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 $n \geqslant 0$. 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 $n \geqslant 0$.
(3) Every finitely generated A-module M is isomorphic to $A^d \oplus T$, where $d \geqslant 0$ 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 three 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. *Let A be a commutative ring and M be an A-module. Every surjective linear map onto a finite free module looks like projection out of a direct sum decomposition. That is, if $f\colon M \twoheadrightarrow A^n$ is A-linear and onto, then there is an A-module isomorphism $h\colon M \cong A^n \oplus \ker f$ where $h(m) = (f(m), *)$, making f the first component of h.*

Proof. Let $A^n = Ae_1 \oplus \cdots \oplus Ae_n$ and pick $m_i \in M$ such that $f(m_i) = e_i$. Let $g\colon A^n \to M$ by

$$g(c_1e_1 + \cdots + c_ne_n) = c_1m_1 + \cdots + c_nm_n$$

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

(i.e., g is A-linear and $g(e_i) = m_i$). So $f(g(v)) = v$ for all $v \in A^n$ (just check at $v = e_i$ and use linearity). Define the function $h\colon M \to A^n \oplus \ker f$ by $h(m) = (f(m), m - g(f(m)))$. Check that h is an isomorphism as Exercise 2. ∎

A linear surjection $f\colon M \twoheadrightarrow N$ of A-modules induces an isomorphism $M/\ker f \cong N$ but there is usually *not* a direct sum decomposition $M \cong N \oplus \ker f$. That is, we can't usually split off $\ker f$ as a direct summand of M. For example, the surjection $f\colon \mathbf{Z} \twoheadrightarrow \mathbf{Z}/6\mathbf{Z}$ doesn't come from an isomorphism $\mathbf{Z} \cong (\mathbf{Z}/6\mathbf{Z}) \oplus \ker f$. Lemma 1.2 says there is such a splitting when $N = A^n$. This is a useful property of finite free modules.

Lemma 1.3. *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 $d \geqslant 1$ 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 $e_1, \ldots, e_n$ 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, $k \leqslant n$.

From the bound $k \leqslant n$, 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 $M \subset A^{n+1} = A \oplus A^n$

and let $\pi\colon A \oplus A^n \twoheadrightarrow A^n$ be projection to the second component of this direct sum. Let's look at the image and kernel of $\pi|_M$, the restriction of π 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 $k \leqslant n$. 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 $\ker(\pi|_M) = M \cap (A \oplus 0)$, with $A \oplus 0 \cong A$ 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 $x = a_0x_0 + a_1x_1 + \cdots + a_kx_k \in \sum_{i=1}^k Ax_i$, so $M \subset \sum_{i=1}^k Ax_i$. ∎

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 the previous proof.

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. We can suppose the free A-module of rank n is A^n itself and 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 $A^{n+1} = A \oplus A^n$ and let $\pi\colon A \oplus A^n \twoheadrightarrow A^n$ be projection to the second component. Since $\pi(M)$ is a submodule of A^n, $\pi(M)$ is free of rank $\leqslant n$ by the inductive hypothesis. Since π maps M onto $\pi(M)$ and $\pi(M)$ is finite free, by Lemma 1.2

$$M \cong \pi(M) \oplus \ker(\pi|_M)$$

and $\ker(\pi|_M) = M \cap (A \oplus 0)$. All submodules of $A \oplus 0 \cong A$ are free of rank $\leqslant 1$. Thus $\pi(M) \oplus \ker(\pi|_M)$ is free of rank $\leqslant n+1$, so M is as well. ∎

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

Nonexample 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 too: every submodule of a free module over a PID is free. The proof allowing infinite bases uses Zorn's lemma. See [1, 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 1.3, 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 $m \leqslant n$. Using Theorem 2.2 on M'' as a submodule of M', $M'' \cong A^k$ with $k \leqslant m$. 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.

