A First Course in Matrix Theory

by

Robert A. Mena
CSULB

Table of Contents

Preface

❶ Basic Concepts 1
❷ Matrix Stacking and Blocking 7
❸ Matrix Multiplication 11
❹ Stacking, Blocking & Matrix Multiplication 26
❺ Inverses 31
❻ Row Reduction & Linear Equations 42
❼ Rank & Systems 53
❽ Inequalities 64
❾ The Geometry of Vectors 69
❿ The Subspaces of a Matrix 79
❶❶ The Notion of Dimension 91
❶❷ Matrices as Transformations 102
❶❸ Determinants & Adjoints 116
❶❹ The Need for Eigenvalues 127
❶❺ Triangularization & Diagonalization 140
❶❻ Symmetric and Orthogonal Matrices 153

On Conics 165

Appendix of Proofs 173

Index 194

Preface

This is a course about matrices. Specifically it is about matrices whose entries are real numbers—however the vast majority of the theorems are still true when one extends the discussion to matrices with complex numbers as entries. In fact, once one adjusts transposes to be conjugate transposes, then all theorems would be available. The reason for the restriction is that one cannot assume that students, mainly sophomores, have prior understanding of the complex number, and to make their background adequate would take too much time away from the matrix material.

Fortunately, since the material is not burdened by the subtleties required for the definition and existence of the continuum, one can be more fully rigorous in the presentation. Thus rigor—not abstraction, is pursued throughout the course. Clarification was necessary since abstraction is often mistaken for rigor in mathematical discussions. For example, abstract vector spaces are not introduced; instead, some interesting ones in terms of matrices are discussed. Linear transformations are viewed simply as matrices. It is believed that once the student is ready for more abstract understanding, the jump can readily be made from the material presented.

On the other hand, all proofs required, except for the Fundamental Theorem of Algebra on the existence of roots of polynomials, are presented in the text. Nevertheless, some of the more intricate, or technical, or just plain pesky, proofs are left for the Appendix of Proofs.

❶ Basic Concepts

This is a course about **matrices**—or **hyper numbers** as they were once called. They have become so pervasive in modern mathematics and related fields, that many high school curricula now include them, while barely 50 years ago, matrices were only taught to upper division mathematics majors.

A matrix is a simple notion—it is a rectangular array of numbers, usually encased in parentheses such as $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ or $\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$. More generally, **one could state that a matrix is a rectangular array of objects**, since later on we will talk of matrices as being made up of matrices themselves. Partly, it is this ability to think recursively about them that makes matrices powerful. For example, $\begin{pmatrix} 1 & 2 & 5 & 6 \\ 3 & 4 & 7 & 8 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$ can also be viewed as $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{C} \end{pmatrix}$ where **A** is standing for $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, **B** for $\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$, **0** is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, and **C** for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

The **size** of a matrix is always given in the form the number of **rows** (first) by the number of **columns**. Thus, $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ is a 2×3 matrix since it has 2 rows and 3 columns. Capital bold letters such as $\mathbf{A}$ will denote **matrices**. Naturally, then when we say $\mathbf{A}$ is $m\times n$, we mean that it has m rows and n columns. A matrix **A** is **square** if it has the same number of rows as columns, such as an $n\times n$ matrix. The matrix $\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$ is square since it is a 3×3 matrix.

A matrix with only one column will often be referred to as a **(column) vector**. Depending on the author, books often referred to either **column vectors** or **row vectors** as **vectors**. But we will be consistent and mean by a vector a column vector. Non-capital bold letters, such as $\mathbf{u}$, will denote **vectors**, *e.g.*, $\mathbf{u}=\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ is a vector of size 3. This does not mean that **A** could not stand for a vector, since every vector is a matrix—it is just that if we use lower case letters, then we definitely know that we have a vector.

Non-capital, non-bold (italic) letters will denote **scalar** quantities, which is another way to refer to numbers in our course. For the time being, if not throughout the course, scalars will be real numbers, *e.g.*, $a = 2$.

A matrix has entries in positions, which are described by row first and then column, thus the entry in the $1,3-$position of the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ is a 3 while the $2,1-$position has a 4. It is customary (among civilized people) to read matrices by rows, so the matrix above would be read 1, 2, 3, 4, 5 and 6 once the size is established. Of particular importance are the main diagonal positions: $1,1-$, $2,2-$, $3,3-$, etc. In a square matrix, this set of positions is called the **main diagonal**. Thus the matrix $\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$ has 1, 5 and 9 in its main diagonal.

If one needs to refer to a position in a matrix abstractly, then one uses the index notation. For example, a_{23} indicates the entry in the $2,3-$position of the matrix $\mathbf{A} = (a_{ij})$.

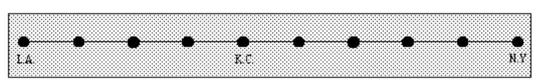
We will use $\mathbf{0}$ to denote a **zero matrix** (or vector) of the necessary size all of whose entries are 0. If the size needs to be clarified, one uses index notation, for example $\mathbf{0}_{2\times 3}$ denotes a 2×3 matrix of all zeroes. If only one index is used, such as $\mathbf{0}_3$, it denotes a square matrix of that size.

The following four examples illustrate **matrices as useful in storing information.**

Example 1. **Inventory.** Let us suppose we are the owners of a small car dealership that sells two brands of cars, **Hondas** (*H*) and **Toyotas** (*T*), and three models for each of the brands, **Sedans** (*S*), **SUV**'s (*V*) and **Coupes** (*C*). Then inventory can easily be stored in a 2×3 matrix where the rows are indexed by the brands and the columns are indexed by the models:

$$\mathbf{V} = \begin{array}{c} \\ H \\ T \end{array} \begin{array}{c} \begin{array}{ccc} S & V & C \end{array} \\ \begin{pmatrix} 5 & 3 & 2 \\ 8 & 4 & 1 \end{pmatrix} \end{array}$$

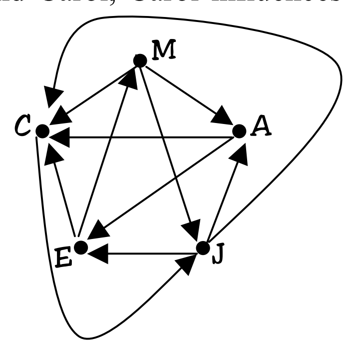
Example 2. **Communication Networks.** Consider the very simple communication network among 10 cities, Los Angeles, New York and Kansas City among them, represented by the following graph. The 10 cities are the **vertices** or **nodes** of the graph, represented by dots. The lines represent the direct linkages between the cities, and they are known as the **edges** of the graph.



For any such graph, we can capture all the information it contains by the use of its **adjacency matrix**. Specifically, consider the cities as indexing the rows of a matrix, and also the columns of a matrix, so we would be considering a 10×10 matrix. There is one important requirement, we have the freedom to label the rows any way we want to, but we are committed to keep the labeling of the columns to be the same. Each of the entries of the matrix is either a $\mathbf{0}$ or a $\mathbf{1}$. For a given row and a given column, we put a $\mathbf{1}$ in that position if the city indicated by the row will be linked directly to the city indicated by the column. Thus for our graph, or example, if were to consider the picture (or graph as it is called) on the left, and if we label the rows of the matrix starting with **LA** and then consecutively until we arrive at **NY**, then the matrix is given by For example, if were to consider the picture (or graph as it is called) on the left, and if we label the rows of the matrix starting with **LA** and then consecutively until we arrive at **NY**, then the matrix is given by $\begin{pmatrix} 0&1&0&0&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0&0&0 \\ 0&1&0&1&0&0&0&0&0&0 \\ 0&0&1&0&1&0&0&0&0&0 \\ 0&0&0&1&0&1&0&0&0&0 \\ 0&0&0&0&1&0&1&0&0&0 \\ 0&0&0&0&0&1&0&1&0&0 \\ 0&0&0&0&0&0&1&0&1&0 \\ 0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&1&0 \end{pmatrix}$. Note all of its entries are 0 or 1 so it is known as a $(0,1)-$ matrix.

Closely associated with the previous example is the following

Example 3. Influence Networks. Suppose that among 5 people the following influence patterns hold: Mark influences Alison, Carol and Jason, on the other hand Alison influences Emma and Carol, while Emma influences Mark and Carol, Carol influences Jason, and Jason influences Alison, Carol and Emma. We can represent this information via a directed graph, which is just like a graph except that now the lines connecting the vertices are actually arrows since they may have a direction.



But again we can encapsulate the information in a 5×5 adjacency matrix. If we list our vertices alphabetically, we get the following matrix: $\begin{pmatrix} 0&1&1&0&0 \\ 0&0&0&1&0 \\ 0&1&0&0&1 \\ 1&1&1&0&0 \\ 1&1&0&1&0 \end{pmatrix}$.

Example 4. Dinner Arrangements. As a prosperous, urban, young professional you are interested in showing off both your possessions and your acquaintances. Therefore you have a scheme of inviting your friends to dinner so they can get acquainted with each other, and with your apartment. Your brand new dining room table holds at most 4 hence you can have a maximum of 3 guests any one night. What you are trying to compute is the least number of nights you are going to have guests in order for any two of your friends to have at least one dinner together in your apartment. At present you consider you have 6 friends you would like to have over for dinner.

In this case, you have $\binom{6}{2} = 15$ pairs to entertain, and any one night you can take care of $\binom{3}{2} = 3$ pairs. It will take at least 5 nights. But can it be done in 5 nights? As a help in our tribulations, let's build a matrix with the following idea in mind: the rows of the matrix are indexed by your friends, so there are 6 rows; the columns of the matrix are indexed by the nights of entertaining, so there are 5 columns. The entries of the matrix are either **0**'s or **1**'s. For a given row and a given column, we put a **1** in that position if the friend indicated by that row is coming to dinner the night indicated by the column, otherwise we put a **0**. Thus, every column has at most 3 **1**'s (so in total there can only be at most 15 **1**'s in the matrix). How about each row? In one night, you can take care of friend A with B & C. In another night, A can come with D & E. But that means A has to come a third night since he has not had dinner with F. That means every row has to have at least 3 ones, so there would have to be at least 18 ones in the matrix, which means your scheme cannot be done in 5 nights.

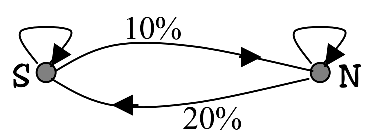
How about 6 nights? Pursuing the idea of the matrix, which paid off in the previous consideration, we now have a 6×6 matrix. Every column has at most 3 ones, and every row has at least 3 ones, so it must be that every row and column has exactly 3 ones. It does not take a long time to come up with a (basically unique) set up:

$$\begin{array}{c} \\ \mathsf{A} \\ \mathsf{B} \\ \mathsf{C} \\ \mathsf{D} \\ \mathsf{E} \\ \mathsf{F} \end{array} \begin{array}{c} \begin{array}{cccccc} \mathbf{m} & \mathbf{t} & \mathbf{w} & \mathbf{t} & \mathbf{f} & \mathbf{s} \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

which is acceptable. Such a matrix is called an **incidence matrix** for the arrangement.

One disadvantage (if we want to call it that) is that some friends are going to have dinner together twice (A&B on **monday** & **tuesday**, C&D on **friday** & **saturday**, and E&F on **wednesday** & **thursday**).

Example 5. Transition Processes. Every year, 10% of the people in Southern California move to Northern California while 20% of the people from Northern California move to Southern California. In this case, our digraph is very simple:



We build a matrix in a very similar fashion to what we did when doing the digraphs—except that now rather than 0's and 1's, we will use the probabilities as the entries in the matrix. Thus, for example, in the $1-2$ position, we will put the probability of going from situation 1 to situation 2. Thus, if we let 1 be Southern California and 2 be Northern California, our matrix would be $\mathbf{A} = \begin{pmatrix} 0.9 & 0.1 \\ 0.2 & 0.8 \end{pmatrix}$. This matrix is called the **transition matrix**.

The two most basic operations on matrices are that of **addition** (or **subtraction**), and **scalar multiplication**.

Two matrices can be added (or subtracted) exactly when their sizes are the same, and then the addition (subtraction) is simply accomplished by adding (subtracting) the corresponding entries.

Any matrix can be multiplied by any scalar,
where every entry of the matrix is multiplied by the given scalar.

Example 1 Revisited. Returning to the car dealership example, where our inventory of cars was represented by the matrix $\mathbf{V}=\begin{pmatrix}5 & 3 & 2\\ 8 & 4 & 1\end{pmatrix}$. Suppose we were to get a shipment of cars, which, of course, is also represented by a 2×3 matrix, $\mathbf{S}=\begin{pmatrix}5 & 2 & 3\\ 1 & 3 & 3\end{pmatrix}$. Then the new inventory, $\mathbf{N}$, would be represented by the sum of the two matrices, $\mathbf{N}=\mathbf{V}+\mathbf{S}=\begin{pmatrix}10 & 5 & 5\\ 9 & 7 & 4\end{pmatrix}$.

