

Introduction We will study matrices in reduced row-echelon form in some detail, and use the terms and notation we develop to prove that no matter how we go about reducing a matrix to reduced row-echelon form, the result will be the same. That is, $(A | I) \rightarrow (\text{rref} | M)$ will always result in the same rref matrix and nearly the same matrix M (if done correctly). Bretscher discusses this in Exercises 64 – 67, pp 133 – 134, Section 3.3.

We can show that if $(A | I) \rightarrow (R | M)$ and R is a reduced row-echelon form matrix, then $\ker A = \ker R$ (showing this could be on a test!).

We begin by studying an arbitrary matrix R of size $m \times n$ that is in rref form. We need to look at the entries of R , so we will sometimes write $R = (r_{ij})$, where $1 \leq i \leq m$ and $1 \leq j \leq n$. An important by-product of our study is an easy rule for writing down a basis for $\ker R$. Let's look at an example of an rref R_o :

$$R_o := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 & 4 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

R_o is 4×6 and it has 3 rows with leading ones. The columns with the leading ones are 1, 3 and 4. There is one zero column and one zero row. There are 2 non-leading non-zero columns.

When we work with an arbitrary R we'll set up some notation to describe it partially:

- We let ℓ denote the number of rows in R with leading ones. These rows are rows one thru ℓ . For R_o , $\ell = 3$.
- We define the set $L \subseteq \{1, 2, \dots, n\}$ to be the set of column numbers of the columns that contain leading ones, and we write $L = \{j_1, j_2, \dots, j_\ell\}$, where $j_1 < j_2 < \dots < j_\ell$. Thus column j_i has the “one” that is in row i . For R_o , whose $\ell = 3$, we have $j_1 = 1$, $j_2 = 3$, and $j_3 = 4$, so $L = \{1, 3, 4\}$
- We next define the set $N \subseteq \{1, 2, \dots, n\}$ to be the set of all the column numbers of non-leading columns. Thus $N = \{1, 2, \dots, n\} \setminus L$, so N has $n - \ell$ members. For R_o , $N = \{1, 2, 3, 4, 5, 6\} \setminus \{1, 3, 4\} = \{2, 5, 6\}$.

Let's suppose that $p \in N$. Then Re_p is the p -th column of R and $Re_p = \sum_{i=1}^m r_{ij}e_i$. **A key idea:** if $r_{ij} \neq 0$, there is a leading “one” in row i . This means that $e_i = Re_{j_i}$. In words, the column of R that has a 1 in row i is e_i and the column that contains that 1 is column j_i . In our example R_o , there is a 1 in row 2. That 1 is in column 3. Thus $R_o e_3 = e_2 = R_o e_{j_2}$ because $3 = j_2$ (this is tricky because we are “reading a definition backwards”).

We can exploit the observation that $e_i = Re_{j_i}$. We had $Re_p = \sum_{i=1}^m r_{ij}e_i$. We can rewrite this as

$$Re_p = \sum_{\substack{i=1 \\ r_{ip} \neq 0}}^m r_{ip}e_i = \sum_{\substack{i=1 \\ r_{ip} \neq 0}}^m r_{ip}Re_{j_i},$$

and then as

$$R \left(e_p - \sum_{\substack{i=1 \\ r_{ip} \neq 0}}^m r_{ip}e_{j_i} \right) = 0.$$

In other words,

$$e_p - \sum_{\substack{i=1 \\ r_{ip} \neq 0}}^m r_{ip}e_{j_i} \in \ker R.$$

Since it is a nuisance to keep writing $r_{ip} \neq 0$, we will do this: even if $r_{ip} = 0$, we can still write $r_{ip}e_{j_i}$ because it's zero anyway, as long as there is a leading 1 in row i . This does not work, tho, if row i has no leading 1, which

is the case in our R_o when $i = 4$. But we can handle that case too, by letting $j_i = 0$ if row i has no leading 1 and by introducing the convention that $e_0 = 0$ (it's the column vector in \mathbb{R}^n that has zeroes in every row except the zero-th row. Since the zeroth row does not exist, $e_0 = 0$).

