RELATED 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 scalars $a_1, \ldots, a_n$ in R such that $a_1e_1, \ldots, a_ne_n$ is a basis of M'. We call this basis of M and basis of M' *aligned bases*.

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 n nonzero $a'_1, \ldots, a'_n$ and $a''_1, \ldots, a''_n$ in R such that

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

we'll call $\{a'_1e_1, \ldots, a'_ne_n\}$ and $\{a''_1e_1, \ldots, a''_ne_n\}$ a pair of *related aligned bases* for the two submodules of M. 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. To keep things interesting, we assume from now on that R is not a field, so R contains prime elements.

The following example shows such a pair of bases does not always exist for submodules of R^2.

Let π be prime in R. Inside R^2 set

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

and

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

First we determine a pair of aligned bases for M' and M'' separately as submodules of R^2. The first one is easy since it's given to us in the definition: $M' = R\binom{1}{0} + R\pi^2\binom{0}{1}$, so $R^2/M' \cong R/(\pi^2)$. For M'', we rewrite it as

$$M'' = R\binom{0}{\pi^2} + R\binom{1}{\pi} = R\pi^2\binom{0}{1} + R\binom{1}{\pi},$$

so $R^2/M'' \cong R/(\pi^2)$.

Suppose there is a 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. From the known structure of R^2/M' and R^2/M'',

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

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.

This example raises some questions. Are there related aligned bases for two full submodules M' and M'' of R^2 when R^2/M' and R^2/M'' are isomorphic to $R/(\pi)$? What about when R^2/M' and R^2/M'' have relatively prime R-cardinality (that is, the products of the moduli in a cyclic decomposition of each quotient module are relatively prime to each other)?

In a positive direction, there are related aligned bases for any finite set of nonzero ideals in the ring of integers of a number field, viewed as $\mathbf{Z}$-submodules of the ring of integers. This is proved in [1], which also includes the above example for the case $R = \mathbf{Z}$ and $\pi = 3$.

We now seek a criterion on pairs of full submodules which determines when they have a pair of related aligned bases. We will use a description of full submodules as images of linear operators. When M is a finite free R-module and M' is a full submodule with aligned bases $\{e_1, \cdots, e_n\}$ and $\{a_1e_1, \cdots, a_ne_n\}$, 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 $L\colon M \to M$ is a linear operator with nonzero determinant, then $L(M)$ is a full submodule of M. So the full submodules of M are the same thing as images of linear operators on M with nonzero determinant. How much does a full submodule determine an operator having it as an image? If A and A' are two linear operators on M with nonzero determinant such that $A(M) = A'(M)$, then $A = A'U$ where $U \in \mathrm{GL}(M)$. The converse is easy, so A is determined by $A(M)$ up to right multiplication by some element of $\mathrm{GL}(M)$.

Pick two full submodules of M, say $A(M)$ and $B(M)$. There is a basis $e_1, \ldots, e_n$ of M and two sets of n nonzero $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ 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 determined by $D(e_i) = a_ie_i$ and $D'(e_i) = b_ie_i$. Written as matrices with respect to the basis $e_1, \ldots, e_n$, D and D' become diagonal matrices. 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 1. *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. Then the submodules $A(M)$ and $B(M)$ of M admit related aligned bases.*

Proof. Set $A' = AU$ and $B' = BV$, so $A'(M) = A(M)$ and $B'(M) = B(M)$. From the structure theorem for modules over a PID, there is a basis $e_1, \ldots, e_n$ of M and nonzero

$a_1, \ldots, a_n$ in R such that

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

Let $a_1, \ldots, a_k$ be the distinct values among $a_1, \ldots, a_n$. Then

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

where $M_i = \{v \in M : A'(v) = a_i v\}$ (and $M_i \neq \{0\}$).

For $v \in M_i$, $A'(B'v) = B'(A'v) = B'(a_i v) = a_i(B'v)$, so $B'(M_i) \subset M_i$ for all i. Let d_i be the rank of M_i. Since M_i is a finite free R-module, the structure theorem for modules over a PID says there is a basis $e_{i1}, \ldots, e_{id_i}$ of M_i and nonzero $c_{i1}, \ldots, c_{id_i}$ in R such that

$$M_i = Re_{i1} \oplus \cdots \oplus Re_{id_i}, \quad B'(M_i) = Rc_{i1}e_{i1} \oplus \cdots \oplus Rc_{id_i}e_{id_i}.$$

Then

$$M = \bigoplus_{i=1}^{k} M_i = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{d_i} Re_{ij},$$

$$B(M) = B'(M) = \bigoplus_{i=1}^{k} B'(M_i) = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{d_i} Rc_{ij}e_{ij},$$

and

$$A(M) = A'(M) = \bigoplus_{i=1}^{k} A'(M_i) = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{d_i} RA'(e_{ij}) = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{d_i} Ra_i e_{ij}.$$

So we have found related aligned bases for $A(M)$ and $B(M)$. □

Let's consider now any finite number of full submodules, not just two. The definition of related aligned bases for more than two submodules is clear.

Corollary 1. *For $r \geq 2$ and $A_1, \ldots, A_r$ in $\mathrm{End}(M)$ with nonzero determinants, the submodules $A_1(M), \ldots, A_r(M)$ of M admit related aligned bases if and only if there are $U_1, \ldots, U_r$ in $\mathrm{GL}(M)$ such that $A_1U_1, \ldots, A_rU_r$ are pairwise commuting.*

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

Proof. If there are related aligned bases for the submodules then the same argument as before leads to $U_1, \ldots, U_r$ such that $A_1U_1, \ldots, A_rU_r$ are pairwise commuting. Conversely, if there are $U_1, \ldots, U_r$ in $\mathrm{GL}(M)$ such that $A_1U_1, \ldots, A_rU_r$ are pairwise commuting, set $A'_1 = A_1U_1, \ldots, A'_r = A_rU_r$.

From the structure theorem for modules over a PID, there is a basis $e_1, \ldots, e_n$ of M and nonzero $a_1, \ldots, a_n$ in R such that

$$M = \bigoplus_{i=1}^{n} Re_i, \quad A_1(M) = A'_1(M) = \bigoplus_{i=1}^{n} Ra_i e_i.$$

Let $a_1, \ldots, a_k$ be the distinct values among $a_1, \ldots, a_n$. Then

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

where $M_i = \{v \in M : A'_1(v) = a_i v\}$ (and $M_i \neq \{0\}$). As before, each M_i is preserved by $A'_2, \ldots, A'_r$ and the restrictions of these operators[1] to M_i are pairwise commuting with nonzero determinant, so by induction on the number of operators there are related aligned bases for $A'_2(M_i), \ldots, A'_r(M_i)$ as submodules of M_i (that is, each M_i has a basis which

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

can be scaled termwise to provide a basis of those submodules). All elements of M_i are eigenvectors for A_1', so stringing together the bases of $M', \dots, M_k$ to give a basis of M, we have a related aligned basis for $A_1'(M), \dots, A_r'(M)$, which are the same submodules as $A_1(M), \dots, A_r(M)$. $\square$

References

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