On the other hand, if we had sales for the following month as given by $\mathbf{L}=\begin{pmatrix}1 & 2 & 0\\ 3 & 0 & 1\end{pmatrix}$, then the new inventory would be $\mathbf{M}=\mathbf{N}-\mathbf{L}=\begin{pmatrix}9 & 3 & 5\\ 6 & 7 & 3\end{pmatrix}$.

Similarly, suppose we wanted to double our inventory, then $2\mathbf{V}=\begin{pmatrix}10 & 6 & 4\\ 16 & 8 & 2\end{pmatrix}$, which naturally is nothing but $\mathbf{V}+\mathbf{V}$.

There are basically no differences between addition of matrices and addition of numbers, nor are there any differences between scalar multiplication of matrices and multiplication of numbers, and thus, one is not likely to commit any errors when performing these operations.

One does, however, need to keep in mind
the required uniformity of sizes before addition can be performed.

But with this obvious requirement met, one can assume the following easily recognizable properties of numbers:

$\mathbf{A}+\mathbf{B}=\mathbf{B}+\mathbf{A}$ commutativity of addition
$\mathbf{A}+(\mathbf{B}+\mathbf{C})=(\mathbf{A}+\mathbf{B})+\mathbf{C}$ associativity of addition

$\mathbf{A}+\mathbf{0}=\mathbf{A}$	zero matrix
$\mathbf{A}+(-\mathbf{A})=\mathbf{0}$	negatives
$a(\mathbf{A}+\mathbf{B})=a\mathbf{A}+a\mathbf{B}$	distributivity of scalar multiplication
$(a+b)\mathbf{A}=a\mathbf{A}+b\mathbf{A}$	distributivity of scalar multiplication

An easy consequence of these properties is the following **cancellation** property:

if $\mathbf{A}+\mathbf{C}=\mathbf{B}+\mathbf{C}$, then $\mathbf{A}=\mathbf{B}$.

The proof is easy: given that $\mathbf{A}+\mathbf{C}=\mathbf{B}+\mathbf{C}$, then by adding $-\mathbf{C}$ to both sides one obtains the conclusion.

We have just discussed to operations on matrices that are inherently equivalent to similar operations on numbers—but in the next section we take advantage of the matrix idea, and definitely do something that is not usually done with numbers.

❷ Matrix Stacking and Blocking

If $\mathbf{A}$ and $\mathbf{B}$ are matrices (including the possibility of vectors), then we can perhaps make new matrices by stacking them either horizontally or vertically.

More precisely, suppose $\mathbf{A}$ is $m \times n$ and $\mathbf{B}$ is $p \times q$. Then if we are to make a new matrix by **stacking** them horizontally, $\begin{pmatrix} \mathbf{A} & \mathbf{B} \end{pmatrix}$, then what is necessary (and also obviously sufficient) is that they have the same number of rows, in other words, $m = p$, and then the resulting matrix would be of size $m \times (n+q)$. Thus if $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$, then $\begin{pmatrix} \mathbf{A} & \mathbf{B} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 7 \\ 3 & 4 & 8 \\ 5 & 6 & 9 \end{pmatrix}$.

But we can also stack matrices vertically $\begin{pmatrix} \mathbf{A} \\ \mathbf{C} \end{pmatrix}$, and then what is needed is that they have the same number of columns, $n = q$, and then the resulting matrix is of size $(m+p) \times n$. *E.g.*, if $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ and $\mathbf{C} = \begin{pmatrix} 7 & 8 \end{pmatrix}$, then $\begin{pmatrix} \mathbf{A} \\ \mathbf{C} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{pmatrix}$.

One common occurrence of horizontal stacking is that of making a matrix out of a collection (ordered) of vectors, from $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ each of size *m*, we can make the $m \times n$ matrix $\mathbf{A} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$. Or equivalently, one can think of a matrix as the (horizontal) stack of its columns.

We will use $\mathbf{A}^{\mathrm{T}}$ to denote the **transpose** of the matrix $\mathbf{A}$. This is the matrix obtained from $\mathbf{A}$ by switching the role of rows and columns, hence the first row becomes the first column, and the second row becomes the second column, etcetera. Thus, for example, $\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}$. In particular, the transpose of a (column) vector $\mathbf{u}$ is a row vector, $\mathbf{u}^{\mathrm{T}}$. In general, if $\mathbf{A}$ is $m \times n$, then $\mathbf{A}^{\mathrm{T}}$ is of size $n \times m$.

Naturally, the transpose of a square matrix is a square matrix of the same size, but it may be a different matrix.

If, however, $\mathbf{A} = \mathbf{A}^{\mathrm{T}}$, then the matrix is called **symmetric**. Note, *e.g.*, that the adjacency matrix in the communication network example above was symmetric since all communication was two-way. But in the following example, the influence network, the matrix was not symmetric. In fact, the transpose matrix in that example would be interpreted as **being influenced by** rather that **influence**.

It is easy to see that as long on either side makes sense,

$$(\mathbf{A}+\mathbf{B})^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}} + \mathbf{B}^{\mathrm{T}},$$

namely

the transpose of a sum is the sum of the transposes.

And easily $(a\mathbf{A})^{\mathrm{T}} = a\mathbf{A}^{\mathrm{T}}$.

Similarly to the horizontal stacking of columns above, from row vectors, $\mathbf{v}_1^{\mathrm{T}}, \mathbf{v}_2^{\mathrm{T}}, \ldots, \mathbf{v}_m^{\mathrm{T}}$, all of size n, we can stack them vertically, to obtain an $m \times n$ matrix $\begin{pmatrix} \mathbf{v}_1^{\mathrm{T}} \\ \mathbf{v}_2^{\mathrm{T}} \\ \vdots \\ \mathbf{v}_m^{\mathrm{T}} \end{pmatrix}$. Or, again any matrix can be thought of as the vertical stacking of its rows.

There are two special stacking constructions of matrices that work for any size matrices. They will not play much of a role in our course, but since they are easily described, and they perhaps may be important in later courses, we use them as an example of further stackings.

Example 1. Direct Sums & Tensor Products. Suppose $\mathbf{A}$ is $m \times n$ and $\mathbf{B}$ is $p \times q$. Then their **direct sum** $\mathbf{A} \oplus \mathbf{B}$ is given by then $(m+p)\times(n+q)$ matrix that looks like $\begin{pmatrix} \mathbf{A} & \mathbf{0}_{m\times q} \\ \mathbf{0}_{p\times n} & \mathbf{B} \end{pmatrix}$.

For example, let $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} a & b \end{pmatrix}$, then $\mathbf{A} \oplus \mathbf{B} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 5 & 6 & 0 & 0 \\ 0 & 0 & a & b \end{pmatrix}$. One can think of direct sums as a **diagonal stacking**. An easy, yet useful fact is that if $\mathbf{A}+\mathbf{C}$ makes sense, and $\mathbf{B}+\mathbf{D}$ makes sense, then $(\mathbf{A}\oplus\mathbf{B})+(\mathbf{C}\oplus\mathbf{D})$ makes sense and it equals

$$(\mathbf{A}\oplus\mathbf{B})+(\mathbf{C}\oplus\mathbf{D}) = (\mathbf{A}+\mathbf{C})\oplus(\mathbf{B}+\mathbf{D}).$$

A different construction is given by tensor products, which is abstractly described as follows if $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{jk})$, then their **tensor product** $\mathbf{A}\otimes\mathbf{B}$ is given by

$$\mathbf{A}\otimes\mathbf{B}=\begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \cdots & a_{2n}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & a_{m2}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{pmatrix}.$$

Observe that the size of the tensor product is then given by $mp\times nq$.

For example, let $\mathbf{A}=\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ and $\mathbf{B}=\begin{pmatrix} a & b \end{pmatrix}$, then $\mathbf{A}\otimes\mathbf{B}=\begin{pmatrix} a & b & 2a & 2b \\ 3a & 3b & 4a & 4b \\ 5a & 5b & 6a & 6b \end{pmatrix}$. Observe that the tensor product of a scalar and a matrix is nothing but the scalar product.

Just as we took the direct sum of two matrices we could have taken the direct sum of arbitrarily many matrices, and the same applies for the tensor product.

A direct sum of 1×1 matrices (or scalars) is a **diagonal** matrix since all of its non-main diagonal entries are 0. A matrix that has zeroes below the main diagonal is called **upper triangular** while those that have zeros above the main diagonal are called **lower triangular**. These are naturally reserved for square matrices. For example, $\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$ is diagonal, while $\begin{pmatrix} 3 & 2 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 3 & 0 \\ 1 & 4 \end{pmatrix}$ are triangular, upper and lower respectively.

So far we have been stacking matrices, namely from smaller pieces we have been manufacturing larger matrices. But the reverse process is just as easy and valid. We will refer to it as blocking a matrix, but there are other names in the literature for decomposition of matrices into blocks. In fact any matrix can be broken into pieces by just grouping collection of rows and columns.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example 2. Consider the 10×10 matrix on the right as being broken into blocks of our choosing. One such partition is as follows: $\begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \mathbf{A}_{13} & \mathbf{A}_{14} \\ \mathbf{A}_{21} & \mathbf{A}_{22} & \mathbf{A}_{23} & \mathbf{A}_{24} \\ \mathbf{A}_{31} & \mathbf{A}_{32} & \mathbf{A}_{33} & \mathbf{A}_{34} \\ \mathbf{A}_{41} & \mathbf{A}_{42} & \mathbf{A}_{43} & \mathbf{A}_{44} \end{pmatrix}$ where the diagonal blocks are as follows: $\mathbf{A}_{11}=(1)=\mathbf{A}_{44}$, $\mathbf{A}_{22}=\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $\mathbf{A}_{33}=\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$,

and hence we think of the matrix as partitioned in the following manner:

$$
\begin{array}{c|ccc|ccccc|c}
\mathbf{1} & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\hline
0 & \mathbf{1} & \mathbf{1} & \mathbf{0} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & \mathbf{1} & \mathbf{1} & \mathbf{0} & 0 & 1 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 \\
0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 0 \\
0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1}
\end{array}
$$

Of course the decomposition could have been arbitrary just as long as we decompose into rectangles. In this particular case, we have a **balanced block decomposition** because all of the diagonal blocks are square.

Note that one of the advantages of block decompositions is the ability to consider the partitioned matrix as (block) upper triangular since every block below the main diagonal is a **0** block.

So, in this section we have learned to view matrices as arrays of matrices—and we have seen that we have freedom on how to partition or how to stack, and some judgment is required when doing so—we will keep exploring this throughout the course.

But now we look at the most fundamental operation on matrices: **multiplication**.

❸ Matrix Multiplication

The basic ingredient in matrix multiplication, that great contribution from the nineteenth century, is the product of a row times a column. It is simple, but powerfully recursive:

$$\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix}=\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n$$

It makes sense as long as $\alpha_i\beta_i$ makes sense for all $i=1,\ldots,n$ (the n is, of course, arbitrary), and as long as we can add the resulting products. Observe the very important requirement

> **that the number of rows in the column has to be the same as the number of columns in the row.**

Example 1. The simplest and best-known example of this is simply a row vector of numbers times a column vector of numbers,

$$\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}a\\ b\\ c\\ d\end{pmatrix}=1a+2b+3c+4d\,.$$

This important operation developed first as a vector with vector operation, and it is usually encountered first as the important **dot product** of two vectors: in fact if $\mathbf{u}=\begin{pmatrix}1\\ 2\\ 3\\ 4\end{pmatrix}$ and $\mathbf{v}=\begin{pmatrix}a\\ b\\ c\\ d\end{pmatrix}$, then one defines their dot product by

$$\mathbf{u}\cdot\mathbf{v}=1\cdot a+2\cdot b+3\cdot c+4\cdot d\,.$$

Observe that from the matrix point of view this would be written as $\mathbf{u}^{\mathrm{T}}\mathbf{v}$ (without the dot since juxtaposition denotes matrix multiplication), so

$$\mathbf{u}\cdot\mathbf{v}=\mathbf{u}^{\mathrm{T}}\mathbf{v}\,.$$

But how do we multiply two matrices **A** and **B**? Suppose simply as in the following example that **A** has just two rows and **B** has only one column—so we are in fact very close to the example above, then we multiply each row of **A** by the column of **B**.

Example 1 Revisited Again. This example should provide evidence for the reasons behind matrix multiplication. As before suppose the inventory is given by the matrix

$\mathbf{V} = \begin{pmatrix} 5 & 3 & 2 \\ 8 & 4 & 1 \end{pmatrix}$, and suppose that the price of a sedan is 15 (in thousands of dollars), of an *SUV* is 24 and that of a coupe is 18. Then the amount of inventory in Hondas is given by the first entry of the product $\begin{pmatrix} 5 & 3 & 2 \\ 8 & 4 & 1 \end{pmatrix}\begin{pmatrix} 15 \\ 24 \\ 18 \end{pmatrix} = \begin{pmatrix} 183 \\ 234 \end{pmatrix}$, so the dealership has \$183,000 in Honda inventory and \$234,000 in Toyotas.

