PRIMITIVE VECTORS AND SL_n

KEITH CONRAD

An n-tuple $[a_1, \ldots, a_n] \in \mathbf{Z}^n$ is called *primitive* when its coordinates are relatively prime as an n-tuple. For instance, $[6, 10, 15]$ is a primitive vector in $\mathbf{Z}^3$: even though its coordinates are not pairwise relatively prime they are relatively prime as a triple. We use brackets rather than parentheses for vectors so that we may reserve the use of parentheses for greatest common divisors and ideals later.

Any primitive vector $[a_1, a_2] \in \mathbf{Z}^2$ can be used as the first row of an integral matrix with determinant 1: since $(a_1, a_2) = 1$ we can write $a_1x + a_2y = 1$ for some $x, y \in \mathbf{Z}$, which is equivalent to $\det\left(\begin{smallmatrix} a_1 & a_2 \\ -y & x \end{smallmatrix}\right) = 1$. This is a matrix in $\mathrm{SL}_2(\mathbf{Z})$. There is a generalization to longer primitive vectors:

Theorem 1. *For $n \geq 2$, any $[a_1, \ldots, a_n] \in \mathbf{Z}^n$ with $(a_1, \ldots, a_n) = (1)$ is the first row of a matrix in $\mathrm{SL}_n(\mathbf{Z})$.*

Proof. See [4], where Theorem 1 is used to prove the structure theorem for finitely generated abelian groups. □

The converse of Theorem 1 is also true: for $n \geq 2$, the first row of any matrix in $\mathrm{SL}_n(\mathbf{Z})$ is a primitive vector, since expansion of the determinant along the first row shows 1 is a $\mathbf{Z}$-linear combination of the entries in the first row.

If we work in any commutative ring A, and call a vector $[a_1, \ldots, a_n] \in A^n$ primitive when the ideal $(a_1, \ldots, a_n)$ is the unit ideal of A, is it true that any primitive vector in A^n is the first row of a matrix in $\mathrm{SL}_n(A)$? The answer is no. The simplest example occurs for the ring $R = \mathbf{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$, where the vector $[x, y, z] \in R^3$ is primitive (because $x \cdot x + y \cdot y + z \cdot z = 1$ in R) but $[x, y, z]$ is not the first row of a matrix in $\mathrm{SL}_3(R)$ (or even $\mathrm{GL}_3(R)$); this turns out to follow from the topological fact that any continuous vector field on the sphere vanishes somewhere. The technical buzzword here is "stably free module" if you want to look up further references to this phenomenon.

Despite the failure of Theorem 1 to generalize to all commutative rings, it does generalize to some rings besides $\mathbf{Z}$. For instance, Theorem 1 generalizes to vectors with coordinates in any PID. (The proof in [4] for $A = \mathbf{Z}$ only uses PID properties of $\mathbf{Z}$, so it is valid for any PID; or see [3, Lemma 5.20], which is essentially the proof from [4], including the same notation and introducing a minor mistake.) Our interest is in a further generalization: by a nice use of the Chinese remainder theorem, Theorem 1 can be proved for vectors with coordinates coming from any Dedekind domain.

Theorem 2. *Let A be a Dedekind domain. If $n \geq 2$ and the ideal $(a_1, \ldots, a_n)$ is the unit ideal $(1) = A$ then the n-tuple $[a_1, \ldots, a_n]$ is the first row of a matrix in $\mathrm{SL}_n(A)$.*

To prove this, following the ideas in [1], we first establish two lemmas.

Lemma 3. *Let A be a commutative ring and pick a vector $v \in A^n$ and a matrix $U \in \mathrm{SL}_n(A)$. Then v is the first row of a matrix in $\mathrm{SL}_n(A)$ if and only if the product $vU \in A^n$ is the first row of a matrix in $\mathrm{SL}_n(A)$.*

Proof. Suppose there is a matrix $M \in \mathrm{SL}_n(A)$ with first row v. Then $MU \in \mathrm{SL}_n(A)$ has first row vU. Conversely, if there is a matrix $N \in \mathrm{SL}_n(A)$ with first row vU then $NU^{-1} \in \mathrm{SL}_n(A)$ has first row $(vU)U^{-1} = v$. □

The following lemma about Dedekind domains will provide a reduction step in the proof of Theorem 2.

Lemma 4. *Let A be a Dedekind domain. If $n \geq 3$ and $(a_1, \ldots, a_n) = (1)$ in A with $a_1, \ldots, a_{n-2}$ not all 0 then there is some $b \in A$ such that $(a_1, \ldots, a_{n-2}, a_{n-1} + ba_n) = (1)$.*

The point here is that we can turn a set of n generators of the unit ideal into a set of $n-1$ generators by combining two terms in a particularly simple way.

