(5)}(T/5T) = 1 + 1 = 2.$$

For general $n$, $\omega_{\mathbf{Z}}(\mathbf{Z}/n\mathbf{Z})$ is the number of prime factors of $n$, which explains the name "primary cardinality" for $\omega_A(T)$. (In number theory, $\omega(n)$ is the standard notation for the number of prime factors of $n$.) The multiplicity of the prime factors of $n$ does not play

a role in $\omega_{\mathbf{Z}}(\mathbf{Z}/n\mathbf{Z})$. For example, if we run through the same calculation for $\mathbf{Z}/10\mathbf{Z}$ and $10\mathbf{Z}/100\mathbf{Z}$ (both cyclic of order 10) then $\omega_{\mathbf{Z}}(\mathbf{Z}/10\mathbf{Z}) = 2$ and $\omega_{\mathbf{Z}}(10\mathbf{Z}/100\mathbf{Z}) = 2$. So unlike the ordinary notion of size, a finite abelian group and a proper subgroup (like $\mathbf{Z}/100\mathbf{Z}$ and its subgroup $10\mathbf{Z}/100\mathbf{Z}$) could have the same primary cardinality.

In the sum defining $\omega_A(T)$, each term $\dim_{A/(\pi)}(T/\pi T)$ is finite since $T$ being finitely generated as an $A$-module makes $T/\pi T$ finitely generated as an $A/(\pi)$-vector space. The following lemma explains why the sum defining $\omega_A(T)$ has only finitely many nonzero terms.

**Theorem 5.28.** *Let $T$ be a finitely generated torsion $A$-module. The ideal $\mathrm{Ann}_A(T) = \{a \in A : aT = 0\}$ is not $(0)$ and $\dim_{A/(\pi)}(T/\pi T) > 0$ if and only if $\pi \mid \mathrm{Ann}_A(T)$, which occurs for only finitely many prime ideals $(\pi)$.*

In the paragraph following Example 5.6, we saw $\mathrm{Ann}_A(T) \neq (0)$ by a formula for this ideal in terms of a cyclic decomposition of $T$ . The point of reproving $\mathrm{Ann}_A(T) \neq (0)$ again is to see it can be done without relying on a cyclic decomposition.

*Proof.* To show $\mathrm{Ann}_A(T) \neq (0)$ we will use a finite spanning set of $T$ as an $A$-module, say $\{t_1, \ldots, t_k\}$. Since each element of $T$ is an $A$-linear combination of $t_1, \ldots, t_k$, for $a \in A$ we have $aT = \{0\}$ if and only if $at_1 = 0, \ldots, at_k = 0$. Since $T$ is a torsion module, each of $t_1, \ldots, t_k$ is killed by some nonzero element of $A$, and the product of such elements is a single nonzero element of $A$ killing all of $t_1, \ldots, t_k$ and thus killing all of $T$. Thus $\mathrm{Ann}_A(T) \neq (0)$.

The ideal $\mathrm{Ann}_A(T)$ is principal, so it has a generator that is not 0, say $\mathrm{Ann}_A(T) = (\alpha)$. We will show $\dim_{A/(\pi)}(T/\pi T) > 0$ if and only if $\pi \mid \alpha$, or equivalently $\dim_{A/(\pi)}(T/\pi T) = 0$ if and only if $\pi \nmid \alpha$.

If $\pi \nmid \alpha$ then $(\alpha, \pi) = (1)$ since $\pi$ is prime, so $\alpha x + \pi y = 1$ for some $x$ and $y$ in $A$. Thus for each $t \in T$, $t = (\alpha x + \pi y)t = x(\alpha t) + \pi(yt) = \pi(yt)$ since $\alpha t = 0$. This shows $T \subset \pi T$, and the reverse containment is obvious, so $\pi T = T$ and thus $T/\pi T = 0$.