In general, suppose **A** is $m \times n$ and **B** is $p \times q$. We think of the first one, **A**, as the vertical stacking of its rows while the second one, **B**, as the horizontal stacking of its columns. Then we take **the product of every row of the first factor times any column of the second one**. But in order for us to be able to multiply a row of **A** with a column of **B**, we must have agreement of size of a row with a column, namely, we must have that

$$n = p\,.$$

In other words, in order to be able to multiply two matrices,

the number of columns of the first factors has to be the same as the number of rows of the second factor.

In symbols, if we let $\mathbf{A} = \begin{pmatrix} \mathbf{v}_1^{\mathrm{T}} \\ \mathbf{v}_2^{\mathrm{T}} \\ \vdots \\ \mathbf{v}_m^{\mathrm{T}} \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_q \end{pmatrix}$, then

$$\mathbf{AB} = \begin{pmatrix} \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_1 & \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_2 & \cdots & \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_q \\ \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_1 & \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_2 & \cdots & \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_q \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_1 & \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_2 & \cdots & \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_q \end{pmatrix}.$$

So their product is of size $m \times q$, the number of rows of the first factor by the number of columns of the second factor. And in short, what is the $i-j$-entry of the product, the dot product of i^{th} row of the first factor with the j^{th} column of the second factor.

Example 2. We do a simple numerical example: let $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, and let $\mathbf{B} = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$.

Note that $\mathbf{AB}$ makes sense, and it will be of size 2×2: $\mathbf{AB} = \begin{pmatrix} a + 2c + 3e & b + 2d + 3f \\ 4a + 5c + 6e & 4b + 5d + 6f \end{pmatrix}$.

But also $\mathbf{BA}$ makes sense, but it is 3×3: $\mathbf{BA} = \begin{pmatrix} a + 4b & 2a + 5b & 3a + 6b \\ c + 4d & 2c + 5d & 3c + 6d \\ e + 4f & 2e + 5f & 3e + 6f \end{pmatrix}$.

This example illustrates one of the most shocking features of matrix multiplication:
the order of multiplication matters.

And in that example it was patently obvious since the sizes of **AB** and **BA** were different. But in the next example, we see that there are deeper issues than just size.

Example 3. Let $\mathbf{A}=\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$ and let $\mathbf{B}=\begin{pmatrix}1 & -1\\ 1 & -1\end{pmatrix}$. Then $\mathbf{AB}=\begin{pmatrix}2 & -2\\ 2 & -2\end{pmatrix}$, but $\mathbf{BA}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$, and we have two very worthwhile observations:

- first **AB** and **BA** may be different even if their sizes are the same.
- a product, **BA** in our case, can be **0** without either of them being **0**.

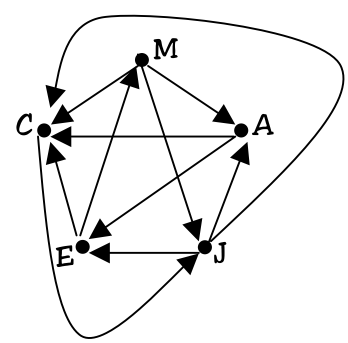
Neither of these occurs when considering multiplication of numbers.

So far we have stressed the rows of the first factor times the columns of the second factor way of viewing matrix multiplication—but there are also some other very useful ways to view matrix multiplication. The most elemental way to view matrix multiplication abstractly is the entries-of-the-matrix way. Namely, let **A** be $m\times n$, **B** be $n\times p$, so that $\mathbf{M}=\mathbf{AB}$ will be $m\times p$. Suppose $\mathbf{A}=\left(a_{ij}\right)$, $\mathbf{B}=\left(b_{jk}\right)$ and $\mathbf{M}=\left(m_{ik}\right)$, then we can simply state that

$$m_{ik}=a_{i1}b_{1k}+a_{i2}b_{2k}+\cdots+a_{in}b_{nk}=\sum_{l=1}^{n}a_{il}b_{lk}\ .$$

Observe that if a matrix **A** is to be multiplied by itself, it is necessary and sufficient that the matrix be square since the number of rows of the second factor has to be the same as the number of columns of the first factor. Of course, one refers to **A** times **A**, $\mathbf{AA}$, by $\mathbf{A}^2$ and calls it the **square** of **A**, or **A** squared.

Example 3 Revisited. Let us return to the influence network where the adjacency matrix was given by $\mathbf{A}=\begin{pmatrix}0 & 1 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 1\\ 1 & 1 & 1 & 0 & 0\\ 1 & 1 & 0 & 1 & 0\end{pmatrix}$.



Note that since **A** is 5×5 we can in fact compute $\mathbf{M}=\mathbf{A}\times\mathbf{A}=\mathbf{A}^2$.

We can ask what would be the meaning to the square of the matrix. But before we do that we need to discuss the notion of path. Suppose we have a sequence of edges: $A\to E\to C$. This is called a **path** from A to C of length 2, or a **2-path**. Similarly, the sequence $J\to A\to E\to C$ would be a path from J to C of length 3, or a **3-path**, and so on we could extend the concept to paths of any length. It is not relevant whether the vertices, or the edges are distinct or not. Thus for example, $\mathbf{J} \to \mathbf{C} \to \mathbf{J} \to \mathbf{C}$ is a path from **J** to **C** of length 3. It is common to call a path a **cycle** if the ending vertex is the same as the beginning vertex: for example, $\mathbf{J} \to \mathbf{C} \to \mathbf{J}$ is a 2-cycle.

What is the meaning of the $1,3-$entry of $\mathbf{M}$? Note that this entry corresponds to **Alyson-Emma**. We have that

$$m_{13} = a_{11}a_{13} + a_{12}a_{23} + a_{13}a_{33} + a_{14}a_{43} + a_{15}a_{53} = 0,$$

We know $a_{\mathbf{A}i}$ is **0** unless $\mathbf{A} \to i$ and similarly $a_{i\mathbf{E}}$ is **0** unless $i \to \mathbf{E}$. If either of these two terms is **0**, $a_{\mathbf{A}i}a_{i\mathbf{E}}$ contributes nothing to the sum, and otherwise the contribution is $1 = 1 \times 1$. The sum is counting then the number of times we have $\mathbf{A} \to i \to \mathbf{E}$, in other words the number of 2-paths from **A** to **E**. Hence $\mathbf{M}^2$ counts the number of 2-paths between any two vertices. So why is the $1,3-$entry of $\mathbf{M}$ equal to 0? Because there was no way for **Alison** to influence **Emma** via a third person, there was no **Alison** $\to$ **?** $\to$ **Emma**, since the only other person **Alison** influenced was **Carol** and **Carol** had no direct effect on **Emma**.

On the other hand,

$$m_{42} = a_{41}a_{12} + a_{42}a_{22} + a_{43}a_{32} + a_{44}a_{42} + a_{45}a_{52} = 2.$$

This happens because we have **Jason** $\to$ **Alison** $\to$ **Carol** and **Jason** $\to$ **Emma** $\to$ **Carol**, so there were two ways for **Jason** to influence **Carol** via another person.

By similar considerations, the $4,2-$position of $\mathbf{A}^3 = \mathbf{A} \times \mathbf{A}^2$ is 3 since we have 3 ways to travel from **Jason** to **Carol** via exactly 3 arrows: $\mathbf{J} \to \mathbf{A} \to \mathbf{E} \to \mathbf{C}$, $\mathbf{J} \to \mathbf{C} \to \mathbf{J} \to \mathbf{C}$, and $\mathbf{J} \to \mathbf{E} \to \mathbf{M} \to \mathbf{C}$.

One obvious consequence of the expression $m_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk} = \sum_{l=1}^{n} a_{il}b_{lk}$ is the fundamental fact that matrix multiplication is **associative**: let $\mathbf{A}$ be $m \times n$, $\mathbf{B}$ be $n \times p$, and $\mathbf{C}$ be $p \times q$. Let $\mathbf{M} = \mathbf{AB}$, and $\mathbf{N} = \mathbf{BC}$, then $\mathbf{MC}$ and $\mathbf{AN}$ both make sense, and the wonderful fact is that they are equal is true, since

$$\sum_{k=1}^{p} m_{ik}c_{kt} = \sum_{k=1}^{p}\sum_{l=1}^{n} \left(a_{il}b_{lk}\right)c_{kt} = \sum_{k=1}^{p}\sum_{l=1}^{n} a_{il}\left(b_{lk}c_{kt}\right) = \sum_{l=1}^{n}\sum_{k=1}^{p} a_{il}\left(b_{lk}c_{kt}\right) = \sum_{l=1}^{n} a_{il}n_{lt}$$

from which we get the tremendously useful fact that

$$(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$$

and as was mentioned above, this is called **associativity of multiplication**.

For example, suppose $\mathbf{A}$ is 5×3, $\mathbf{B}$ 3×2, and $\mathbf{C}$ is 2×4. Then $\mathbf{M} = \mathbf{AB}$ is 5×2, and $\mathbf{N} = \mathbf{BC}$ is 3×4, so $\mathbf{MC}$ and $\mathbf{AN}$ are both 5×4, but more than just the same size, as stated above they are equal. To consider just one entry, say the $5,4-$position in both matrices equals

$$a_{51}b_{11}c_{14}+a_{51}b_{12}c_{24}+a_{52}b_{21}c_{14}+a_{52}b_{22}c_{24}+a_{53}b_{31}c_{14}+a_{53}b_{32}c_{24}.$$

Observe that because we do not have commutativity, the order of the factors definitely matters in general, but that because we have associativity, the order in which we perform the multiplications does not matter as long as we respect the order of the factors. And this choice can be of great consequence as the following example will illustrate.

Example 4. How many single number multiplications in a matrix multiplication? Let $\mathbf{A}$ be $m\times n$, $\mathbf{B}$ be $n\times p$, and $\mathbf{M}=\mathbf{AB}$, which is be $m\times p$. Then since

$$m_{ik}=a_{i1}b_{1k}+a_{i2}b_{2k}+\cdots+a_{in}b_{nk}=\sum_{l=1}^{n}a_{il}b_{lk},$$

it is clear that it takes *n* multiplications to compute one entry of $\mathbf{M}$, and since $\mathbf{M}$ has mp entries, it will take mnp multiplications to compute the product.

Let us consider what associativity does for us in the following case: suppose $\mathbf{M}_1$ is a 5×10 matrix, while $\mathbf{M}_2$ is 10×20, $\mathbf{M}_3$ is 20×5 and $\mathbf{M}_4$ is 5×1. How many ways can we accomplish the multiplication $\mathbf{M}_1\times\mathbf{M}_2\times\mathbf{M}_3\times\mathbf{M}_4$? And how many multiplications will it take in each case? We can only multiply two matrices at a time, and we have the choices on the table as well as the number of multiplications it takes to do each of them.

$(\mathbf{M}_1\times\mathbf{M}_2)\times(\mathbf{M}_3\times\mathbf{M}_4)$	$5\times10\times20+20\times5\times1+5\times20\times1=1200$
$\mathbf{M}_1\times(\mathbf{M}_2\times(\mathbf{M}_3\times\mathbf{M}_4))$	$20\times5\times1+10\times20\times1+5\times10\times1=350$
$\mathbf{M}_1\times((\mathbf{M}_2\times\mathbf{M}_3)\times\mathbf{M}_4)$	$10\times20\times5+10\times5\times1+5\times10\times1=1100$
$((\mathbf{M}_1\times\mathbf{M}_2)\times\mathbf{M}_3)\times\mathbf{M}_4$	$5\times10\times20+5\times20\times5+5\times5\times1=1525$
$(\mathbf{M}_1\times(\mathbf{M}_2\times\mathbf{M}_3))\times\mathbf{M}_4$	$10\times20\times5+5\times10\times5+5\times5\times1=1275$

and we can see there is great difference between the numbers! Associativity is wonderful, it allows us to pick the second option.

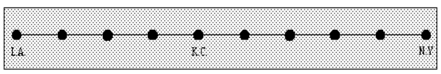
Example 5. Powers of a Square Matrix. We saw before that for any square matrix A, we can let $\mathbf{A}^2=\mathbf{AA}$ denote the square of that matrix. However, to even discuss the cube, we needed associativity, since $\mathbf{A}^3$ could conceivably be defined in two different ways: $(\mathbf{AA})\mathbf{A}$ or $\mathbf{A}(\mathbf{AA})$, but fortunately, we do not have to make that distinction, and thus we can define $\mathbf{A}^3=\mathbf{AAA}$ without any problems. Similarly, $\mathbf{A}^4=\mathbf{AAAA}$, and in general for any positive integer *n*, one can define $\mathbf{A}^n=\underbrace{\mathbf{AA}\cdots\mathbf{A}}_{n}$. Observe however that we do not have meaning yet for $\mathbf{A}^0$, nor do we have meaning for other exponents such as negative integers like $\mathbf{A}^{-1}$, nor for fractional exponents such as $\mathbf{A}^{\frac{1}{2}}$. Note however, that because of associativity, we do have the fundamental **law of exponents**:

$$\mathbf{A}^n\mathbf{A}^m = \mathbf{A}^{n+m} \text{ for any positive integers } n \text{ and } m.$$

Now that we have powers we can revisit another previous example.