For example, if we look at $p = 5$ for R_o , we have (using these notions)

$$R_o e_5 = 0 \cdot e_1 + 3e_2 + 4e_3 + 0 \cdot e_4 = 0 \cdot R_o e_1 + 3R_o e_3 + 4R_o e_4 + 0 \cdot R_o e_0 = R_o(0 \cdot e_1 + 3e_3 + 4e_4 + 0 \cdot e_0).$$

Thus $R_o(e_5 - (3e_3 + 4e_4)) = 0$. In addition, $R_o e_2 = 0$ and $R_o(e_6 - (4e_1 + 2e_3 - e_4)) = 0$.

After all this defining, we can write, when $p \in N$, and knowing that $r_{ip} = 0$ if $i > \ell$,

$$(*) \quad R \left(e_p - \sum_{i=1}^{\ell} r_{ip} e_{j_i} \right) = 0, \quad \text{or: } z_p := e_p - \sum_{i=1}^{\ell} r_{ip} e_{j_i} \in \ker R \quad (\text{where we had } m \text{ before we can now put } \ell).$$

An important observation about (*): each j_i that has a non-zero r_{ip} is less than p . This is so because every non-zero entry in a non-leading column lies in a row with a leading one to its left, that is, with a *smaller* column number.

There is an “easy” way to write down the kernel vectors z_p defined in (*), but it involves a lot of not quite necessary writing: place an $n \times n$ identity matrix under R and perform *column* operations on the combined matrix $\begin{pmatrix} R \\ I \end{pmatrix}$

to eliminate all the non-leading columns from R . The columns that lie below the zero columns in the new version of R will form a basis for the kernel of R . If you do this for our example matrix R_o , you'll see that these are precisely the vectors $z_p = e_p - \sum_{i=1}^m r_{ip} e_{j_i}$, constructed for each $p \in N$.

Now we will show that the vectors z_p form a basis for $\ker R$. There are two things to do: (1) Show that the vectors z_p form a linearly independent set, (2) Show that every element of the kernel of R is a linear combination of the vectors z_p .

(1) If $\sum_{p \in N} \alpha_p z_p = 0$ we want to show that all the $\alpha_p = 0$. Let us suppose not, and let K be the *last* p such that $\alpha_p \neq 0$, so that $\alpha_K \neq 0$ and $\alpha_p = 0$ if $p > K$.

Then

$$\alpha_K z_K = \alpha_K (e_K - \sum_{i=1}^m r_{iK} e_{j_i}) = - \sum_{p \in N, p < K} \alpha_p (e_p - \sum_{i=1}^m r_{ip} e_{j_i}).$$

Let's divide the equation by α_K and move the sum on the left over to the right:

$$z_K + \sum_{i=1}^m r_{iK} e_{j_i} = e_K = \sum_{i=1}^m r_{iK} e_{j_i} - \frac{1}{\alpha_K} \sum_{p \in N, p < K} \alpha_p (e_p - \sum_{i=1}^m r_{ip} e_{j_i}).$$

This is absurd (i.e., this is a contradiction) because every vector “ e_q ” on the right has subscript q less than K , and we know that the standard basis vectors can't be expressed as linear combinations of the *other* standard basis vectors. This proves that the vectors in (*) form a linearly independent set.

(2) We suppose now that $\hat{x} = \sum_{j=1}^n \hat{x}_j e_j \in \ker R$. We want to show that $\hat{x} = \sum_{p \in N} \beta_p (e_p - \sum_{i=1}^m r_{ip} e_{j_i})$ for (unique!) scalars β_p , $p \in N$. To begin, we can write (only changing notation)

$$\hat{x} = \sum_{j=1}^n \hat{x}_j e_j = \sum_{j \in L} \hat{x}_j e_j + \sum_{j \in N} \hat{x}_j e_j = \sum_{i=1}^{\ell} \hat{x}_{j_i} e_{j_i} + \sum_{p \in N} \hat{x}_p e_p.$$

Since $\hat{x} \in \ker R$,

$$(**) \quad 0 = R\hat{x} = \sum_{i=1}^{\ell} \hat{x}_{j_i} R e_{j_i} + \sum_{p \in N} \hat{x}_p R e_p = \sum_{i=1}^{\ell} \hat{x}_{j_i} e_i + \sum_{p \in N} \hat{x}_p \sum_{i=1}^m r_{ip} R e_{j_i} = \sum_{i=1}^{\ell} \hat{x}_{j_i} e_i + \sum_{p \in N} \hat{x}_p \sum_{i=1}^m r_{ip} e_i.$$

