SIMULTANEOUSLY ALIGNED BASES

KEITH CONRAD

Let R be a PID, n be a positive integer, and M be a finite free R-module of rank n. By the structure theorem for modules over a PID, for any submodule M' of M also having rank n (to be called a *full submodule* of M) we can find a basis $e_1, \ldots, e_n$ of M and nonzero $a_1, \ldots, a_n$ in R such that $a_1e_1, \ldots, a_ne_n$ is a basis of M'. We call such a pair of bases of M and M' *aligned*.

Pick two full submodules of M, say M' and M''. If there is a basis $e_1, \ldots, e_n$ of M and two sets of nonzero $a'_1, \ldots, a'_n$ and $a''_1, \ldots, a''_n$ in R such that

$$M = \bigoplus_{i=1}^n Re_i, \quad M' = \bigoplus_{i=1}^n Ra'_ie_i, \quad M'' = \bigoplus_{i=1}^n Ra''_ie_i$$

then we'll say M' and M'' admit *simultaneously aligned bases*. Do such bases always exist? Of course if R is a field then they do because the only full submodule of M is M, so the situation is trivial.

The following example shows simultaneously aligned bases need not exist in R^2 if R is not a field.

Example 1. Let R be a PID that is not a field, so R contains prime elements. Let π be prime in R. Inside R^2 set

$$M' = R\begin{pmatrix}1\\0\end{pmatrix} + R\begin{pmatrix}0\\\pi^2\end{pmatrix} = \left\{\begin{pmatrix}x\\y\end{pmatrix} : y \equiv 0 \bmod \pi^2\right\} \tag{1}$$

and

$$M'' = R\begin{pmatrix}\pi\\0\end{pmatrix} + R\begin{pmatrix}1\\\pi\end{pmatrix} = \left\{\begin{pmatrix}x\\y\end{pmatrix} : y \equiv 0 \bmod \pi, \pi x \equiv y \bmod \pi^2\right\}. \tag{2}$$

First we determine an aligned basis for M' and for M'' as submodules of R^2. The first one is easy: $M' = R\binom{1}{0} + R\pi^2\binom{0}{1}$, so we can use $\{\binom{1}{0}, \binom{0}{1}\}$ as a basis of R^2 and $\{\binom{1}{0}, \pi^2\binom{0}{1}\}$ as a basis of M'. For M'', we rewrite it as

$$M'' = R\begin{pmatrix}0\\\pi^2\end{pmatrix} + R\begin{pmatrix}1\\\pi\end{pmatrix} = R\pi^2\begin{pmatrix}0\\1\end{pmatrix} + R\begin{pmatrix}1\\\pi\end{pmatrix},$$

so we can use $\{\binom{0}{1}, \binom{1}{\pi}\}$ as a basis of R^2 and $\{\pi^2\binom{0}{1}, \binom{1}{\pi}\}$ as a basis of M''. Using these aligned bases we see that R^2/M' and R^2/M'' are both isomorphic to $R/(\pi^2)$.

Suppose there is some basis $\{e_1, e_2\}$ of R^2 and nonzero a_1, a_2, b_1, b_2 in R such that $\{a_1e_1, a_2e_2\}$ is a basis of M' and $\{b_1e_1, b_2e_2\}$ is a basis of M''. We are going to get a contradiction. Since $R^2/M' \cong R/(a_1) \times R/(a_2)$ and $R^2/M'' \cong R/(b_1) \times R/(b_2)$, from the known structure of R^2/M' and R^2/M'' we have

$$(a_1a_2) = (\pi^2), \quad (b_1b_2) = (\pi^2). \tag{3}$$

Write $e_1 = \binom{x_1}{y_1}$ and $e_2 = \binom{x_2}{y_2}$, so being a basis of R^2 is equivalent to

$$x_1y_2 - x_2y_1 \in R^\times. \tag{4}$$

Granting (3), to have $\{a_1e_1, a_2e_2\}$ be a basis of M' and $\{b_1e_1, b_2e_2\}$ be a basis of M'' is equivalent to having a_1e_1 and a_2e_2 lying in M' and b_1e_1 and b_2e_2 lying in M''.