Example 2 Revisited. Let us return to the communication network example. Extending the idea explained in the previous example, if $\mathbf{M}$ is the adjacency matrix, then $\mathbf{M}^2$ counts the number of 2-paths between any two vertices, $\mathbf{M}^3$ counts the number of 3-paths between vertices, $\mathbf{M}^4$ the number of 4-paths, etcetera. Hence we have that

for any positive integer *k*, the $i, j-$position of $\mathbf{M}^k$ denotes the number of *k*-paths from vertex *i* to vertex *j*.



We can compute the first three powers of the adjacency matrix $\mathbf{A}$ from **Example 2**. They are

$$\mathbf{A} = \begin{vmatrix} 0&1&0&0&0&0&0&0&0&0\\ 1&0&1&0&0&0&0&0&0&0\\ 0&1&0&1&0&0&0&0&0&0\\ 0&0&1&0&1&0&0&0&0&0\\ 0&0&0&1&0&1&0&0&0&0\\ 0&0&0&0&1&0&1&0&0&0\\ 0&0&0&0&0&1&0&1&0&0\\ 0&0&0&0&0&0&1&0&1&0\\ 0&0&0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&0&0&1&0 \end{vmatrix} \quad \mathbf{A}^2 = \begin{vmatrix} 1&0&1&0&0&0&0&0&0&0\\ 0&2&0&1&0&0&0&0&0&0\\ 1&0&2&0&1&0&0&0&0&0\\ 0&1&0&2&0&1&0&0&0&0\\ 0&0&1&0&2&0&1&0&0&0\\ 0&0&0&1&0&2&0&1&0&0\\ 0&0&0&0&1&0&2&0&1&0\\ 0&0&0&0&0&1&0&2&0&1\\ 0&0&0&0&0&0&1&0&2&0\\ 0&0&0&0&0&0&0&1&0&1 \end{vmatrix} \quad \mathbf{A}^3 = \begin{vmatrix} 0&2&0&1&0&0&0&0&0&0\\ 2&0&3&0&1&0&0&0&0&0\\ 0&3&0&3&0&1&0&0&0&0\\ 1&0&3&0&3&0&1&0&0&0\\ 0&1&0&3&0&3&0&1&0&0\\ 0&0&1&0&3&0&3&0&1&0\\ 0&0&0&1&0&3&0&3&0&1\\ 0&0&0&0&1&0&3&0&3&0\\ 0&0&0&0&0&1&0&3&0&2\\ 0&0&0&0&0&0&1&0&2&0 \end{vmatrix}$$

Why is the $1,1-$entry of $\mathbf{A}^2$ equal to 1? If without loss, we let the first three consecutive cities in the picture be: LA, LV (Las Vegas), and AQ (Albuquerque), then we can say because we can go $\mathrm{LA} \rightarrow \mathrm{LV} \rightarrow \mathrm{LA}$, and that is the only way we can go from LA to LA via a 2-path, while the $1,3-$ entry is also 1 because we can do $\mathrm{LA} \rightarrow \mathrm{LV} \rightarrow \mathrm{AQ}$, while the $2,2-$entry is 2 because we can do the following: $\mathrm{LV} \rightarrow \mathrm{LA} \rightarrow \mathrm{LV}$ and $\mathrm{LV} \rightarrow \mathrm{AQ} \rightarrow \mathrm{LV}$.

In $\mathbf{A}^3$, the $2,3-$entry is 3 because we can do the following: $\mathrm{LV} \rightarrow \mathrm{AQ} \rightarrow \mathrm{LV} \rightarrow \mathrm{AQ}$, $\mathrm{LV} \rightarrow \mathrm{LA} \rightarrow \mathrm{LV} \rightarrow \mathrm{AQ}$ and $\mathrm{LV} \rightarrow \mathrm{AQ} \rightarrow \mathrm{DV} \rightarrow \mathrm{AQ}$.

We get another immediate benefit of the entry-per-entry view of multiplication. Similarly to the argument for associativity, we get an argument for distributivity. Let $\mathbf{A}$ be $m \times n$, $\mathbf{B}$ be $n \times p$, and $\mathbf{C}$ be $n \times p$. Then since

$$\sum_{l=1}^{n} a_{il}\left(b_{lk} + c_{lk}\right) = \sum_{l=1}^{n} a_{il}b_{lk} + \sum_{l=1}^{n} a_{il}c_{lk},$$

we obtain the fundamental:

$$\mathbf{A}(\mathbf{B}+\mathbf{C})=\mathbf{AB}+\mathbf{AC}.$$

Just as easy is the other equation if we assume the appropriate sizes for the matrices:

$$(\mathbf{A}+\mathbf{B})\mathbf{C}=\mathbf{AC}+\mathbf{BC}.$$

By now we have seen two ways to visualize matrix multiplication—the **row times column** way and the **entry-by-entry** way. We now visit yet another way of multiplying matrices and that is **columns by rows**!! Let us return to the original definition of matrix multiplication:

$$\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix}=\alpha_1\beta_1+\alpha_2\beta_2+\cdots+\alpha_n\beta_n$$

and consider the special case when one of the factors is made up of scalars, in other words one of the factors is a vector. For example suppose that the $\beta's$ are scalars, then since scalars commute with anything, we could rewrite the product in the form

$$\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix}=\beta_1\alpha_1+\beta_2\alpha_2+\cdots+\beta_n\alpha_n$$

and we would be looking at an important construct—a linear combination of the $\alpha's$, a fundamental concept that will stay with us throughout the course.

If $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_n$ are vectors then any expression of the form

$$a_1\mathbf{u}_1+a_2\mathbf{u}_2+\cdots+a_n\mathbf{u}_n$$

where a_1, a_2, …, a_n are scalars is called a **linear combination** of $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_n$. Note that $\mathbf{0}$ is always a linear combination by letting all scalars equal 0.

Let us start with an example.

Example 6. Consider the following product: $\begin{pmatrix}a & b & c & d\end{pmatrix}\begin{pmatrix}1\\2\\3\\4\end{pmatrix}=a+2b+3c+4d$. Note that we do not need to specify that a, b, c and d are numbers, they could be column vectors in their own right. More concretely, consider now the product of a matrix times a column vector:

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \end{pmatrix}\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \left(\begin{pmatrix} a \\ e \\ i \end{pmatrix} \quad \begin{pmatrix} b \\ f \\ j \end{pmatrix} \quad \begin{pmatrix} c \\ g \\ k \end{pmatrix} \quad \begin{pmatrix} d \\ h \\ l \end{pmatrix}\right)\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = 1\begin{pmatrix} a \\ e \\ i \end{pmatrix} + 2\begin{pmatrix} b \\ f \\ j \end{pmatrix} + 3\begin{pmatrix} c \\ g \\ k \end{pmatrix} + 4\begin{pmatrix} d \\ h \\ l \end{pmatrix} = \begin{pmatrix} a+2b+3c+4d \\ e+2f+3g+4h \\ i+2j+3k+4l \end{pmatrix}.$$

Thus, when we multiply a matrix times a vector, we always obtain a linear combination of the columns, so we are visualizing this product **as the columns of the first factor times the rows of the second factor**.

Reiterating, if $\mathbf{A} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$, then $\mathbf{Ax}$, for any vector $\mathbf{x} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$, is a linear combination of the columns of **A**, $a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n$. And conversely any linear combination $a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n$ of vectors can be thought of as a matrix times a vector if we let $\mathbf{A} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$ and $\mathbf{x} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$. Thus, regardless of the size of the vectors, $7\mathbf{u} - 3\mathbf{v} + 4\mathbf{w} = \begin{pmatrix} \mathbf{u} & \mathbf{v} & \mathbf{w} \end{pmatrix}\begin{pmatrix} 7 \\ -3 \\ 4 \end{pmatrix}$.

Example 7. More concretely, consider

$$\begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12 \\ 4 & 8 & 12 & 16 \\ 5 & 10 & 15 & 20 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = 1\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} + 2\begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \\ 10 \end{pmatrix} + 3\begin{pmatrix} 5 \\ 6 \\ 9 \\ 12 \\ 15 \end{pmatrix} + 4\begin{pmatrix} 7 \\ 8 \\ 12 \\ 16 \\ 20 \end{pmatrix} = \begin{pmatrix} 50 \\ 60 \\ 90 \\ 120 \\ 150 \end{pmatrix}.$$

Example 8. Diagonal Matrices. Let $\mathbf{A} = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12 \\ 4 & 8 & 12 & 16 \\ 5 & 10 & 15 & 20 \end{pmatrix}$. What happens to **A** when we multiply it by a diagonal matrix? Suppose $\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Then when we multiply

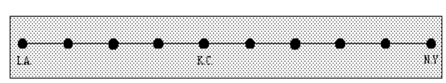
$$\mathbf{AD} = \begin{pmatrix} 1 & 6 & -5 & 0 \\ 2 & 8 & -6 & 0 \\ 3 & 12 & -9 & 0 \\ 4 & 16 & -12 & 0 \\ 5 & 20 & -15 & 0 \end{pmatrix}$$, and we should notice what has occurred, **every column of A has been multiplied by the respective entry in D**.

Abstractly, let $\mathbf{A} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$ and let us consider $\mathbf{Ax}_1$ where $\mathbf{x}_1 = \begin{pmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Easily, we get $\mathbf{Ax}_1 = a_1\mathbf{u}_1$. Similarly, if $\mathbf{x}_2 = \begin{pmatrix} 0 \\ a_2 \\ \vdots \\ 0 \end{pmatrix}$, then $\mathbf{Ax}_2 = a_2\mathbf{u}_2$. Continuing in this fashion, $\mathbf{Ax}_3 = a_3\mathbf{u}_3$ if $\mathbf{x}_3$ has zeroes in every position except the third entry which is a_3, and in general, with the obvious extension of the notation, $\mathbf{Ax}_i = a_i\mathbf{u}_i$. By simple stacking we get the following fact about multiplication with diagonal matrices. Let $\mathbf{A} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$ and let $\mathbf{D} = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$ be a diagonal matrix. Then

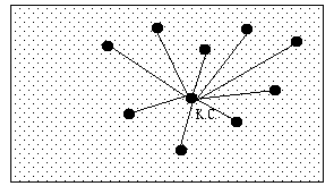
$$\mathbf{AD} = \begin{pmatrix} a_1\mathbf{u}_1 & a_2\mathbf{u}_2 & \cdots & a_n\mathbf{u}_n \end{pmatrix}.$$

Thus, $\begin{pmatrix} \mathbf{u} & \mathbf{v} & \mathbf{w} \end{pmatrix} \begin{pmatrix} 7 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 7\mathbf{u} & -3\mathbf{v} & 4\mathbf{w} \end{pmatrix}$.

One can use the idea of linear combination of the columns to mentally multiply matrices especially if one of the factors is a $(0,1)-$matrix. We gain revisit the communication network example. It actually stemmed from the 1950's, when the **AT&T** Company had decided to build 10 relay station network distributed throughout the country. The idea was to link these stations in order to establish a national communication network. Naturally, there were two opposing forces to contend with: the cost of linking pairs of stations (regardless of distance) versus the desire for a solid network, one not vulnerable to breakdowns, nor to long relays, circuit overflow, or even sabotage. A balance had to be achieved between these two contending positions. One of the possible solutions was the one previously looked at in **Example 2**:



It is easily shown that in order to have a connected network 9 edges were minimal, so indeed this network was optimal in cost, but certainly susceptible to long relays, and fragile if one station breaks down. The long relays can easily be observed in the graph, but they are also reflected by the powers of the adjacency matrix. Since there is not path from **LA** to **NY** shorter than length 9, the first power of $\mathbf{A}$ in which the $\mathbf{LA}, \mathbf{NY}$ – position is not 0 is the 9th power, $\mathbf{A}^9$. So there were other networks considered.