We can rearrange the double sum:

$$\sum_{p \in N} \hat{x}_p \sum_{i=1}^{\ell} r_{ip} e_i = \sum_{i=1}^{\ell} \left(\sum_{p \in N} \hat{x}_p r_{ip} \right) e_i.$$

Now we can combine the sums in the last term in (**):

$$0 = \sum_{i=1}^{\ell} \hat{x}_{j_i} e_i + \sum_{p \in N} \hat{x}_p \sum_{i=1}^{\ell} r_{ip} e_i = \sum_{i=1}^{\ell} \left(\hat{x}_{j_i} + \sum_{p \in N} \hat{x}_p r_{ip} \right) e_i.$$

Since the set of standard basis vectors in \mathbb{R}^m is linearly independent, $\hat{x}_{j_i} + \sum_{p \in N} \hat{x}_p r_{ip} = 0$ for each i . Thus $\hat{x}_{j_i} = -\sum_{p \in N} \hat{x}_p r_{ip}$ for each i , $1 \leq i \leq \ell$.

Now we can return to \hat{x} and make substitutions:

$$\hat{x} = \sum_{i=1}^{\ell} \hat{x}_{j_i} e_{j_i} + \sum_{p \in N} \hat{x}_p e_p = -\sum_{i=1}^{\ell} \sum_{p \in N} \hat{x}_p r_{ip} e_{j_i} + \sum_{p \in N} \hat{x}_p e_p = \sum_{p \in N} \hat{x}_p \left(e_p - \sum_{i=1}^{\ell} r_{ip} e_{j_i} \right),$$

so that \hat{x} is a linear combination of the basis vectors z_p shown in (*). We sought, and have found, numbers $\beta_p = \hat{x}_p$ for $p \in N$. Thus the kernel has a basis given by the vectors shown in (*).

Summary so far

We started with a matrix R in reduced row echelon form. We defined some quantities associated with R :

- The number ℓ of leading ones in the rows of R , and we noticed that these leading ones are in rows 1 thru ℓ , and that rows $\ell + 1$ thru m are zero rows.
- The set L of the column numbers of the ℓ columns that contain leading 1's. We also defined these column numbers as $j_1 < j_2 < \dots < j_{\ell}$, where j_i stands for the number of the column that has a leading one in row i . We noticed that $i \leq j_i$. For convenience we defined $j_0 = 0$ and $e_0 = 0$.
- The set N of the column numbers of the $n - \ell$ columns that do not contain leading 1's. We noticed that $N = \{1, 2, \dots, n\} \setminus L$.
- The basis vectors $z_p := e_p - \sum_{i=1}^{\ell} r_{ip} e_{j_i} \in \ker R$, where $p \in N$. Let us notice now that actually $z_p := e_p - \sum_{i=1}^{p-1} r_{ip} e_{j_i}$ because every r_{ip} with $i \geq p$ is zero (because a non-leading column can't have a non-zero entry on or below the main diagonal).

Analysis of the image of A .

Suppose we start with a matrix A and perform Elementary Row Operations on it: $(A | I) \rightarrow (R | M)$. Here is an example:

$$A_o = \begin{pmatrix} 1 & 0 & 1 & 0 & 3 & 6 \\ 2 & 0 & 2 & 1 & 10 & 11 \\ 3 & 0 & 3 & 1 & 13 & 17 \\ 4 & 0 & 3 & 1 & 13 & 21 \end{pmatrix}, \quad M_o = \begin{pmatrix} 0 & 0 & -1 & 1 \\ 0 & -1 & 2 & -1 \\ 0 & 3 & -2 & 0 \\ 1 & 1 & -1 & 0 \end{pmatrix}, \quad R_o = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 & 4 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix};$$

You should check that $M_o A_o = R_o$. If we multiply the last row of M_o by a non-zero scalar, for example 2, forming a matrix M_2 , we still will have $M_2 A_o = R_o$. Thus the matrix M is not unique. We will show that R is unique, however.