Nonexample 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, 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 $m \leqslant n$ 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 $N = (1+2i)\mathbf{Z}[i]$. So $M = \mathbf{Z} + \mathbf{Z}i$ and

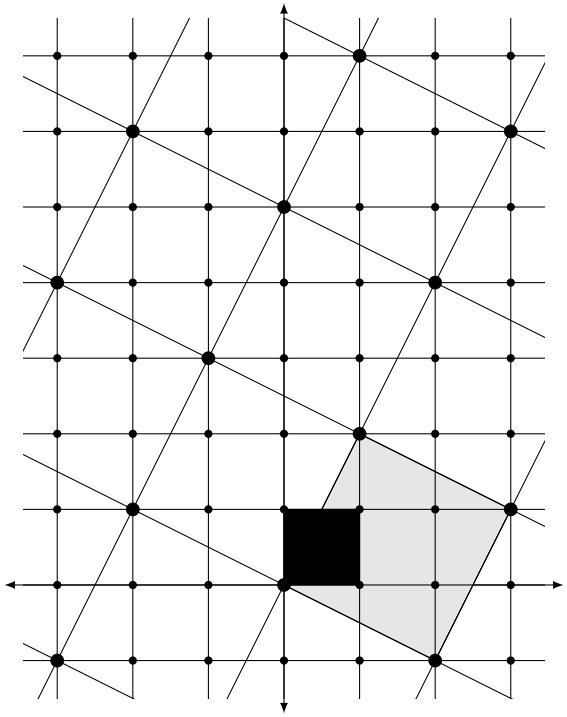
$$N = (1+2i)\mathbf{Z}[i] = (1+2i)\mathbf{Z} + (1+2i)\mathbf{Z}i = \mathbf{Z}(1+2i) + \mathbf{Z}(-2+i).$$

The obvious $\mathbf{Z}$-bases for M and N 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 N 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, we use new bases: $\{1+2i, i\}$ for M and $\{1+2i, 5i\}$ for N. 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 vectors 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.



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

FIGURE 1. Nonaligned bases for a modules and submodule

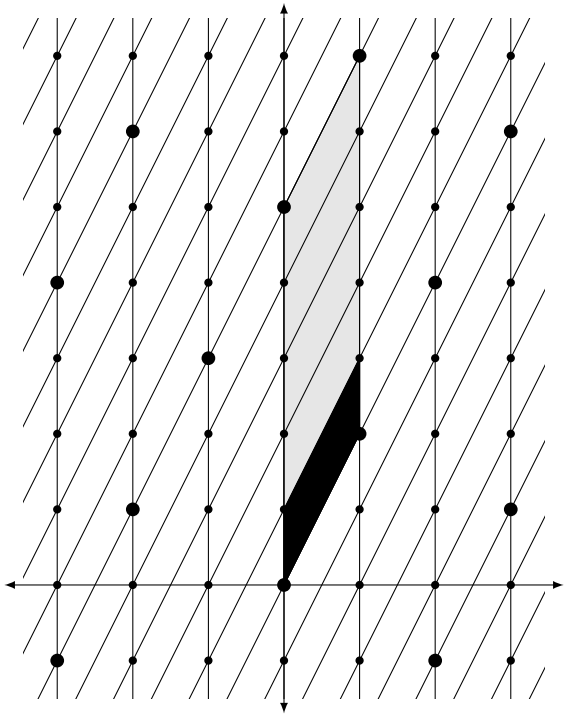
Translating the parallelograms across the plane produces two new networks of lines (both sharing all the vertical lines) The intersection points are *the same* as before; make sure you can see the vertices of the large box from Figure 1 as intersection points of lines in Figure 2. In Figure 2 five of the parallelograms for M fill up of the parallelograms for N. These bases are aligned.