Example 2 Extended. Here is another 9-edge network:

This **Kansas City** model has for its adjacency matrix (if we choose **KC** has the first vertex)

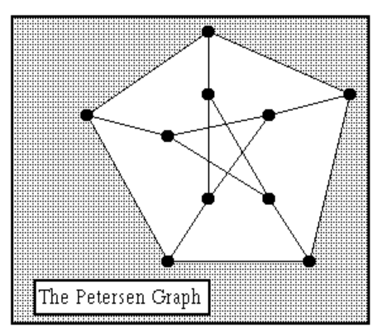
$$\mathbf{B} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

. To square this matrix mentally is quite easy. We see that the first column of the square is $\mathbf{Bu}_1$ where $\mathbf{u}_1$ is its first column, so it is the sum of all columns but the first one, while all other columns of $\mathbf{B}^2$ are just copies of the first column of $\mathbf{B}$. So

$$\mathbf{B}^2 = \begin{pmatrix} 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

—**all head, no hands.**

Needless to say, the **KC** model has short relays, but **KC** is certainly overloaded, and a break down there (due to malfunction or sabotage) would be a total disaster in communication.



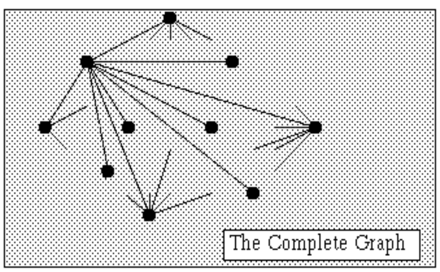
It would be perhaps unfair to leave the story unfinished. The engineers at **AT&T** proposed as a solution a graph stemming from the 19th century known as the **Petersen Graph**, Its virtues were clear:

- only 15 edges,
- every vertex is balanced (3 edges from each),
- longest relay is 2,
- safe from one or two vertex breakdowns.

Some of its efficiency is reflected by the adjacency matrix and its square:

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \text{ and } \mathbf{C}^2 = \begin{pmatrix} 3 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 3 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 3 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 3 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 3 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 3 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 3 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 3 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 3 \end{pmatrix}.$$

We see its efficiency since there are no ones wasted between the adjacency matrix and its square. In other words, if we let $\mathbf{J}_n$ denote the $n \times n$ matrix composed of only 1's, then we have that $\mathbf{C} + \mathbf{C}^2 = \mathbf{J}_{10} + 2\mathbf{I}_{10}$.


The Complete Graph

Unfortunately, the U.S. government was not happy with the explanations for the Petersen graph and instead they required for the **complete graph** to be built which has 45 edges, and the matrix $\mathbf{J}_{10} - \mathbf{I}_{10}$ for its adjacency matrix.

But all we have stated about columns in the previous paragraphs can also be stated about rows, and the easiest ways to understand this switch is via a theorem about transposes.

Suppose $\mathbf{A}$ is 8×5 and $\mathbf{B}$ is 5×7, then we can certainly multiply $\mathbf{AB}$ and obtain a matrix of size 8×7. Now $\mathbf{A}^{\mathrm{T}}$ is 5×8 and $\mathbf{B}^{\mathrm{T}}$ is 7×5, so $\mathbf{A}^{\mathrm{T}}\mathbf{B}^{\mathrm{T}}$ does not make sense, but $\mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$ does and it is of size 7×8—and what one may suspect happens indeed does. All that is basically needed for the proof is the key observation that for vector of the same size:

$$\mathbf{v}^{\mathrm{T}}\mathbf{u} = \mathbf{v} \cdot \mathbf{u} = \mathbf{u} \cdot \mathbf{v} = \mathbf{u}^{\mathrm{T}}\mathbf{v}.$$

The following efficient argument might be convincing. For example, the $5,6-$entry of $(\mathbf{AB})^{\mathrm{T}}$ is the $6,5-$entry of $\mathbf{AB}$. The latter equals the dot product of the 6th row of $\mathbf{A}$ with the 5th column of $\mathbf{B}$, which is the same as the dot product of the 5th row of $\mathbf{B}^{\mathrm{T}}$ and the 6th column of $\mathbf{A}^{\mathrm{T}}$ which is the $5,6-$entry of $\mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$. Thus, we have

Theorem. (Transposes.) Let $\mathbf{A}$ be $m \times n$ and let $\mathbf{B}$ be $n \times p$. Then

$$(\mathbf{AB})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}.$$

Example 9. Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$. Now $\mathbf{AB} = \begin{pmatrix} a+4b & 2a+5b & 3a+6b \\ c+4d & 2c+5d & 3c+6d \\ e+4f & 2e+5f & 3e+6f \end{pmatrix}$. Also $\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} a & c & e \\ b & d & f \end{pmatrix}$ and $\mathbf{B}^{\mathrm{T}} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$, and although $\mathbf{A}^{\mathrm{T}}\mathbf{B}^{\mathrm{T}}$ makes sense in this case, the result would be a 2×2 matrix. Rather it is $\mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} a+4b & c+4d & e+4f \\ 2a+5b & 2c+5d & 2e+5f \\ 3a+6b & 3c+6d & 3e+6f \end{pmatrix}$ which provides a 3×3 matrix, the transpose of the original product.

Thus from the theorem, we immediately have the corresponding claim about a row vector times a matrix $\mathbf{A}$. The resulting vector will be a linear combination of the rows of $\mathbf{A}$. For example:

$$\begin{pmatrix} 1 & -1 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12 \\ 4 & 8 & 12 & 16 \\ 5 & 10 & 15 & 20 \end{pmatrix} = 1\begin{pmatrix} 1 & 3 & 5 & 7 \end{pmatrix} - 1\begin{pmatrix} 2 & 4 & 6 & 8 \end{pmatrix} + 2\begin{pmatrix} 3 & 6 & 9 & 12 \end{pmatrix}$$

$$+0\begin{pmatrix} 4 & 8 & 12 & 16 \end{pmatrix} + 3\begin{pmatrix} 5 & 10 & 15 & 20 \end{pmatrix} = \begin{pmatrix} 20 & 41 & 62 & 83 \end{pmatrix}.$$

Thus, when we multiply a matrix times a vector, we always obtain a linear combination of the columns, or the rows as the case may be.

Example 10. Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$, and if we think of $\mathbf{A} = \begin{pmatrix} \mathbf{v}_1^{\mathrm{T}} \\ \mathbf{v}_2^{\mathrm{T}} \\ \mathbf{v}_3^{\mathrm{T}} \end{pmatrix}$, then

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\mathbf{A} = \begin{pmatrix} a+2c+3e & b+2d+3f \end{pmatrix} = 1\mathbf{v}_1^{\mathrm{T}} + 2\mathbf{v}_2^{\mathrm{T}} + 3\mathbf{v}_3^{\mathrm{T}}.$$

Example 11. Diagonal Matrices II. If we then multiply a matrix on the left by a diagonal matrix, the end result will be a matrix in which the rows have been multiplied by the corresponding entries of the diagonal matrix. *E.g.,*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \\ j & k & l \end{pmatrix} = \begin{pmatrix} a & b & c \\ -d & -e & -f \\ 3g & 3h & 3i \\ 0 & 0 & 0 \end{pmatrix}.$$

If $\mathbf{A} = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12 \\ 4 & 8 & 12 & 16 \\ 5 & 10 & 15 & 20 \end{pmatrix}$ and $\mathbf{E} = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$, then $\mathbf{EA} = \begin{pmatrix} -1 & -3 & -5 & -7 \\ 6 & 12 & 18 & 24 \\ 0 & 0 & 0 & 0 \\ 4 & 8 & 12 & 16 \\ 10 & 20 & 30 & 40 \end{pmatrix}$, **every row of A has been multiplied by the respective entry in E**.

In particular, this finishes explaining the name identity matrix for $\mathbf{I}_n$, because it does act like 1 does for numbers—namely, for any $m \times n$ matrix **A**,

$$\mathbf{I}_m\mathbf{A} = \mathbf{A}\mathbf{I}_n = \mathbf{A}.$$

In particular for any square matrix **A** of size n, $\mathbf{I}_n\mathbf{A} = \mathbf{A}\mathbf{I}_n = \mathbf{A}$, and thus just like we do for numbers, one defines $\mathbf{A}^0 = \mathbf{I}$ for a square matrix where the **I** is of the same size as **A**. Note that by this definition the fundamental law of exponents has been extended:

$$\mathbf{A}^n\mathbf{A}^m = \mathbf{A}^{n+m} \text{ for any nonnegative integers } n \text{ and } m.$$

Example 4 Revisited. Let us recall that in that example you were interested in dinner arrangements for six friends, and thus you had come up with the following incidence matrix **M**:

$$\begin{array}{c|cccccc} & \mathbf{m} & \mathbf{t} & \mathbf{w} & \mathbf{t} & \mathbf{f} & \mathbf{s} \\ \hline \mathcal{A} & 1 & 1 & 1 & 0 & 0 & 0 \\ \mathcal{B} & 1 & 1 & 0 & 1 & 0 & 0 \\ \mathcal{C} & 1 & 0 & 0 & 0 & 1 & 1 \\ \mathcal{D} & 0 & 1 & 0 & 0 & 1 & 1 \\ \mathcal{E} & 0 & 0 & 1 & 1 & 1 & 0 \\ \mathcal{F} & 0 & 0 & 1 & 1 & 0 & 1 \end{array}$$

In general, what does $\mathbf{MM}^{\mathrm{T}}$ compute? As usual, it is the product of a row of **M** with a column of $\mathbf{M}^{\mathrm{T}}$, but such a column is a row of **M**, and thus for any matrix **M**, the matrix $\mathbf{MM}^{\mathrm{T}}$ has for its $i, j-$entry is the dot product of row i with row j. For a (0,1)-matrix, it counts the number of **1**'s they share, and in fact for the matrix above, we get: $\begin{pmatrix} 3 & 2 & 1 & 1 & 1 & 1 \\ 2 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 2 & 1 & 1 \\ 1 & 1 & 2 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 2 \\ 1 & 1 & 1 & 1 & 2 & 3 \end{pmatrix}$, and this matrix reflects the fact that friends $\mathcal{A}$ and $\mathcal{B}$ will have two dinners together, and so will $\mathcal{C}$ & $\mathcal{D}$, and $\mathcal{E}$ and $\mathcal{F}$.

Note that for any matrix **M**,

$$\mathbf{MM}^{\mathrm{T}} \text{ is a symmetric matrix}$$

since

$$\left(\mathbf{MM}^{\mathrm{T}}\right)^{\mathrm{T}} = \mathbf{M}^{\mathrm{T}^{\mathrm{T}}}\mathbf{M}^{\mathrm{T}} = \mathbf{MM}^{\mathrm{T}}.$$

Dually, for any matrix **M**, $\mathbf{M}^{\mathrm{T}}\mathbf{M}$ **computes the dot product of any two columns of M**, and it is also symmetric.

Maybe it would better to have 7 friends. In that case, we have $\binom{7}{2} = 21$ pairs to take care of, and still 3 per night, so it will take 7 nights minimum. Can it be done in 7 nights? Yes, and the solution is again basically unique. Here's the incidence matrix:

$$\begin{array}{c} \\ \mathbf{A} \\ \mathbf{B} \\ \mathbf{C} \\ \mathbf{D} \\ \mathbf{E} \\ \mathbf{F} \\ \mathbf{G} \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathbf{m} & \mathbf{t} & \mathbf{w} & \mathbf{t} & \mathbf{f} & \mathbf{s} & \mathbf{s} \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

—which is in some ways superior to the 6 friends set up in that any two friends have dinner together exactly once. And it only cost one more dinner to take care of one more friend. And indeed that efficiency is illustrated when we compute $\mathbf{M}^{\mathrm{T}}\mathbf{M} = 2\mathbf{I}_7 + \mathbf{J}_7$, and we see very little waste!

It would not be beneficial to have 8 friends. We have now $\binom{8}{2} = 28$ pairs to take care of, and being able to take care of at most 3 a night, it will take at least 10 nights to cover our scheme. Since we have to give at least 3 more dinners to take care of just one more acquaintance we will cold-bloodedly drop him. As to whether to go with 6 or 7 friends we will leave for you to decide.

Example 12. **Things that do commute.** We have learned that in general matrices do not commute. However, it is also true that some times matrices do. This following are all true for an arbitrary square matrix **A**. We have clearly

- **A** commutes with **I** and **A**.

More generally,

- **A** commutes with all of its powers because of associativity: $\mathbf{A}\mathbf{A}^n = \mathbf{A}^n\mathbf{A}$.
- If **A** commutes with **B** and **C**, then by distributivity, it commutes with $\mathbf{B}+\mathbf{C}$:
$$\mathbf{A}(\mathbf{B}+\mathbf{C}) = \mathbf{AB}+\mathbf{AC} = \mathbf{BA}+\mathbf{CA} = (\mathbf{B}+\mathbf{C})\mathbf{A}.$$

Also, since scalars commute with matrices, $\mathbf{A}(a\mathbf{B}) = a(\mathbf{AB})$,

- if **A** commutes with **B**, then it commutes with any scalar multiple of **B**.