If $Ax = y$ (so that $y \in \text{Im } A$) then

$$y = M^{-1} R x = \sum_{j=1}^n x_j M^{-1} R e_j = \sum_{i=1}^{\ell} x_{j_i} A e_{j_i} + \sum_{p \in N} x_p M^{-1} R e_p.$$

We recall (from $(*)$) that when $p \in N$, $Re_p = R \sum_{i=1}^{\ell} r_{ip} e_{j_i}$. We now substitute this into the formula above for y and use the fact that $M^{-1}R = A$:

$$y = \sum_{i=1}^{\ell} x_{j_i} A e_{j_i} + \sum_{p \in N} x_p A \sum_{i=1}^{\ell} r_{ip} e_{j_i} = \sum_{i=1}^{\ell} \left(x_{j_i} + \sum_{p \in N} x_p r_{ip} \right) A e_{j_i},$$

so now we know that $y \in \text{span} \{A e_{j_i} : 1 \leq i \leq \ell\}$. In words, the image of A is the span of the columns of A that correspond to the columns of R that hold leading ones.

Let's multiply both sides of the last equation by M :

$$My = \sum_{i=1}^{\ell} \left(x_{j_i} + \sum_{p \in N} x_p r_{ip} \right) M A e_{j_i} = \sum_{i=1}^{\ell} \left(x_{j_i} + \sum_{p \in N} x_p r_{ip} \right) R e_{j_i} = \sum_{i=1}^{\ell} \left(x_{j_i} + \sum_{p \in N} x_p r_{ip} \right) e_i = \sum_{i=1}^{\ell} (My)_i e_i.$$

This equation tells us that $y = \sum_{i=1}^{\ell} (My)_i A e_{j_i} = A \sum_{i=1}^{\ell} (My)_i e_{j_i}$.

We want to know how to find the vectors x that solve the equation $Ax = b$. We know that one possibility is: no solution. For our example here is a b that yields no solutions: $(1, 2, 4, 3)$. We imagine calculating $M_o b$ and we look at the last entry of $M_o b$, which is $1 + 2 - 4 = -1 \neq 0$. But if $A_o x = b$, then $M_o A_o b = M_o b$ and $M_o A_o = R_o$, so then $M_o b = R_o b$. These vectors are not equal because their last entries do not agree: the last entry of $R_o b$ is 0 and the last entry of $M_o b$ is -1 .

On the other hand, if $b_o = (2, 1, 3, 4)$ then the last entry of $M_o b_o$ is zero, and we can conclude that a solution of $A_o x = b_o$ does exist.

Here is a procedure for analyzing the equation $Ax = b$ that comes out of what we have done so far:

- Calculate Mb . If its i th entry, $(Mb)_i$, is non-zero for some $i > \ell$, there is no solution; if every $(Mb)_i = 0$ when $i > \ell$, then there is a solution. Why?
- If it has been established that a solution exists, a "particular" solution, s_p , can be found using the (standard-basis) coordinates of Mb : is $s_p := \sum_{i=1}^{\ell} (Mb)_i e_{j_i}$. I.e., $As_p = b$.
- If it has been established that a solution exists, the "general" solution is $x = s_p + \sum_{j \in N} \gamma_j z_j$, where the z_j are the basis vectors for $\ker A = \ker R$ defined in $(*)$. Thus, if a particular solution exists, the solution set consists of a subspace of dimension $n - \ell$, shifted away from the origin by adding s_p to each member of the kernel.

The number we have been calling ℓ is usually called the "rank" of the matrix A . The rank of A_o is therefore 3.

For our example, $M_o b_o = (1, 1, -3, 0)$, so a solution exists.

Since $L = \{1, 3, 4\}$ our particular solution is $x_p = 1e_1 + 1e_3 + (-3)e_4$.

We have, from just before $(*)$, $z_2 = e_2$, $z_5 = e_5 - (3e_3 + 4e_4)$ and $z_6 = e_6 - (4e_1 + 2e_3 - e_4)$. Thus the general solution of $A_o x = b_o$ is

$$x = \begin{pmatrix} 1 \\ 0 \\ 1 \\ -3 \\ 0 \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t_2 \begin{pmatrix} 0 \\ 0 \\ -3 \\ -4 \\ 1 \\ 0 \end{pmatrix} + t_3 \begin{pmatrix} -4 \\ -2 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \text{ where } t_1, t_2 \text{ and } t_3 \text{ are arbitrary real numbers.}$$

The proof of the Theorem: two rref's are equal iff their kernels are equal

Now let us be given two matrices, R and \tilde{R} , both in rref form, both of size $m \times n$. We define the same quantities for \tilde{R} that we did for R but we denote them $\tilde{\ell}$, \tilde{L} , \tilde{N} , \tilde{z}_p (for $p \in \tilde{N}$). If $R = \tilde{R}$, certainly $\ker R = \ker \tilde{R}$.