If $\pi \mid \alpha$, write $\alpha = \pi\alpha'$. Then $\alpha' \notin (\alpha)$ (since $\alpha \nmid \alpha'$), so $\alpha' T \neq \{0\}$: for some $t \in T$ we have $\alpha' t \neq 0$. We can't have $t \in \pi T$ since then $\alpha' t \in \alpha' \pi T = \alpha T = \{0\}$, which isn't true. So $T/\pi T \neq \{0\}$.

We have $\dim_{A/(\pi)}(T/\pi T) > 0$ if and only if $T/\pi T \neq 0$, and we showed that is the same as $\pi \mid \alpha$. A nonzero element of $A$ has only finitely many prime factors *up to unit multiple*, so $\pi \mid \alpha$ for only finitely many prime ideals $(\pi)$. □

**Corollary 5.29.** *We have $\omega_A(T) = 0$ if and only if $T = 0$.*

*Proof.* Obviously if $T = 0$ then $\omega_A(T) = 0$. Conversely, if $\omega_A(T) = 0$ then for all prime elements $\pi$ we have $\dim_{A/(\pi)}(T/\pi T) = 0$, so $T = \pi T$. By Theorem 5.28, the ideal $\mathrm{Ann}_A(T)$ has no prime factors, so $\mathrm{Ann}_A(T) = (1)$. That $1 \in \mathrm{Ann}_A(T)$ implies $1 \cdot T = 0$, so $T = 0$. □

**Theorem 5.30.** *For finitely generated torsion $A$-modules $T_1$ and $T_2$, $\omega_A(T_1 \oplus T_2) = \omega_A(T_1) + \omega_A(T_2)$.*

*Proof.* For each prime $\pi$, $\pi(T_1 \oplus T_2) = \pi T_1 \oplus \pi T_2$, so $(T_1 \oplus T_2)/\pi(T_1 \oplus T_2) \cong (T_1/\pi T_1) \oplus (T_2/\pi T_2)$. Isomorphic vector spaces have the same dimension, so

$$\begin{aligned} \dim_{A/(\pi)}(T_1 \oplus T_2)/\pi(T_1 \oplus T_2) &= \dim_{A/(\pi)}((T_1/\pi T_1) \oplus (T_2/\pi T_2)) \\ &= \dim_{A/(\pi)}(T_1/\pi T_1) + \dim_{A/(\pi)}(T_2/\pi T_2), \end{aligned}$$

and summing over all $(\pi)$ gives us $\omega_A(T_1 \oplus T_2) = \omega_A(T_1) + \omega_A(T_2)$. □

**Example 5.31.** For $a \in A - \{0\}$, $A/(a)$ is isomorphic to a direct sum of cyclic modules of the form $A/(\pi^k)$ for prime $\pi$ by the Chinese remainder theorem:

$$a = u\pi_1^{k_1} \cdots \pi_r^{k_r} \Longrightarrow A/(a) \cong A/(\pi_1^{k_1}) \oplus \cdots \oplus A/(\pi_r^{k_r}),$$

where $u \in A^\times$ and $\pi_1, \ldots, \pi_r$ are nonassociate primes in $A$. So each nonzero finitely generated torsion $A$-module $T$ is isomorphic to a direct sum of cyclic torsion $A$-modules:

$$T \cong A/(\pi_1^{e_1}) \oplus \cdots \oplus A/(\pi_n^{e_n}),$$

where $\pi_1, \ldots, \pi_n$ are prime and $e_1, \ldots, e_n$ are positive integers. (The primes could be the same when $T$ is not cyclic, *e.g.*, $(\mathbf{Z}/15\mathbf{Z})^\times = \langle 2 \bmod 15\rangle \oplus \langle -1 \bmod 15\rangle \cong \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.)