A polynomial of a (square) matrix is a linear combination of its powers. For example, $2\mathbf{I}+3\mathbf{A}+4\mathbf{A}^3-5\mathbf{A}^6$ is a polynomial in **A**. This is reasonable since we can think of that expression as nothing but $p(\mathbf{A})$ where $p(x)$ is the polynomial $2+3x+4x^3-5x^6$. Recall that $\mathbf{A}^0 = \mathbf{I}$. As an obvious consequence of facts above we get

- **A** commutes with any polynomial in **A**.

It may happen that the only matrices that commute with a given matrix are exactly its polynomials. For example, let $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, and let $\mathbf{B} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\mathbf{AB} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}$ while

$\mathbf{BA} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix}$, so the only way we can have $\mathbf{AB} = \mathbf{BA}$ is to have $c = 0$ and $a = d$, but then $\mathbf{B} = a\mathbf{I} + b\mathbf{A}$, a polynomial in $\mathbf{A}$.

As we leave this fundamental section on multiplication of matrices, we make a few closing remarks: **although a matrix is not a set of vectors, one can visualize it as such, and actually in two different ways, its row vectors, or its column vectors.**

We also put the most important properties that do or do not hold for this important operation in an easy summary:

Properties that DO necessarily hold	
$\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}$	associativity of multiplication
$\mathbf{AI} = \mathbf{A} = \mathbf{IA}$	identity matrix
$\mathbf{AO} = \mathbf{O} = \mathbf{OA}$	zero annihilates
$(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$	distributivity of multiplication
$\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{AB} + \mathbf{AC}$	distributivity of multiplication

Properties that do NOT necessarily hold	
$\mathbf{AB} = \mathbf{BA}$	commutativity of multiplication
If $\mathbf{AB} = \mathbf{O}$, then $\mathbf{A} = \mathbf{O}$ or $\mathbf{B} = \mathbf{O}$	cancellation
If $\mathbf{AB} = \mathbf{AC}$, then $\mathbf{B} = \mathbf{C}$	cancellation

❹ Stacking, Blocking & Matrix Multiplication

Let us start by recalling the beauty and power of the definition of a row times a product:

$$\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_n\end{pmatrix}\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix} = \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n .$$

This definition did not depend on the nature of the components. Namely it is immaterial how we view the components of the vectors or matrices that we are multiplying, the end result is the same.

And of course we saw from its inception that matrix multiplication relied on stacking for its definition. Specifically for any matrix product one is just stacking rows and columns to build that product. Hence the following stacking rules are perfectly obvious:

- ❍ Let $\mathbf{A}$ be $m\times n$, $\mathbf{B}$ be $p\times n$, and $\mathbf{C}$ be $n\times q$. Then obviously, $\mathbf{AC}$ and $\mathbf{BC}$ make sense, but $\begin{pmatrix}\mathbf{A}\\ \mathbf{B}\end{pmatrix}\mathbf{C}$ also makes sense, and then

$$\begin{pmatrix}\mathbf{A}\\ \mathbf{B}\end{pmatrix}\mathbf{C} = \begin{pmatrix}\mathbf{AC}\\ \mathbf{BC}\end{pmatrix}.$$

Note we can even see this product as a 2×1 matrix times a 1×1. Thus in particular some interesting special cases are: $\begin{pmatrix}\mathbf{A}\\ \mathbf{0}\end{pmatrix}\mathbf{C} = \begin{pmatrix}\mathbf{AC}\\ \mathbf{0}\end{pmatrix}$, or $\begin{pmatrix}\mathbf{A}\\ \mathbf{I}\end{pmatrix}\mathbf{C} = \begin{pmatrix}\mathbf{AC}\\ \mathbf{C}\end{pmatrix}$. For example

$$\begin{pmatrix}1 & 2\\ 3 & 4\\ 1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a+2c & b+2d\\ 3a+4c & 3b+4d\\ a & b\\ c & d\end{pmatrix}.$$

- ☐ Let $\mathbf{A}$ be $m\times n$, $\mathbf{B}$ be $n\times p$, and $\mathbf{C}$ be $n\times q$. Then obviously, $\mathbf{AB}$ and $\mathbf{AC}$ make sense, but $\mathbf{A}\begin{pmatrix}\mathbf{B} & \mathbf{C}\end{pmatrix}$ also makes sense, and then

$$\mathbf{A}\begin{pmatrix}\mathbf{B} & \mathbf{C}\end{pmatrix} = \begin{pmatrix}\mathbf{AB} & \mathbf{AC}\end{pmatrix}.$$

Again we can see this product as a 1×1 times a 1×2, and similar special cases hold: $\mathbf{A}\begin{pmatrix}\mathbf{B} & \mathbf{0}\end{pmatrix} = \begin{pmatrix}\mathbf{AB} & \mathbf{0}\end{pmatrix}$ or $\mathbf{A}\begin{pmatrix}\mathbf{B} & \mathbf{I}\end{pmatrix} = \begin{pmatrix}\mathbf{AB} & \mathbf{A}\end{pmatrix}$. For example

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 0 & 1 & 2 & 3\\ 0 & 1 & 4 & 5 & 6\end{pmatrix} = \begin{pmatrix}a & b & a+4b & 2a+5b & 3a+6b\\ c & d & c+4d & 2c+5d & 3c+6d\end{pmatrix}.$$

By combining the previous two rules one has then

❑ Let $\mathbf{A}$ be $m\times n$, $\mathbf{B}$ be $p\times n$, $\mathbf{C}$ be $n\times q$, and $\mathbf{D}$ be $n\times r$. Then obviously, $\mathbf{AC}$, $\mathbf{AD}$, $\mathbf{BC}$ and $\mathbf{BD}$ all make sense, but so does $\begin{pmatrix}\mathbf{A}\\ \mathbf{B}\end{pmatrix}\begin{pmatrix}\mathbf{C} & \mathbf{D}\end{pmatrix}$, and then

$$\begin{pmatrix}\mathbf{A}\\ \mathbf{B}\end{pmatrix}\begin{pmatrix}\mathbf{C} & \mathbf{D}\end{pmatrix}=\begin{pmatrix}\mathbf{AC} & \mathbf{AD}\\ \mathbf{BC} & \mathbf{BD}\end{pmatrix}.$$

For example $\begin{pmatrix}1&2\\3&4\\1&0\\0&1\end{pmatrix}\begin{pmatrix}1&0&1&2&3\\0&1&4&5&6\end{pmatrix}=\begin{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix}\mathbf{I} & \begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}\\ \mathbf{I} & \mathbf{I}\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}\end{pmatrix}=$

$$\begin{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix} & \begin{pmatrix}9&12&15\\19&26&33\end{pmatrix}\\ \begin{pmatrix}1&0\\0&1\end{pmatrix} & \begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}\end{pmatrix}=\begin{pmatrix}1&2&9&12&15\\3&4&19&26&33\\1&0&1&2&3\\0&1&4&5&6\end{pmatrix}.$$

But by extending on the last three rules, we get the following block multiplication rule:

■ Let $\mathbf{A}$ be $m\times n$, $\mathbf{B}$ be $p\times n$, $\mathbf{C}$ be $m\times q$, and $\mathbf{D}$ be $p\times q$. Let $\mathbf{X}$ be $n\times r$, $\mathbf{Y}$ be $q\times r$, $\mathbf{Z}$ be $n\times s$, and $\mathbf{W}$ be $q\times s$. Then all expressions in the following equation make sense and the equation is valid:

$$\begin{pmatrix}\mathbf{A} & \mathbf{C}\\ \mathbf{B} & \mathbf{D}\end{pmatrix}\begin{pmatrix}\mathbf{X} & \mathbf{Z}\\ \mathbf{Y} & \mathbf{W}\end{pmatrix}=\begin{pmatrix}\mathbf{AX}+\mathbf{CY} & \mathbf{AZ}+\mathbf{CW}\\ \mathbf{BX}+\mathbf{DY} & \mathbf{BZ}+\mathbf{DW}\end{pmatrix}.$$

Example 1. Let $\mathbf{M}=\begin{pmatrix}1&1&1\\0&0&3\\0&0&3\end{pmatrix}$ and let $\mathbf{N}=\begin{pmatrix}1&1&1&2\\1&1&3&4\\0&0&1&1\end{pmatrix}$. Then we can visualize $\mathbf{M}$ and $\mathbf{N}$ as 2×2 matrices: $\mathbf{M}=\begin{pmatrix}\begin{pmatrix}1&1\end{pmatrix} & 1\\ \begin{pmatrix}0&0\\0&0\end{pmatrix} & \begin{pmatrix}3\\3\end{pmatrix}\end{pmatrix}$, so $\mathbf{M}=\begin{pmatrix}\mathbf{A} & \mathbf{C}\\ \mathbf{B} & \mathbf{D}\end{pmatrix}$ where $\mathbf{A}=\begin{pmatrix}1 & 1\end{pmatrix}$, $\mathbf{B}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$, $\mathbf{C}=\begin{pmatrix}1\end{pmatrix}$, and $\mathbf{D}=\begin{pmatrix}3\\3\end{pmatrix}$ while $\mathbf{N}=\begin{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix} & \begin{pmatrix}1&2\\3&4\end{pmatrix}\\ \begin{pmatrix}0&0\end{pmatrix} & \begin{pmatrix}1&1\end{pmatrix}\end{pmatrix}$, so $\mathbf{N}=\begin{pmatrix}\mathbf{X} & \mathbf{Z}\\ \mathbf{Y} & \mathbf{W}\end{pmatrix}$ where $\mathbf{X}=\begin{pmatrix}1&1\\1&1\end{pmatrix}$, $\mathbf{Y}=\begin{pmatrix}0 & 0\end{pmatrix}$, $\mathbf{Z}=\begin{pmatrix}1&2\\3&4\end{pmatrix}$, and $\mathbf{W}=\begin{pmatrix}1 & 1\end{pmatrix}$, now

$$\mathbf{AX}+\mathbf{CY}=\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix}+\begin{pmatrix}1\end{pmatrix}\begin{pmatrix}0 & 0\end{pmatrix}=\begin{pmatrix}2 & 2\end{pmatrix}+\begin{pmatrix}0 & 0\end{pmatrix}=\begin{pmatrix}2 & 2\end{pmatrix}$$

$$\mathbf{AZ}+\mathbf{CW}=\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix}+\begin{pmatrix}1\end{pmatrix}\begin{pmatrix}1 & 1\end{pmatrix}=\begin{pmatrix}4 & 6\end{pmatrix}+\begin{pmatrix}1 & 1\end{pmatrix}=\begin{pmatrix}5 & 7\end{pmatrix}$$

$$\mathbf{BX}+\mathbf{DY}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix}+\begin{pmatrix}3\\3\end{pmatrix}\begin{pmatrix}0 & 0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

$$\mathbf{BZ}+\mathbf{DW}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix}+\begin{pmatrix}3\\3\end{pmatrix}\begin{pmatrix}1&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}+\begin{pmatrix}3&3\\3&3\end{pmatrix}=\begin{pmatrix}3&3\\3&3\end{pmatrix}$$

and we see that
$$\begin{pmatrix}\mathbf{AX}+\mathbf{CY}&\mathbf{AZ}+\mathbf{CW}\\\mathbf{BX}+\mathbf{DY}&\mathbf{BZ}+\mathbf{DW}\end{pmatrix}=\begin{pmatrix}\begin{pmatrix}2&2\end{pmatrix}&\begin{pmatrix}5&7\end{pmatrix}\\\begin{pmatrix}0&0\\0&0\end{pmatrix}&\begin{pmatrix}3&3\\3&3\end{pmatrix}\end{pmatrix}=\begin{pmatrix}2&2&5&7\\0&0&3&3\\0&0&3&3\end{pmatrix}=\mathbf{MN}.$$

But, as always, care has to be given to the order of the multiplications.

The key is that the sizes have to make sense—but once they do, one is free to block or stack any way one wants.

And the theorem below further clarifies the generality of block multiplication.