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*

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

Proof. A basis of M gives us coordinate functions for that basis, which are linear maps $M \to A$. Having a set of bases for M and M' as in the theorem means there are a set of "compatible" coordinate systems on M and M'. To motivate the main idea in the proof, first suppose the theorem is true and let's see what it tells us about linear maps $\varphi\colon M \to A$ when they are restricted to M':

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



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

FIGURE 2. Aligned bases for a module and submodule

Write $Aa_1 + \cdots + Aa_m = Ac$, so $\varphi(M') \subset Ac$ for every $\varphi \in M^\vee$. Moreover, writing $c = x_1a_1 + \cdots + x_ma_m$ with $x_j \in A$ (the choice of x_i's may not be unique, but fix such a representation for c) and defining $\psi\colon M \to A$ by $\psi(\sum_{i=1}^n c_iv_i) = \sum_{j=1}^m c_jx_j$, we have $\psi(\sum_{i=1}^m a_iv_i) = c$, so

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

The set of all ideals $\varphi(M')$ as φ runs over linear maps $M \to A$ has Ac as the unique maximal member in this set with respect to inclusion (this is not saying Ac is a maximal ideal!).

Now we start over and define S to be the set of ideals $\varphi(M')$ where $\varphi\colon M \to A$ is A-linear. This includes nonzero ideals; for example, let M have A-basis $\{e_1, \ldots, e_n\}$, so $M = \bigoplus_{i=1}^n Ae_i$. At least one coordinate function for this basis is not identically 0 on M', and the image of that coordinate function on M' is a nonzero ideal in S.

Each nonzero ideal in A is contained in only finitely many ideals since A is a PID, so S contains maximal members with respect to inclusion. Call one of these maximal members Aa_1, so $a_1 \neq 0$.[2] We know already that $Aa_1 = \varphi_1(M')$ for some linear map $\varphi_1\colon M \to A$. There's some $v' \in M'$ such that

$$a_1 = \varphi_1(v').$$

Eventually we are going to show φ_1 takes the value 1 on M.

Claim: For every linear map $\varphi\colon M \to A$, $a_1 \mid \varphi(v')$.

[2]We anticipate Aa_1 will be the unique maximal member of S by the argument at the start of the proof, but at the moment it is just some maximal member of S.

To show this, set $\varphi(v') = a_\varphi \in A$. Since A is a PID, $Aa_1 + Aa_\varphi = Ad$ for some d, so $Aa_1 \subset Ad$. We have $d = xa_1 + ya_\varphi$ for some $x, y \in A$. Then

$$d = x\varphi_1(v') + y\varphi(v') = (x\varphi_1 + y\varphi)(v'),$$

so $dA \subset (x\varphi_1 + y\varphi)(M') \in S$. Hence

$$\varphi_1(M') = Aa_1 \subset Ad \subset (x\varphi_1 + y\varphi)(M').$$

Since $x\varphi_1 + y\varphi$ is a linear map $M \to A$ it belongs to S, so maximality of $\varphi_1(M')$ in S implies

$$\varphi_1(M') = (x\varphi_1 + y\varphi)(M') = Ad.$$

Hence $Aa_1 = Ad = Aa_1 + Aa_\varphi$, which implies $a_\varphi \in Aa_1$, so $a_1 \mid a_\varphi$.

With the claim proved, we are ready to build aligned bases in M and M'. Letting $M = \bigoplus_{i=1}^n Ae_i$ for some basis $\{e_1, \dots, e_n\}$, write

$$v' = c_1e_1 + \cdots + c_ne_n$$

for $c_i \in A$. The ith coordinate function for this basis is a linear map $M \to A$ taking the value c_i at v', so c_i is a multiple of a_1 by our claim. Writing $c_i = a_1b_i$,

$$v' = \sum_{i=1}^n c_ie_i = \sum_{i=1}^n a_1b_ie_i = a_1(b_1e_1 + \cdots + b_ne_n) = a_1v_1,$$

say. Then

$$a_1 = \varphi_1(v') = \varphi_1(a_1v_1) = a_1\varphi_1(v_1),$$

so $\varphi_1(v_1) = 1$. We have found an element of M at which φ_1 takes the value 1.