Having $a_1e_1 = \binom{a_1x_1}{a_1y_1}$ and $a_2e_2 = \binom{a_2x_2}{a_2y_2}$ in M' is equivalent to $a_1y_1, a_2y_2 \equiv 0 \bmod \pi^2$. By (4), y_1 and y_2 can't both be divisible by π, so one of a_1 or a_2 is divisible by π^2. Therefore by (3), $\{(a_1),(a_2)\} = \{(1),(\pi^2)\}$. So far the roles of e_1 and e_2 have been symmetric, so without loss of generality we can take

$$(a_1) = (1), \quad (a_2) = (\pi^2).$$

Therefore $y_1 \equiv 0 \bmod \pi^2$, so $y_2 \not\equiv 0 \bmod \pi$ (because y_1 and y_2 are relatively prime).

Having $b_1e_1 = \binom{b_1x_1}{b_1y_1}$ and $b_2e_2 = \binom{b_2x_2}{b_2y_2}$ in M'' implies $b_1y_1, b_2y_2 \equiv 0 \bmod \pi$, so $b_2 \equiv 0 \bmod \pi$. It also implies, by (2), that $\pi b_1x_1 \equiv b_1y_1 \bmod \pi^2$ and $\pi b_2x_2 \equiv b_2y_2 \bmod \pi^2$. Since y_1 is a multiple of π^2 and b_2 is a multiple of π, these congruences mod π^2 become $\pi b_1x_1 \equiv 0 \bmod \pi^2$ and $0 \equiv b_2y_2 \bmod \pi^2$. Since y_2 is not a multiple of π, $b_2 \equiv 0 \bmod \pi^2$, so from (3) we have $(b_1) = (1)$ and $(b_2) = (\pi^2)$. Therefore $\pi b_1x_1 \equiv 0 \bmod \pi^2 \Rightarrow x_1 \equiv 0 \bmod \pi$. But x_1 and y_1 can't both be multiples of π since they are relatively prime, so we have a contradiction.

We now seek a criterion on pairs of full submodules that determines when they have simultaneously aligned bases. When M is a finite free R-module and M' is a full submodule with aligned bases $\{e_1, \cdots, e_n\}$ for M and $\{a_1e_1, \cdots, a_ne_n\}$ for M', the linear operator $A\colon M \to M$ where $A(e_i) = a_ie_i$ has image M' and $\det A = a_1 \cdots a_n \neq 0$. Conversely, if $A\colon M \to M$ is a linear operator with nonzero determinant, then $A(M)$ is a full submodule of M with $(\det A) = (c_1 \dots c_k)$ as ideals, where $M/A(M)$ has the cyclic decomposition $R/(c_1) \times \cdots \times R/(c_k)$. Therefore the full submodules of M are the same thing as images of linear operators $A\colon M \to M$ with nonzero determinant, and $\det A$ is determined up to unit multiple by the structure of $M/A(M)$ as an R-module. Writing a full submodule M' of M as $A(M)$ for some linear operator A on M, how much does M' determine A?

Lemma 2. *If A_1 and A_2 are two linear operators on M with nonzero determinant, then $A_1(M) = A_2(M)$ if and only if $A_1 = A_2U$ for some $U \in \mathrm{GL}(M)$.*

Proof. Let $e_1, \dots, e_n$ be a basis of M. If $A_1(M) = A_2(M)$ then $A_1(e_i) = A_2(f_i)$ for some $f_i \in M$. Let $U\colon M \to M$ be the linear map satisfying $U(e_i) = f_i$ for all i. Then $A_1(e_i) = A_2(U(e_i)) = A_2U(e_i)$, so by linearity $A_1(m) = A_2U(m)$ for all $m \in M$, and thus $A_1 = A_2U$. From $A_1(M) = A_2(M)$ we get $M/A_1(M) = M/A_2(M)$, so $\det A_1$ and $\det A_2$ are equal up to unit multiple. Then the condition $\det A_1 = (\det A_2)(\det U)$ implies $\det U \in R^\times$, so $U \in \mathrm{GL}(M)$.