Theorem (Block Multiplication). Let $\mathbf{M}$ and $\mathbf{N}$ be such that $\mathbf{MN}$ makes sense. Suppose $\mathbf{M}=\begin{pmatrix}\mathbf{A}&\mathbf{C}\\\mathbf{B}&\mathbf{D}\end{pmatrix}$ and $\mathbf{N}=\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\\mathbf{Y}&\mathbf{W}\end{pmatrix}$ are in block decomposition form. If $\mathbf{AX}$ makes sense, then we can block multiply $\mathbf{MN}$, in other words:
$$\mathbf{MN}=\begin{pmatrix}\mathbf{A}&\mathbf{C}\\\mathbf{B}&\mathbf{D}\end{pmatrix}\begin{pmatrix}\mathbf{X}&\mathbf{Z}\\\mathbf{Y}&\mathbf{W}\end{pmatrix}=\begin{pmatrix}\mathbf{AX}+\mathbf{CY}&\mathbf{AZ}+\mathbf{CW}\\\mathbf{BX}+\mathbf{DY}&\mathbf{BZ}+\mathbf{DW}\end{pmatrix}.$$

Proof. Suppose that $\mathbf{M}$ is $p\times q$ and $\mathbf{N}$ is $q\times r$. Furthermore assume $\mathbf{A}$ is $k\times m$ and $\mathbf{X}$ is $m\times n$. Then we easily gather the following information

Matrix	B	C	D	Y	Z	W
Size	$(p-k)\times m$	$k\times(q-m)$	$(p-k)\times(q-m)$	$(q-m)\times n$	$m\times(r-n)$	$(q-m)\times(r-n)$

But then $\mathbf{AX}$ and $\mathbf{CY}$ are both of size $k\times n$, so $\mathbf{AX}+\mathbf{CY}$ is of the same size. Similarly, $\mathbf{AZ}+\mathbf{CW}$, $\mathbf{BX}+\mathbf{DY}$ and $\mathbf{BZ}+\mathbf{DW}$ all make sense, and so by ■ we are done. ⌘

A particularly interesting case of the theorem is that of powers of a square matrix.

Corollary (Balanced Block). Let $\mathbf{M}$ be a square matrix and suppose $\mathbf{M}=\begin{pmatrix}\mathbf{A}&\mathbf{C}\\\mathbf{B}&\mathbf{D}\end{pmatrix}$ where $\mathbf{A}$ is square. Then $\mathbf{M}^2=\begin{pmatrix}\mathbf{A}^2+\mathbf{CB}&\mathbf{AC}+\mathbf{CD}\\\mathbf{BA}+\mathbf{DB}&\mathbf{BC}+\mathbf{D}^2\end{pmatrix}$.

Example 2. Let $\mathbf{A}$ be the adjacency matrix of the Petersen graph. So we know that $\mathbf{A}$ is a 10×10 symmetric $(0,1)-$matrix with 3 ones in each row. Also $\mathbf{A}^2+\mathbf{A}=2\mathbf{I}_{10}+\mathbf{J}_{10}$. Consider the matrix $\mathbf{M}=\begin{pmatrix}\mathbf{A}&\mathbf{1}\\\mathbf{1}^{\mathrm{T}}&0\end{pmatrix}$ where $\mathbf{1}$ denotes a vector of all ones. In this case, for the stacking to be possible, it is a vector of size 10. Then by block multiplication $\mathbf{M}^2=\begin{pmatrix}\mathbf{A}^2+\mathbf{J}_{10}&3\mathbf{1}\\3\mathbf{1}^{\mathrm{T}}&10\end{pmatrix}=\begin{pmatrix}2\mathbf{I}_{10}+2\mathbf{J}_{10}-\mathbf{A}&3\mathbf{1}\\3\mathbf{1}^{\mathrm{T}}&10\end{pmatrix}$, so $\mathbf{M}^2+\mathbf{M}=\begin{pmatrix}2\mathbf{I}_{10}+2\mathbf{J}_{10}&4\mathbf{1}\\4\mathbf{1}^{\mathrm{T}}&10\end{pmatrix}$.

Another nice application of block multiplication is the following theorem.

The previous example illustrated one of the powerful applications of block decomposition, the ability to prove theorems like the following—but before we cite it, **we will always assume when in an abstract discussion when we multiply matrices, the sizes are compatible.**

> **Corollary (Block Upper Triangular Matrices).** Let $\mathbf{M}$ and $\mathbf{N}$ be such that $\mathbf{MN}$ makes sense. Suppose $\mathbf{M} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{0} & \mathbf{D} \end{pmatrix}$ and $\mathbf{N} = \begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ \mathbf{0} & \mathbf{W} \end{pmatrix}$ are in block upper triangular form. If $\mathbf{AX}$ makes sense, then their product is also in (block) upper triangular form. Moreover, the diagonal blocks of the product are the respective products of the diagonal blocks.

Proof. If we take $\begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{0} & \mathbf{D} \end{pmatrix}$ and $\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ \mathbf{0} & \mathbf{W} \end{pmatrix}$, then by the theorem, their product is given by $\begin{pmatrix} \mathbf{AX} & \mathbf{AZ}+\mathbf{CW} \\ \mathbf{0} & \mathbf{DW} \end{pmatrix}$, and our claim is proven. ⌘.

The example above was already an illustration of the last corollary. But we should also emphasize that there is nothing special about the 2×2 form of the matrix—the same would be true for a 3×3, 4×4, etcetera.

Recall that we observed before that a matrix in block form can be multiplied by itself only if the decomposition is balanced, in other words only if the diagonal blocks are square. But the theorem tells us that if such as decomposition is upper triangular, the square of the matrix will also be so.

As another illustration of the theorem, consider the matrix from **Example 3** above. It is a 10×10, but it can be viewed as a 4×4 (balanced) block decomposition as we saw in that example, and so its square will also be (block) upper triangular, and so will its cube.

$$\mathbf{M}\qquad \begin{array}{c|ccc|ccccc|c} 1&0&0&0&1&0&1&1&0&0\\ \hline 0&1&1&1&0&0&0&1&0&0\\ 0&1&1&0&0&1&0&1&1&0\\ 0&1&1&1&0&0&1&1&0&0\\ \hline 0&0&0&0&0&0&1&0&0&1\\ 0&0&0&0&1&0&0&1&0&0\\ 0&0&0&0&0&1&0&1&1&1\\ 0&0&0&0&1&0&0&1&1&1\\ 0&0&0&0&0&1&0&0&0&2\\ \hline 0&0&0&0&0&0&0&0&0&1 \end{array}$$

$$\mathbf{M}^2\qquad \begin{array}{c|ccc|ccccc|c} 1&0&0&0&2&1&2&3&2&3\\ \hline 0&3&3&2&1&1&1&4&2&1\\ 0&2&2&1&2&2&0&4&2&3\\ 0&3&3&2&1&2&1&5&3&2\\ \hline 0&0&0&0&0&1&0&1&1&2\\ 0&0&0&0&1&0&1&1&1&2\\ 0&0&0&0&2&1&0&2&1&4\\ 0&0&0&0&1&1&1&1&1&5\\ 0&0&0&0&1&0&0&1&0&2\\ \hline 0&0&0&0&0&0&0&0&0&1 \end{array}$$

$$\mathbf{M}^3\qquad \begin{array}{c|ccc|ccccc|c} 1&0&0&0&5&4&3&7&5&14\\ \hline 0&8&8&5&5&6&3&14&8&11\\ 0&5&5&3&6&4&3&11&6&13\\ 0&8&8&5&7&7&3&16&9&15\\ \hline 0&0&0&0&2&1&0&2&1&5\\ 0&0&0&0&1&2&1&2&2&7\\ 0&0&0&0&3&1&2&3&2&10\\ 0&0&0&0&2&2&1&3&2&10\\ 0&0&0&0&1&0&1&1&1&4\\ \hline 0&0&0&0&0&0&0&0&0&1 \end{array}$$

Because it is true for block triangular matrices, then it is also true for

Corollary (Triangular Matrices). Let $\mathbf{M}$ and $\mathbf{N}$ be square of the same size.
❶ If $\mathbf{M}$ and $\mathbf{N}$ are upper triangular, then so is their product.
❷ If $\mathbf{M}$ and $\mathbf{N}$ are lower triangular, then so is their product.
❸ If $\mathbf{M}$ and $\mathbf{N}$ are diagonal, then so is their product.
And in all three cases, the diagonal entries are just the products of the respective diagonal entries.

Proof. The key idea for ❶ is that any upper triangular matrix can be thought of as a block upper triangular with only two blocks, and then one proceeds by induction. By transposing ❶ one obtains ❷, and ❸ is an immediate consequence of ❶ and ❷. ⌘

Induction is one of the major techniques that are used to prove results about matrices. We use statement ❶ to illustrate the idea of proving statements by induction. So we consider upper triangular matrices $\mathbf{M}$ and $\mathbf{N}$. If they are 2×2, then it is easily done. Now suppose they are 3×3, then $\mathbf{M}=\begin{pmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{0} & c\end{pmatrix}$ and $\mathbf{N}=\begin{pmatrix}\mathbf{X} & \mathbf{Y}\\ \mathbf{0} & z\end{pmatrix}$ where $\mathbf{A}$ and $\mathbf{X}$ are 2×2 upper triangular, and since $\mathbf{MN}=\begin{pmatrix}\mathbf{AX} & \mathbf{AY}+z\mathbf{B}\\ \mathbf{0} & cz\end{pmatrix}$ we can claim the theorem is true since we know that $\mathbf{AX}$ is upper triangular with the respective product of the diagonal entries on the main diagonal. So now we know the theorem is true for 3×3's. So let $\mathbf{M}$ and $\mathbf{N}$ be 4×4, then $\mathbf{M}=\begin{pmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{0} & c\end{pmatrix}$ and $\mathbf{N}=\begin{pmatrix}\mathbf{X} & \mathbf{Y}\\ \mathbf{0} & z\end{pmatrix}$ where $\mathbf{A}$ and $\mathbf{X}$ are 3×3 upper triangular et cetera.

In a formal proof by induction one goes from the $n\times n$ case to the $n+1\times n+1$ one, and thus one proves it for all cases.

❺ Inverses

In this section we will concentrate almost exclusively on square matrices. Such a matrix $\mathbf{A}$ is called **invertible** if there is a matrix $\mathbf{X}$ such that $\mathbf{AX} = \mathbf{I} = \mathbf{XA}$. If such a matrix $\mathbf{X}$ exists it will be referred to as an **inverse** of $\mathbf{A}$. The indefinite article **an** will be proven to be definite **the** soon below.

Example 1. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}$ and let $\mathbf{X} = \frac{1}{24}\begin{pmatrix} 24 & -12 & -2 \\ 0 & 6 & -5 \\ 0 & 0 & 4 \end{pmatrix}$. Then readily, $\mathbf{AX} = \mathbf{I} = \mathbf{XA}$.

Or if $\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$, then $\mathbf{X} = \frac{1}{6}\begin{pmatrix} 6 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ satisfies $\mathbf{AX} = \mathbf{I} = \mathbf{XA}$.

Inverse Fact #1. The inverse of $\mathbf{I}$ is $\mathbf{I}$. The identity is invertible, and its inverse is itself.

Proof. Trivially, $\mathbf{II} = \mathbf{I}$. ⌘

Inverse Fact #2. The inverse is unique. For any square matrix $\mathbf{A}$, there can be at most one matrix $\mathbf{X}$ such that $\mathbf{AX} = \mathbf{I} = \mathbf{XA}$.

Proof. Suppose that we have that both $\mathbf{X}$ and $\mathbf{Y}$ work, namely, suppose we have that both $\mathbf{AX} = \mathbf{I} = \mathbf{XA}$ and $\mathbf{AY} = \mathbf{I} = \mathbf{YA}$. We show that $\mathbf{X} = \mathbf{Y}$. The argument is a one-liner:

$$\mathbf{X} = \mathbf{XI} = \mathbf{X}(\mathbf{AY}) = (\mathbf{XA})\mathbf{Y} = \mathbf{IY} = \mathbf{Y}.$$ ⌘

Thus, we are entitled to refer to $\mathbf{X}$ (provided it exists for a given $\mathbf{A}$) as **the inverse** of $\mathbf{A}$, and, naturally, one refers to it as $\mathbf{A}^{-1}$. This allows us to extend, for any invertible matrix, the fundamental **law of exponents**:

$$\mathbf{A}^n\mathbf{A}^m = \mathbf{A}^{n+m} \text{ for any integers } n \text{ and } m.$$

Inverse Fact #3. The inverse is really unique. For any invertible matrix $\mathbf{A}$, if $\mathbf{AX} = \mathbf{I}$, or $\mathbf{XA} = \mathbf{I}$, then $\mathbf{X} = \mathbf{A}^{-1}$.

Proof. Suppose that $\mathbf{AX} = \mathbf{I}$, then multiplying on the left by $\mathbf{A}^{-1}$, we get $\mathbf{A}^{-1}(\mathbf{AX}) = \mathbf{A}^{-1}\mathbf{I}$, and so $(\mathbf{A}^{-1}\mathbf{A})\mathbf{X} = \mathbf{A}^{-1}$, but that means $\mathbf{X} = \mathbf{A}^{-1}$. Similarly, for the other side. ⌘

We should remark that we assumed here that $\mathbf{A}$ was invertible. Below we will prove a much deeper theorem that drops that assumption.

Inverse Fact #4. The inverse of the inverse is itself. Let $\mathbf{A}$ be invertible. Then so is $\mathbf{A}^{-1}$, and $(\mathbf{A}^{-1})^{-1} = \mathbf{A}$.