The module M can be written as $Av_1 + \ker\varphi_1$ since for all $v \in M$

$$v = \varphi_1(v)v_1 + (v - \varphi_1(v)v_1).$$

Also $Av_1 \cap \ker\varphi_1 = \{0\}$ (check!). Thus $M = Av_1 \oplus \ker\varphi_1$. Since M is free of rank n its submodule $\ker\varphi_1$ is free and necessarily of rank $n-1$.

How does M' fit in this decomposition of M?[3] For all $w \in M'$ we have

$$w = \varphi_1(w)v_1 + (w - \varphi_1(w)v_1)$$

and the first term is

$$\varphi_1(w)v_1 \in \varphi_1(M')v_1 = (Aa_1)v_1 = Aa_1v_1 = Av' \subset M'.$$

So $w - \varphi_1(w)v_1 \in M'$ too. Therefore

$$M' = \underbrace{(M' \cap Av_1)}_{=Aa_1v_1} \oplus (M' \cap \ker\varphi_1).$$

So $M = Av_1 \oplus \ker\varphi_1$ and $M' = Aa_1v_1 \oplus (M' \cap \ker\varphi_1)$. This last equation tells us $M' \cap \ker\varphi_1$ is free of rank $m-1$ since M' is free of rank m. If $m = 1$ then we're done. If $m > 1$, then we can describe how $M' \cap \ker\varphi_1$ sits in $\ker\varphi_1$ by induction on the rank: we have a basis $v_2, \dots, v_n$ of $\ker\varphi_1$ and $a_2, \dots, a_m \in A - \{0\}$ such that $a_2v_2, \dots, a_mv_m$ is a basis of $M' \cap \ker\varphi_1$. ∎

Corollary 2.11. *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.*

[3]Warning: if $M = M_1 \oplus M_2$ and $N \subset M$, usually $N \neq (N \cap M_1) \oplus (N \cap M_2)$. For example, consider $M = \mathbf{Z}^2 = \mathbf{Z}(1,0) \oplus \mathbf{Z}(0,1)$ with $N = \mathbf{Z}(1,1)$.

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

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

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

3. Application to matrix groups

In this section we give an application of Corollary 2.6 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 $x_1, \ldots, x_n$.

Nonexample 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 is that there is a nonzero $a \in A$ such that 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. ∎

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 2.11, $A^n/N \cong \left(\bigoplus_{j=1}^m A/(a_j)\right) \oplus A^{n-m}$ for some $m \leqslant n$ 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 $n \geqslant 0$ 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. Use the description of T in Theorem 4.1. ∎

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 as well 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 $\{(1,0),(0,1)\}$ and $\{(1,1),(0,1)\}$. Therefore it can be written as $F_1 \oplus T_1$, where $F_1 = \langle (1,0) \rangle \cong \mathbf{Z}$ and $T_1 = 0 \oplus \mathbf{Z}/(2)$, and also as $F_2 \oplus T_2$ where $F_2 = \langle (1,1) \rangle \cong \mathbf{Z}$ 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 ± 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 ±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_{tor} of M, we have $F \cong M/T = M/M_{\mathrm{tor}}$ so the rank of F is the rank of the finite free module M/M_{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 here is 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 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 (see Dirichlet's unit theorem or the Birch and Swinnerton-Dyer conjecture).

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

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

This is not the same thing as the annihilator ideal $\mathrm{Ann}_A(T) = \{a \in A : aT = 0\}$, just as in group theory the order of a finite abelian group is not the same thing in general as the least positive integer whose power kills everything in the group (the exponent of the group).

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.*, $\mathbf{Z}/(4)\times\mathbf{Z}/(5) \cong \mathbf{Z}/(20)$), so we really need to check A-cardinality is well-defined. But first we look at a few examples of A-cardinality.