Conversely, if $A_1 = A_2U$ with $U \in \mathrm{GL}(M)$ then $A_1(M) = A_2(U(M)) = A_2(M)$. □

By this lemma, if we write a full submodule of M as $A(M)$ for some $A \in \mathrm{End}(M)$, then A is determined by $A(M)$ up to right multiplication by an element of $\mathrm{GL}(M)$.

Pick two full submodules of M, say $A(M)$ and $B(M)$, with simultaneously aligned bases: there is a basis $e_1, \dots, e_n$ of M and two sets of n nonzero $a_1, \dots, a_n$ and $b_1, \dots, b_n$ in R such that

$$M = \bigoplus_{i=1}^n Re_i, \quad A(M) = \bigoplus_{i=1}^n Ra_ie_i, \quad B(M) = \bigoplus_{i=1}^n Rb_ie_i.$$

Let $D\colon M \to M$ and $D'\colon M \to M$ be the linear maps defined by $D(e_i) = a_ie_i$ and $D'(e_i) = b_ie_i$. Written as matrices with respect to the basis $e_1, \dots, e_n$, both D and D' become diagonal matrices, so D and D' are diagonalizable operators on M. Easily $A(M) = D(M)$ and $B(M) = D'(M)$, so $D = AU$ and $D' = BV$ for some U and V in $\mathrm{GL}(M)$. Obviously D and D' commute, so AU and BV commute. We now show the converse is true too.

Theorem 3. *Choose A and B in* $\mathrm{End}(M)$ *with* $\det A \neq 0$ *and* $\det B \neq 0$. *Suppose there are U and V in* $\mathrm{GL}(M)$ *such that AU and BV commute and are diagonalizable. Then the submodules $A(M)$ and $B(M)$ of M have simultaneously aligned bases.*

Proof. Set $A' = AU$ and $B' = BV$, so $A'(M) = A(M)$ and $B'(M) = B(M)$. Since A' is diagonalizable, there is a basis $e_1, \dots, e_n$ of M and nonzero $a_1, \dots, a_n$ in R such that $A'(e_i) = a_i e_i$ for all i. Then

$$M = \bigoplus_{i=1}^{n} Re_i, \quad A'(M) = \bigoplus_{i=1}^{n} RA'(e_i) = \bigoplus_{i=1}^{n} Ra_i e_i.$$

Let $\lambda_1, \dots, \lambda_k$ be the distinct values among $a_1, \dots, a_n$ and set $M_j = \{v \in M : A'(v) = \lambda_j v\}$ (this is the λ_j-eigenspace of A'). Each e_i is in some M_j, so $M = M_1 + M_2 + \cdots + M_k$. Elements from different M_j's are linearly independent (same as proof in vector spaces that eigenvectors for different eigenvalues of a linear operator are linearly independent). Therefore

$$M = M_1 \oplus \cdots \oplus M_k.$$

For $v \in M_j$, $A'(B'v) = B'(A'v) = B'(\lambda_j v) = \lambda_j(B'v)$, so $B'(M_j) \subset M_j$ for all j. Let d_j be the rank of M_j. Since M_j is a finite free R-module, the structure theorem for modules over a PID says there is a basis $e_{1j}, \dots, e_{d_j j}$ of M_j and nonzero $c_{1j}, \dots, c_{d_j j}$ in R such that

$$M_j = Re_{1j} \oplus \cdots \oplus Re_{d_j j}, \quad B'(M_j) = Rc_{1j}e_{1j} \oplus \cdots \oplus Rc_{d_j j}e_{d_j j}.$$

Then

$$M = \bigoplus_{j=1}^{k} M_j = \bigoplus_{j=1}^{k} \bigoplus_{\ell=1}^{d_j} Re_{\ell j},$$

$$B(M) = B'(M) = \bigoplus_{j=1}^{k} B'(M_j) = \bigoplus_{j=1}^{k} \bigoplus_{\ell=1}^{d_j} Rc_{\ell j}e_{\ell j},$$

and

$$A(M) = A'(M) = \bigoplus_{j=1}^{k} A'(M_j) = \bigoplus_{j=1}^{k} \lambda_j M_j = \bigoplus_{j=1}^{k} \bigoplus_{\ell=1}^{d_j} R\lambda_j e_{\ell j}.$$

We have found simultaneously aligned bases for $A(M)$ and $B(M)$ in M. $\square$

Let's consider now any finite number of full submodules, not just two. The definition of simultaneously aligned bases for more than two full submodules of a finite free R-module is clear: a basis for the whole module that can be scaled to a basis of each of the submodules.