By Theorem 5.30, $\omega_A(T) = \sum_{j=1}^n \omega_A(A/(\pi_j^{e_j}))$. We have $\omega_A(A/(\pi_j^{e_j})) = 1$, so $\omega_A(T) = n$. Thus we have a concrete interpretation for $\omega_A(T)$: it is the number of terms in a decomposition of $T$ as a direct sum of cyclic modules having a prime-power annihilator ideal ($\mathrm{Ann}_A(A/(\pi^e)) = (\pi^e)$ when $\pi$ is prime). For instance, if a finite abelian group $G$ is expressed as a direct sum of cyclic abelian groups of prime-power order then $\omega_{\mathbf{Z}}(G)$ is the number of direct summands, *e.g.*, $\omega_{\mathbf{Z}}((\mathbf{Z}/15\mathbf{Z})^\times)) = \omega_{\mathbf{Z}}((\mathbf{Z}/4\mathbf{Z}) \oplus \mathbf{Z}/2\mathbf{Z}) = 2$.

**Exercises**.

1. Let $A$ be a commutative ring. If every submodule of every finite free $A$-module is a free $A$-module, show $A$ is a PID.
2. Suppose $A$ is a PID and $\pi$ is irreducible in $A$. Inside $A^2$, set
$$M = A\begin{pmatrix}1\\0\end{pmatrix} + A\begin{pmatrix}0\\\pi^2\end{pmatrix} = \left\{\begin{pmatrix}x\\y\end{pmatrix} : y \equiv 0 \bmod \pi^2\right\}$$
and
$$N = A\begin{pmatrix}\pi\\0\end{pmatrix} + A\begin{pmatrix}1\\\pi\end{pmatrix} = \left\{\begin{pmatrix}x\\y\end{pmatrix} : y \equiv 0 \bmod \pi, \pi x \equiv y \bmod \pi^2\right\}.$$
   a) Find a basis $\{e_1, e_2\}$ of $A^2$ and $a_1$ and $a_2$ in $A$ such that $\{a_1e_1, a_2e_2\}$ is a basis of $N$. (Such an aligned pair of bases obviously exists for $A^2$ and $M$.)
   b) Show there is no basis $\{e_1, e_2\}$ of $A^2$ and $a_1, a_2, b_1, b_2$ in $A$ such that $\{a_1e_1, a_2e_2\}$ is a basis of $M$ and $\{b_1e_1, b_2e_2\}$ is a basis of $N$. That is, the submodules $M$ and $N$ of $A^2$ do not admit bases simultaneously aligned with a single basis of $A^2$.
3. If $M$ is a finitely generated module over a PID $A$ and $M'$ is a submodule, is it always possible to align their decompositions into free parts and torsion parts: can we write $M = F \oplus T$ and $M' = F' \oplus T'$ such that $F$ and $F'$ are free, $T$ and $T'$ are torsion, and $F' \subset F$ and $T' \subset T$? If $A$ is not a field, show the answer is no by picking an irreducible $\pi$ in $A$ and using $M = A \oplus A/(\pi)$ and $M' = A(\pi, \overline{1})$. (Hint: first show $M'$ is free.)
4. Let $A$ be a PID.
   a) Prove an analogue of Cauchy's theorem from group theory: for a finitely generated torsion $A$-module $T$ and irreducible $\pi$ in $A$ such that $\pi$ divides $\mathrm{card}_A(T)$, meaning $\pi$ divides a generator of the ideal $\mathrm{card}_A(T)$, show there is some $t \in T$ with "order" $\pi$: the annihilator ideal $\mathrm{Ann}_A(t) = \{a \in A : at = 0\}$ is $\pi A$.
   b) Let $T$ and $T'$ be finitely generated torsion $A$-modules such that $\mathrm{card}_A(T) = \mathrm{card}_A(T')$. If $f\colon T \to T'$ is an $A$-linear map, show $f$ is one-to-one if and only if it is onto. (When $A = \mathbf{Z}$ this is the familiar statement that a homomorphism between finite abelian groups of equal size is one-to-one if and only if it is onto.)

c) Show a finitely generated $A$-module $M$ is a torsion module if and only if there is some $a \neq 0$ in $A$ such that $aM = 0$. (This is false without a hypothesis of finite generatedness, *e.g.*, $\mathbf{Q}/\mathbf{Z}$ is a torsion abelian group and for all nonzero integers $a$ we have $a(\mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}$.)

d) For a finitely generated $A$-module $M$ and submodule $N$, show $M/N$ is a torsion module if and only if there is some $a \neq 0$ in $A$ such that $aM \subset N$.