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. Let $V = \mathbf{R}^2$, viewed as an $\mathbf{R}[X]$-module with X acting on $\mathbf{R}^2$ as the identity matrix. Then, as an $\mathbf{R}[X]$-module, we have V 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 $\mathbf{R}[X]$.

Example 5.4. 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.

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

Theorem 5.5. *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 $(a_1a_2\cdots a_m) = (b_1b_2\cdots b_n)$ 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 π in A, we will show the highest power of π in $a_1a_2\dots a_m$ and $b_1b_2\cdots b_n$ are equal. Therefore by unique factorization (every PID is a UFD) $a_1a_2\dots a_m$ and $b_1b_2\cdots b_n$ are equal up to multiplication by a unit, so $(a_1a_2\dots a_m) = (b_1b_2\cdots b_n)$.

Set $T = A/(a_1) \oplus \cdots \oplus A/(a_m)$. For each irreducible π 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 $\pi^{i-1}T/\pi^iT$ is an A-module on which multiplication by π 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 π^{i-1}) and thus so is its quotient $\pi^{i-1}T/\pi^iT$, so $\pi^{i-1}T/\pi^iT$ is a finite-dimensional $A/(\pi)$-vector space. The dimensions $\dim_{A/(\pi)}(\pi^{i-1}T/\pi^iT)$ will be the key. We will show the highest power of π in $a_1a_2\dots a_m$ is $\sum_{i\geqslant 1}\dim_{A/(\pi)}(\pi^{i-1}T/\pi^iT)$.

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

For $i \geqslant 1$ we will show

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

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

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

which is the highest power of π dividing a.

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

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

so

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

so summing over all $i \geqslant 1$ gives us on the right the sum of the highest powers of π in all a_k's, which is the highest power of π in $a_1a_2 \cdots a_m$.

Step 3: Comparing isomorphic cyclic decompositions.

The number $\dim_{A/(\pi)}(\pi^{i-1}T/\pi^iT)$, 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 $\pi^{i-1}T/\pi^iT \to \pi^{i-1}T'/\pi^iT'$ in a natural way. Therefore $a_1a_2 \dots a_m$ and $b_1b_2 \cdots b_n$ are divisible by the same highest power of π, for all π. ∎

Example 5.6. 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 5.7. For nonzero $a \in A$, $\mathrm{card}_A(A/(a)) = (a)$. (This is trivial only after we know that A-cardinality is well-defined.) For nonzero a and b, $\mathrm{card}_A(A/(ab)) = (ab) = (a)(b) = \mathrm{card}_A(A/(a))\,\mathrm{card}_A(A/(b))$.

Corollary 5.8. *If T is a finitely generated torsion module over A 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 $a_1a_2 \cdots a_m$ 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 5.9. *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 also generalizes from abelian groups to finitely generated modules over a PID, as an ideal.

Definition 5.10. 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 5.11. 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 5.12. 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 5.13. 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 2.11 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 7). 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 5.14. *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 8. ∎

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 5.15. *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_i with f_i, so M' inside M is identified with the $\mathbf{Z}$-span of $f_1, \ldots, f_n$ inside $\mathbf{Z}^n$.

Every $\mathbf{Z}$-linear map $\mathbf{Z}^n \to \mathbf{Z}^n$ is determined by where it sends $e_1, \ldots, e_n$. 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 φ 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

$$[\mathbf{Z}^n : \varphi(\mathbf{Z}^n)] = |a_1a_2 \cdots a_n|. \tag{5.1}$$

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

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

This diagram commutes: $\varphi = \gamma \circ \beta \circ \alpha$. Taking determinants of these $\mathbf{Q}$-linear maps $\mathbf{Q}^n \to \mathbf{Q}^n$,[4]

$$\det(\varphi) = \det(\gamma)\det(\beta)\det(\alpha). \tag{5.2}$$

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

$$\det(\beta\colon \mathbf{Q}^n \to \mathbf{Q}^n) = a_1a_2 \cdots a_n.$$

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

$$\alpha(c_1e_1 + \cdots + c_ne_n) = c_1v_1 + \cdots + c_nv_n, \qquad c_i \in \mathbf{Z}.$$

Therefore α 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 α 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 has determinant ± 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 γ identifies two $\mathbf{Z}$-bases of $\varphi(\mathbf{Z}^n)$. Feeding these determinant formulas into the right side of (5.2),

$$\det(\varphi) = \pm a_1a_2 \cdots a_n. \tag{5.3}$$

[4]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.