Proof. By hypothesis, $(a_1, \ldots, a_{n-2}) \neq (0)$. If $(a_1, \ldots, a_{n-2}) = (1)$ we can take b to be any element of A. So we may assume $(a_1, \ldots, a_{n-2})$ is neither (0) nor (1). Factor $(a_1, \ldots, a_{n-2})$ into primes as $\mathfrak{p}_1 \cdots \mathfrak{p}_r$. (Perhaps some $\mathfrak{p}_i$ are equal.) In particular, $a_1, \ldots, a_{n-2}$ belong to each $\mathfrak{p}_i$.

For $i = 1, 2, \ldots, r$, choose $b_i \in A$ so that $a_{n-1} + b_i a_n \not\equiv 0 \bmod \mathfrak{p}_i$. Why is this possible? Well, when $a_n \not\equiv 0 \bmod \mathfrak{p}_i$ we can solve $a_{n-1} + xa_n \equiv 1 \bmod \mathfrak{p}_i$ since $A/\mathfrak{p}_i$ is a field and then set $b_i = x$. When $a_n \equiv 0 \bmod \mathfrak{p}_i$ we can let b_i be anything at all and we must check that $a_{n-1} \not\equiv 0 \bmod \mathfrak{p}_i$: $a_1, a_2, \ldots, a_{n-2} \in \mathfrak{p}_i$ and $a_n \in \mathfrak{p}_i$, so if $a_{n-1} \in \mathfrak{p}_i$ then $(a_1, \ldots, a_{n-1}, a_n) \subset \mathfrak{p}_i$, but $(a_1, \ldots, a_{n-1}, a_n) = (1)$, which is a contradiction. Thus $a_{n-1} \not\equiv 0 \bmod \mathfrak{p}_i$ when $a_n \equiv 0 \bmod \mathfrak{p}_i$.

Since the $\mathfrak{p}_i$'s are maximal ideals in A, by the Chinese remainder theorem we can find $b \in A$ with $b \equiv b_i \bmod \mathfrak{p}_i$ for all i. (In case $\mathfrak{p}_i = \mathfrak{p}_j$ for some $i \neq j$, we should take care to choose b_i and b_j to be equal in A, which is possible since the conditions constraining b_i and b_j — $a_{n-1} + b_i a_n \not\equiv 0 \bmod \mathfrak{p}_i$ and $a_{n-1} + b_j a_n \not\equiv 0 \bmod \mathfrak{p}_j$ — are the same.) Then for all i, $a_{n-1} + ba_n \equiv a_{n-1} + b_i a_n \not\equiv 0 \bmod \mathfrak{p}_i$. So the principal ideal $(a_{n-1} + ba_n)$ is not contained in any $\mathfrak{p}_i$ We claim the ideal $(a_1, \ldots, a_{n-2}, a_{n-1} + ba_n)$ equals (1). Indeed, if $(a_1, \ldots, a_{n-2}, a_{n-1} + ba_n) \neq (1)$ it lies in some maximal ideal $\mathfrak{p}$. Then $(a_1, \ldots, a_{n-2}) \subset \mathfrak{p}$, so $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$. This implies $\mathfrak{p} = \mathfrak{p}_i$ for some i since $\mathfrak{p}$ is prime and all $\mathfrak{p}_i$ are maximal. However, $a_{n-1} + ba_n \equiv 0 \bmod \mathfrak{p}$ and by construction $a_{n-1} + ba_n \not\equiv 0 \bmod \mathfrak{p}_i$. So having $\mathfrak{p} = \mathfrak{p}_i$ for some i is a contradiction. □

Remark 5. We insist that $n \geq 3$ and that one of $a_1, \ldots, a_{n-2}$ is nonzero in the hypothesis of Lemma 4 because the lemma is false with $n = 2$, *i.e.*, if $(a, a') = (1)$ there might not be any $b \in A$ such that $(a + ba') = (1)$. For instance, let $A = \mathbf{Z}[\sqrt{d}]$ for nonsquare $d \leq -2$, $a = 1 + \sqrt{d}$, and $a' = d$. (Further take $d \equiv 2, 3 \bmod 4$ to be sure A is Dedekind.) Then $(1 + \sqrt{d}, d) = (1)$ but if there were $b \in \mathbf{Z}[\sqrt{-5}]$ such that $(1 + \sqrt{d} + bd) = (1)$ then $1 + \sqrt{d} + bd = \pm 1$. Writing $b = k + \ell\sqrt{d}$ with k and ℓ in $\mathbf{Z}$, we have $1 + dk = \pm 1$ and $1 + d\ell = 0$. The second equation has no integral solution.

Now we prove Theorem 2.

Proof. The theorem is symmetric in the a_i's, since we can create any permutation of the a_i's in the top row of a matrix using a permutation of the columns of the matrix. This will yield a new matrix with top row permuted as intended and determinant ± 1. If the determinant is -1 then we can make another matrix with determinant 1 and the same (permuted) top row. by scaling the entries of a row besides the first by -1.