5. Let $V$ be a finite-dimensional vector space over a field $K$ and $f\colon V \to V$ be an $K$-linear operator. Write $V_f$ for $V$ as a $K[X]$-module where $X$ acts on $V$ as $f$: $Xv = f(v)$ for $v \in V$.

   a) Show $\mathrm{card}_{K[X]}(V_f) = (\chi_f(X))$, where $\chi_f$ is the characteristic polynomial of $f$.

   b) If $\chi_f(X)$ decomposes into linear factors in $K[X]$, so all the eigenvalues of $f$ are in $K$ and we can find a matrix for $f$ in Jordan canonical form, show $\omega_{K[X]}(V_f)$ is the number of Jordan blocks in that matrix.
6. For a pair of finitely generated $A$-modules $M \supset M'$, show $M/M'$ is a torsion module if and only if $M$ and $M'$ have the same rank (that means the free parts of $M$ and $M'$ have equal rank). This generalizes Corollary 2.12 in the case of free modules.
7. Let $T$ be a finitely generated torsion module over the PID $A$ and $T'$ be a submodule. Show $\mathrm{card}_A(T) = \mathrm{card}_A(T')\,\mathrm{card}_A(T/T')$. In particular, if $\mathrm{card}_A(T') = \mathrm{card}_A(T)$ then $\mathrm{card}_A(T/T') = (1)$, so $T/T' = \{0\}$ (Example 5.3) and thus $T' = T$, so if $T'$ is strictly contained in $T$ then $\mathrm{card}_A(T) \subsetneq \mathrm{card}_A(T')$.
8. Let $T$ be a finitely generated torsion module over the PID $A$. Write a cyclic decomposition of $T$ as $A/(a_1) \oplus \cdots A/(a_m)$ for nonzero $a_i$ in $A$.

   a) Show $\mathrm{Ann}_A(T) = (\mathrm{lcm}(a_1, \ldots, a_m))$.

   b) For $t$ and $t'$ in $T$, let $\mathrm{Ann}_A(t) = (a)$ and $\mathrm{Ann}_A(t') = (a')$. Show there is an $A$-linear combination of $t$ and $t'$ whose annihilator ideal is $(\mathrm{lcm}(a, a'))$. (Hint: when $A = \mathbf{Z}$, this becomes the fact from group theory that in a finite abelian group, if $g$ has order $m$ and $h$ has order $n$, then some element of $\langle g, h\rangle$ has order $\mathrm{lcm}(m, n)$.)

   c) Use (a) and (b) to show there is some $t_0 \in T$ such that $\mathrm{Ann}_A(t_0) = \mathrm{Ann}_A(T)$. (Hint: when $A = \mathbf{Z}$, this becomes the statement that in a finite abelian group, the least common multiple of the orders of its elements is the order of some element in the group.)
9. Prove Corollaries 5.23 and 5.24 when $A$ is an arbitrary integral domain, not necessarily a PID.

## References


[1] P. Aluffi, *Algebra: Chaper* 0, Amer. Math. Soc., Providence, 2009.

[2] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields," pp. 33–62 in *Number theory, Noordwijkerhout 1983*, Springer Lecture Notes in Mathematics 1068, Springer-Verlag, Berlin, 1984.

[3] S. Roman, *Advanced Linear Algebra*, 2nd ed., Springer-Verlag, New York, 2005.

[4] J. Rotman, *An Introduction to the Theory of Groups*,4th ed., Springer-Verlag, NY, 1995.

[5] J. Rotman, *Advanced Modern Algebra*, Prentice-Hall, Upper Saddle River, NJ, 2002.

[6] P. Samuel, *Algebraic Theory of Numbers*, Dover, 2008.