Instead, let us suppose that $\ker R = \ker \tilde{R}$ and show that $R = \tilde{R}$ has to be true. Again we suppose not. Then there is a *first* k such that the k -th columns of R and \tilde{R} differ, and we call this K , so that $Re_K \neq \tilde{R}e_K$, but $Re_k = \tilde{R}e_k$ for all $k < K$, if any. There are four possibilities: (1) $K \in L$ and $K \in \tilde{L}$, (2) $K \in L$ and $K \in \tilde{N}$, (3) $K \in N$ and $K \in \tilde{L}$ and (4) $K \in N$ and $K \in \tilde{N}$. We will show that each of these possibilities leads to a contradiction, so no such K exists and thus $R = \tilde{R}$.

Suppose (1) is true. Let us recall that, as we look, left to right, thru the columns of R and \tilde{R} , each new column with a leading 1 uses the next available row as the location for that leading 1. Since $Re_k = \tilde{R}e_k$ for all $k < K$ the next row available for a leading 1 is the same for R and \tilde{R} (if $K = 1$ the next row available is row 1 for both). But then $Re_K = \tilde{R}e_K$, a contradiction. Hence possibility (1) cannot occur.

Suppose (2) is true. Since $K \in \tilde{N}$, $\tilde{z}_K \in \ker \tilde{R} = \ker R$. Thus since $\tilde{r}_{iK} = 0$ if $i \geq K$,

$$0 = R\tilde{z}_K = R \left(e_K - \sum_{i=1}^{\ell} \tilde{r}_{iK} e_{j_i} \right) = Re_K - \sum_{i=1}^{K-1} \tilde{r}_{iK} Re_{j_i} = e_K - \sum_{i=1}^{K-1} \tilde{r}_{iK} e_i \quad \text{or} \quad e_K = \sum_{i=1}^{K-1} \tilde{r}_{iK} e_i.$$

This is absurd, because e_K cannot be a linear combination of the vectors e_i with $i < K$. Hence possibility (2) cannot occur.

For the same reason (or by interchanging the rôles of R and \tilde{R}), possibility (3) cannot occur.

Suppose (4) is true. Then $Re_K \neq \tilde{R}e_K$. From (*) we know that

$$R \left(e_K - \sum_{i=1}^{\ell} r_{iK} e_{j_i} \right) = 0 = Re_K - \sum_{i=1}^{K-1} r_{iK} Re_{j_i} = Re_K - \sum_{i=1}^{K-1} r_{iK} e_i.$$

Since R and \tilde{R} have the same kernel, $\tilde{R} \left(e_K - \sum_{i=1}^{\ell} r_{iK} e_{j_i} \right) = 0$ as well. But then

$$0 = \tilde{R} \left(e_K - \sum_{i=1}^{\ell} r_{iK} e_{j_i} \right) = \tilde{R}e_K - \sum_{i=1}^{K-1} r_{iK} \tilde{R}e_{j_i} = \tilde{R}e_K - \sum_{i=1}^{K-1} r_{iK} e_i.$$

We see from the last terms of these equations that $Re_K = \tilde{R}e_K$. This is a contradiction, so possibility (4) cannot occur.

The proof is complete.

An application of the title Theorem

Suppose that we use Elementary Row Operations on a matrix A , following the scheme $(A | I) \rightarrow (R | M)$ or even the scheme $(A | b | I) \rightarrow (R | Mb | M)$ in case we have only one equation to solve, but want to be able to check our operations for correctness. Another person might do the same, obtaining $(A | I) \rightarrow (\tilde{R} | \tilde{M})$. We assume that $MA = R$ and that $\tilde{M}A = \tilde{R}$. Since we know that R and \tilde{R} have the same kernel, the Theorem tells us that $R = \tilde{R}$. The Theorem does not tell us that $M = \tilde{M}$, and this might not be true, as we have seen.