If $(a_1, \ldots, a_n) = (1)$ and only one a_i is nonzero, without loss of generality (by the previous paragraph) it is a_1 which is nonzero. Then $a_1 \in A^\times$, so the diagonal matrix

$\mathrm{diag}(a_1, 1/a_1, 1, \ldots, 1)$ is in $\mathrm{SL}_n(A)$ and has first row $[a_1, 0, \ldots, 0] = [a_1, a_2, \ldots, a_n]$. If $(a_1, \ldots, a_n) = (1)$ and only two a_i's are nonzero then without loss of generality a_1 and a_2 are nonzero. Then $(a_1, a_2) = (1)$, so $a_1x + a_2y = 1$ for some x and y in A. Therefore $M = \left(\begin{smallmatrix} a_1 & a_2 \\ -y & x \end{smallmatrix}\right)$ lies in $\mathrm{SL}_2(A)$ and the block matrix $\left(\begin{smallmatrix} M & O \\ O & I_{n-2} \end{smallmatrix}\right)$ is in $\mathrm{SL}_n(A)$ with first row $[a_1, a_2, 0, \ldots, 0] = [a_1, a_2, a_3, \ldots, a_n]$. This argument, in particular, verifies the theorem when $n = 2$.

Now take $n \geq 3$ and assume the theorem has been proved for any $n-1$ elements in A which generate the unit ideal. If $(a_1, \ldots, a_{n-1}, a_n) = (1)$, we may assume by the previous paragraph that at least three of the a_i's are nonzero. By symmetry of the theorem in the a_i's, we can take a_{n-1} and a_n nonzero. At least one of $a_1, \ldots, a_{n-2}$ is nonzero, so Lemma 4 tells us $(a_1, \ldots, a_{n-2}, a_{n-1} + ba_n) = (1)$ for some $b \in A$. Then the inductive hypothesis implies $[a_1, \ldots, a_{n-2}, a_{n-1} + ba_n]$ is the first row of a matrix $M \in \mathrm{SL}_{n-1}(A)$. Note that

$$[a_1, a_2, \ldots, a_n] \begin{pmatrix} I_{n-2} & O & O \\ O & 1 & 0 \\ O & b & 1 \end{pmatrix} = [a_1, \ldots, a_{n-2}, a_{n-1} + ba_n, a_n],$$

where the $n \times n$ matrix on the left is clearly in $\mathrm{SL}_n(A)$. The vector on the right side of this equation is the first row of the matrix

$$\begin{pmatrix} M & * \\ O & 1 \end{pmatrix} \in \mathrm{SL}_n(A),$$

where $*$ is the column vector in A^{n-1} with top coordinate a_n and the remaining coordinates equal to 0. Therefore $[a_1, a_2, \ldots, a_n]$ times a matrix in $\mathrm{SL}_n(A)$ is the first row of a matrix in $\mathrm{SL}_n(A)$, so $[a_1, \ldots, a_n]$ is itself the first row of a matrix in $\mathrm{SL}_n(A)$ by Lemma 3. □

Remark 6. The reason Theorem 2 is stated for Dedekind domains is that these are the rings to which Lemma 4 applies. (Check that no other part of the proof of Theorem 2 uses the Dedekind property, *e.g.*, Lemma 3 is valid for all commutative rings.) But in fact the proof of Lemma 4 applies to a broader class of rings than Dedekind domains: it works when A is any Noetherian domain where all nonzero prime ideals are maximal (such as any order in a number field, not just the maximal order). Indeed, any nonzero ideal in such a ring contains – but might not equal – a product of nonzero prime ideals, and we can take $(a_1, \ldots, a_{n-2}) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ instead of $(a_1, \ldots, a_{n-2}) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ in the proof of Lemma 4. Then any maximal ideal $\mathfrak{p}$ containing $(a_1, \ldots, a_{n-2})$ has to be one of the $\mathfrak{p}_i$'s. Check with this change that the proof of Lemma 4 works for Noetherian domains in which all nonzero prime ideals are maximal, so Theorem 2 is valid for such rings.

There is an extension of Theorem 2 to more than one vector. Given $r \leq n$ vectors in A^n, if they are the first r rows of a matrix in $\mathrm{GL}_n(A)$ then the $r \times r$ minors of the $r \times n$ matrix formed from these (row) vectors will generate the unit ideal in A, as one sees by expanding an $n \times n$ determinant as a linear combination of the $r \times r$ minors along the top. The converse is also true for any ring A satisfying Theorem 2. A proof can be found in [2].

References

[1] I. Reiner, *Unimodular Complements*, Amer. Math. Monthly **63** (1956), 246–247.

[2] I. Reiner, *Completion of Primitive Matrices*, Amer. Math. Monthly **73** (1966), 380–381.

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

[4] E. Schenkman, *The Basis Theorem for Finitely Generated Abelian Groups*, Amer. Math. Monthly **67** (1960), 770–771.