Example 4. If we view the ring of integers of a number field as a $\mathbf{Z}$-module, any finite set of nonzero ideals in it has simultaneously aligned $\mathbf{Z}$-bases. This is proved in [1], where Example 1 also appears for the case $R = \mathbf{Z}$ and $\pi = 3$.

Corollary 5. *For $r \geq 2$ and $A_1, \dots, A_r$ in* $\mathrm{End}(M)$ *with nonzero determinants, the submodules $A_1(M), \dots, A_r(M)$ of M have simultaneously aligned bases if and only if there are $U_1, \dots, U_r$ in* $\mathrm{GL}(M)$ *such that $A_1U_1, \dots, A_rU_r$ are diagonalizable and pairwise commuting.*

In particular, if $A_1, \dots, A_r$ are diagonalizable and pairwise commuting in $\mathrm{End}(M)$ *with nonzero determinants then the submodules $A_1(M), \dots, A_r(M)$ of M have simultaneously aligned bases.*

Proof. If there are simultaneously aligned bases for $A_1(M), \dots, A_r(M)$, then the same argument as before leads to $U_1, \dots, U_r$ in $\mathrm{GL}(M)$ such that $A_1U_1, \dots, A_rU_r$ are diagonalizable and pairwise commuting.

Conversely, suppose there are $U_1, \ldots, U_r$ in $\mathrm{GL}(M)$ such that $A_1U_1, \ldots, A_rU_r$ are diagonalizable and pairwise commuting operators on M. Set $A_1' = A_1U_1, \ldots, A_r' = A_rU_r$. We want to show the submodules $A_1(M), \ldots A_r(M)$ have simultaneously aligned bases in M. Since $A_1'(M) = A_1(M), \ldots, A_r'(M) = A_r(M)$, we can replace $A_1, \ldots, A_r$ with $A_1', \ldots, A_r'$: to show $A_1'(M), \ldots, A_r'(M)$ have simultaneously aligned bases when $A_1', \ldots, A_r'$ are diagonalizable and pairwise commuting, we will proceed by the same inductive argument that is used to show a set of commuting diagonalizable operators on a finite-dimensional vector space are simultaneously diagonalizable.

Since A_1' is diagonalizable, there is a basis $e_1, \ldots, e_n$ of M and nonzero $a_1, \ldots, a_n$ in R such that $A_1'(e_i) = a_ie_i$ for all i, so

$$M = \bigoplus_{i=1}^n Re_i, \quad A_1'(M) = \bigoplus_{i=1}^n RA_1'(e_i) = \bigoplus_{i=1}^n Ra_ie_i.$$

Let $\lambda_1, \ldots, \lambda_k$ be the distinct values among $a_1, \ldots, a_n$. Then as before,

$$M = M_1 \oplus \cdots \oplus M_k,$$

where $M_j = \{v \in M : A_1'(v) = \lambda_j v\}$ (and $M_j \neq \{0\}$). As before, each M_j is preserved by $A_2', \ldots, A_r'$ and the restrictions of these operators[1] to M_j are pairwise commuting with nonzero determinant. Once we show the restrictions of $A_2', \ldots, A_r'$ to M_j are each diagonalizable, then by induction on the number of operators there are simultaneously aligned bases for $A_2'(M_j), \ldots, A_r'(M_j)$ as submodules of M_j (that is, each M_j has a basis that can be scaled termwise to provide a basis of those submodules). All elements of M_j are eigenvectors for A_1', so by stringing together bases of $M_1, \ldots, M_k$ to give a basis of M we have a simultaneously aligned basis for $A_1'(M), \ldots, A_r'(M)$ in M, and then we'd be done (since $A_1'(M) = A_1(M), \ldots, A_r'(M) = A_r(M)$).

□

References

[1] H. B. Mann and K. Yamamoto, "On canonical bases of ideals," J. Combinatorial Theory **2** (1967), 71–76.

[1]We have no reason to expect $A_2, \ldots, A_r$ preserve the M_j's.