Comparing (5.1) and (5.3), $|\det(\varphi)| = |a_1a_2\cdots a_n| = [\mathbf{Z}^n : \varphi(\mathbf{Z}^n)] = [M : M']$. ∎

Example 5.16. 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 by finding $\mathbf{Z}$-bases for $\mathbf{Z}[\sqrt{10}]$ and $\mathfrak{a}$ and then computing the determinant of the matrix expressing the second basis in terms of the first. The $\mathbf{Z}$-bases do not have to be aligned to make the calculation.

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: 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 $\mathfrak{a}$. Under the isomorphism $\mathbf{Z}[\sqrt{10}] \to \mathbf{Z}^2$ as abelian groups ($\mathbf{Z}$-modules) by $a + b\sqrt{10} \mapsto \binom{a}{b}$, the ideal $\mathfrak{a}$ is identified 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 5.15 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 5.17. *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 5.15 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 5.15 shows $\det(c_{ij}) = \det\varphi = ua_1 \ldots a_n$, where $u = \det\alpha \det\gamma$ is a unit in A. The K-linear operators α and γ 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 5.18. *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 5.17.

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,

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

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 5.19. *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 5.17, 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 5.18 and the A-index of $\sum Ay_j$ in M is $(\det(c_{ij})) = (1)$, so $\sum Ay_j = M$. ∎

Example 5.20. 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 ± 1, since this matrix expresses $v_1, \ldots, v_n$ in terms of the standard basis of $\mathbf{Z}^n$.

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. Let A be a commutative ring, M be an A-module, and $f\colon M \to A^n$ be an A-linear surjection. For the standard basis $e_1, \ldots, e_n$ of A^n, pick $m_i \in M$ such that $f(m_i) = e_i$. Define the linear maps $g\colon A^n \to M$ by $g(e_i) = m_i$ for all i and $h\colon M \to A^n \oplus \ker f$ by
$$h(m) = (f(m), m - g(f(m)))$$
for all $m \in M$. Show h is an A-module isomorphism. (Hint on surjectivity: for $(x, y) \in A^n \oplus \ker f$ let $m = g(x) + y$. Then $h(m) = (x, y)$.)
3. Suppose A is a PID and π 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.
4. 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 π in A and using $M = A \oplus A/(\pi)$ and $M' = A(\pi, \overline{1})$. (Hint: first show M' is free.)

5. 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 π in A such that π divides $\mathrm{card}_A(T)$, meaning π divides a generator of the ideal $\mathrm{card}_A(T)$, show there is some $t \in T$ with "order" π: the annihilator ideal $\mathrm{Ann}_A(t) = \{a \in A : at = 0\}$ is πA.

   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 even for $A = \mathbf{Z}$, since infinite torsion abelian groups exist.)

   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 $aM \subset N$.

6. Let V be a finite-dimensional vector space over a field K and $f\colon V \to V$ be an K-linear operator. Viewing V as an $K[X]$-module where X acts on V as the map f, show $\mathrm{card}_{K[X]}(V) = (\chi_f(X))$, where χ_f is the characteristic polynomial of f.
7. 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 2.11 in the case of free modules.
8. Let T be a finitely generated torsion module over the PID A and T' be a submodule. Show $\mathrm{card}_A(T) = \mathrm{card}_A(T')\,\mathrm{card}_A(T/T')$.
9. Prove Corollaries 5.18 and 5.19 when A is an arbitrary integral domain, not necessarily a PID.

References

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