Proof. Since $\mathbf{AA}^{-1} = \mathbf{I} = \mathbf{A}^{-1}\mathbf{A}$, this is obvious. ⌘

Inverse Fact #5. The inverse of the transpose is the transpose of the inverse. Let $\mathbf{A}$ be invertible. Then so is $\mathbf{A}^{\mathrm{T}}$, and $\left(\mathbf{A}^{\mathrm{T}}\right)^{-1} = \left(\mathbf{A}^{-1}\right)^{\mathrm{T}}$.

Proof. We have the equations, $\mathbf{AA}^{-1} = \mathbf{I} = \mathbf{A}^{-1}\mathbf{A}$, and so if we transpose them, we get $\left(\mathbf{AA}^{-1}\right)^{\mathrm{T}} = \mathbf{I}^{\mathrm{T}} = \left(\mathbf{A}^{-1}\mathbf{A}\right)^{\mathrm{T}}$, and so $\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{A}^{\mathrm{T}} = \mathbf{I} = \mathbf{A}^{\mathrm{T}}\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}$, done. ⌘

So, for example, if $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}$, then $\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 4 & 0 \\ 3 & 5 & 6 \end{pmatrix}$, and so $\left(\mathbf{A}^{\mathrm{T}}\right)^{-1} = \dfrac{1}{24}\begin{pmatrix} 24 & 0 & 0 \\ -12 & 6 & 0 \\ -2 & -5 & 4 \end{pmatrix}$.

Inverse Fact #6. The inverse of a product is the product of the inverses in reverse order. Let $\mathbf{A}$ and $\mathbf{B}$ be invertible. Then so is $\mathbf{AB}$ and $\left(\mathbf{AB}\right)^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$.

Proof. Associativity comes to our rescue one more time in a brief argument:

$$\left(\mathbf{AB}\right)\left(\mathbf{B}^{-1}\mathbf{A}^{-1}\right) = \mathbf{A}\left(\mathbf{BB}^{-1}\right)\mathbf{A}^{-1} = \mathbf{AIA}^{-1} = \mathbf{AA}^{-1} = \mathbf{I}.$$

Similarly for $\left(\mathbf{B}^{-1}\mathbf{A}^{-1}\right)\left(\mathbf{AB}\right) = \mathbf{I}$. ⌘

Example 2. Diagonal Matrices. Given the way diagonal matrices multiply, it is clear that if all the entries of a diagonal matrix are nonzero, then it is invertible and its inverse is the diagonal matrix with the reciprocal of its entries in the respective order. Thus, if $\mathbf{A} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$, then $\mathbf{A}^{-1} = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix} = \dfrac{1}{12}\begin{pmatrix} 6 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. After the next fact, one can see that the converse is also true, namely, **if one of the entries of a diagonal matrix is 0, the matrix is not invertible**.

Example 3. Permutation Matrices. Let n be a positive integer. A square matrix of size n is called a **permutation matrix** if and only if it is (0,1) and every row and every column has exactly one 1. For example, obviously $\mathbf{I}_n$ is always a permutation. For $n = 2$, there is only one other permutation matrix, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. For $n = 3$, besides the identity, we have 5 others, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. In general, we have

① There are $n!$ permutation matrices of size n.

The reason for this is that we have n choices for putting the 1 in the first row. But then we only have $n-1$ choices for the 1 in the second row, and then $n-2$ for the third row, etcetera. ⌘

② Every permutation $\mathbf{P}$ is invertible, and in fact $\mathbf{P}^{-1} = \mathbf{P}^{\mathrm{T}}$.

We just need to argue that $\mathbf{P}\mathbf{P}^{\mathrm{T}} = \mathbf{I} = \mathbf{P}^{\mathrm{T}}\mathbf{P}$. But we saw before that $\mathbf{P}\mathbf{P}^{\mathrm{T}}$ is the matrix that has the dot product of any two rows of **P** for its entries while in the main diagonal we have the dot product of a row with itself. But since every row of **P** only has one 1 in it, we have 1's in the diagonal of $\mathbf{P}\mathbf{P}^{\mathrm{T}}$. But also since two rows do not have any 1's in common (there is only one 1 in a column), any two rows have dot product 0, and so we get $\mathbf{P}\mathbf{P}^{\mathrm{T}} = \mathbf{I}$. Similarly, for $\mathbf{P}^{\mathrm{T}}\mathbf{P}$. ⌘

By simple multiplication we get the following important claim:

③ If $\mathbf{A}$ is $m \times n$ and **P** is a permutation of size n, then $\mathbf{AP}$ has exactly the same columns as **A**, except they have been rearranged (or permuted) by **P**. And if **Q** is a permutation of size m then $\mathbf{QA}$ has the same rows as **A**, except they have been rearranged (or permuted) by **Q**.

As an immediate consequence of ③, we get

④ If **P** and **Q** are permutations of size n, then so is $\mathbf{PQ}$.

Of course, note that $(\mathbf{PQ})^{-1} = (\mathbf{PQ})^{\mathrm{T}} = \mathbf{Q}^{\mathrm{T}}\mathbf{P}^{\mathrm{T}} = \mathbf{Q}^{-1}\mathbf{P}^{-1}$.

Among the permutation matrices, the simplest ones are the **swaps**, which arise by simply swapping (exchanging places) two rows of the identity matrix, or, what is equivalent, two columns of the identity. Of course, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a swap. For $n = 3$, the swaps are $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. There are 6 swaps for $n = 4$, $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ is one of them.

Observe that all the swaps are symmetric matrices.

Example 4. Is the matrix $\mathbf{A} = \begin{pmatrix} 0 & 0 & 2 \\ 3 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}$ invertible? Since $\mathbf{A} = \mathbf{PD}$ where $\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and $\mathbf{D} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, we have that $\mathbf{A}^{-1} = \mathbf{D}^{-1}\mathbf{P}^{-1} = \mathbf{D}^{-1}\mathbf{P}^{\mathrm{T}} = \begin{pmatrix} 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{4} \\ \frac{1}{2} & 0 & 0 \end{pmatrix}$. Observe that **A** also equals **EP** where $\mathbf{E} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$.

The following fact is easily understood, but its more subtle implications will be further appreciated later. Obviously, $\mathbf{A} \times \mathbf{0} = \mathbf{0}$, but as we have seen before it is possible for the product of two matrices to be $\mathbf{0}$ without either of them being $\mathbf{0}$. However, when the matrix is invertible, it cannot even annihilate a single nonzero vector.

Inverse Fact #7. Cancellation. Suppose $\mathbf{A}$ is invertible. Then the following hold:

❶ If $\mathbf{Au} = \mathbf{0}$, then $\mathbf{u} = \mathbf{0}$.

❷ If $\mathbf{AB} = \mathbf{0}$, then $\mathbf{B} = \mathbf{0}$.

❸ If $\mathbf{AB} = \mathbf{AC}$, then $\mathbf{B} = \mathbf{C}$.

Proof. Suppose $\mathbf{Au} = \mathbf{0}$, and $\mathbf{A}$ is invertible. Then $\mathbf{u} = \mathbf{Iu} = \mathbf{A}^{-1}\mathbf{Au} = \mathbf{A}^{-1}\mathbf{0} = \mathbf{0}$. The second claim follows by considering each column of $\mathbf{B}$ and applying ❶. The last claim follows from $\mathbf{A}(\mathbf{B} - \mathbf{C}) = \mathbf{0}$. ⌘

Inverse Fact #8. The inverse of a 2×2. Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $\mathbf{A}$ is invertible if and only if $ad - bc \neq 0$. If this is the case, then

$$\mathbf{A}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Proof. For any matrix **A**, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If we assume that $ad - bc \neq 0$. Then we immediately get that

$$\mathbf{A}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

If, conversely, $ad - bc = 0$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \mathbf{0}$, and if $\mathbf{A}$ were invertible, then by cancellation we would get that $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \mathbf{0}$ which clearly implies $\mathbf{A} = \mathbf{0}$, which is clearly nonsense. ⌘

Example 5. Let $\mathbf{A} = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix}$, then $\mathbf{A}^{-1} = \frac{1}{5}\begin{pmatrix} 2 & -3 \\ -1 & 4 \end{pmatrix}$.

Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then the expression $ad - bc$ is known as the **determinant** of $\mathbf{A}$, and it will be of some consequence in the future. It is usually denoted by $\det \mathbf{A}$. Now we can restate the previous fact as

$$\mathbf{A} \text{ is invertible if and only if } \det \mathbf{A} \neq 0.$$

As we will see in a future chapter, this is a general theorem about matrices. At present we will only extend the theorem to the 3×3 case. Consider a 3×3 matrix. How is its determinant defined? Let $\mathbf{A}=\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$, then

$$\det \mathbf{A} = aei + bfg + cdh - ceg - afh - bdi\,.$$

If the expression seems difficult to remember, one way to encase it is as follows, repeat the first two columns, and one can see three diagonals (with three elements each) that go from upper left to lower right and another three diagonals that go from upper right to lower left:

$$\begin{array}{ccccccccc} a & & b & & c & & a & & b \\ & \searrow & & \searrow & & \searrow & & & \\ d & & e & & f & & d & & e \\ & & & \searrow & & \searrow & & \searrow & \\ g & & h & & i & & g & & h \end{array} \qquad \begin{array}{ccccccccc} a & & b & & c & & a & & b \\ & & & \swarrow & & \swarrow & & \swarrow & \\ d & & e & & f & & d & & e \\ & \swarrow & & \swarrow & & \swarrow & & & \\ g & & h & & i & & g & & h \end{array}$$

and one can see that the determinant is the sum of the products of the diagonal terms, the first set with a positive sign and the second set with a negative sign. For the future, there is another way to see this determinant—which we now discuss. We need two things though.

First a position in a (square) matrix is **even** if the sum of the row it is in and the column it is in is an even number. Equivalently, a position is even if the row and the column agree in parity, they are both even or they are both odd. If a position is not even, then it is **odd**. Note that the main diagonal has all even positions, and also observe that next to an even in a row or a column is odd. Thus in a 3×3, the positions are as follows, $\begin{pmatrix} \mathsf{e} & \mathsf{o} & \mathsf{e} \\ \mathsf{o} & \mathsf{e} & \mathsf{o} \\ \mathsf{e} & \mathsf{o} & \mathsf{e} \end{pmatrix}$.

The other idea is that of a **subdeterminant**. Given a position of a square matrix, if one scratches out the row and the column, one obtains a smaller matrix, and one where we already know (hopefully) how to compute a determinant, so this determinant is a subdeterminant of the original one. For example, suppose we take $\mathbf{A}=\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$. Then we will build a new matrix by putting in a position the subdeterminant obtained when we scratch the row and column of that position. If we do that we obtain the following matrix:

$$\begin{pmatrix} ei-fh & di-fg & dh-eg \\ bi-ch & ai-cg & ah-bg \\ bf-ce & af-cd & ae-bd \end{pmatrix},$$

and if we transpose this matrix of subdeterminants, and change the sign of every position that is odd, then we obtain the following matrix

$$\mathbf{X}=\begin{pmatrix} ei-fh & ch-bi & bf-ce \\ fg-di & ai-cg & cd-af \\ dh-eg & bg-ah & ae-bd \end{pmatrix}.$$

And the fundamental fact is that

$$\mathbf{AX}=\mathbf{XA}=(\det \mathbf{A})\mathbf{I},$$

which is straightforward to verify. In particular, if $\det \mathbf{A}\neq 0$, then $\mathbf{A}$ is invertible and

$$\mathbf{A}^{-1}=\frac{1}{\det \mathbf{A}}\mathbf{X}.$$

This is the 3×3 extension of a fact seen about 2×2 matrices. Thus we have proven one direction of the following

Inverse Fact #9. The inverse of a 3×3. Let $\mathbf{A}=\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$. Then $\mathbf{A}$ is invertible if and only if $\det \mathbf{A}\neq 0$.

Proof. We saw above that if $\det \mathbf{A}\neq 0$, then $\mathbf{A}^{-1}=\frac{1}{\det \mathbf{A}}\mathbf{X}$ where the matrix is as given

$$\mathbf{X}=\begin{pmatrix} ei-fh & ch-bi & bf-ce \\ fg-di & ai-cg & cd-af \\ dh-eg & bg-ah & ae-bd \end{pmatrix},$$

but in any case we have that $\mathbf{AX}=\mathbf{XA}=(\det \mathbf{A})\mathbf{I}$. For the converse, assume, by way of contradiction that $\mathbf{A}$ is invertible and $\det \mathbf{A}=0$. But since then $\mathbf{AX}=\mathbf{XA}=\mathbf{0}$, we must have that $\mathbf{X}=\mathbf{0}$. Now $\begin{pmatrix} 0 & -i & f \end{pmatrix}\mathbf{A}=\begin{pmatrix} -id+fg & -ie+fh & 0 \end{pmatrix}=\mathbf{0}$, and so we must have that $i=f=0$. Similarly, $\begin{pmatrix} -i & 0 & c \end{pmatrix}\mathbf{A}=\mathbf{0}$. But now we do have a contradiction since we have that $\mathbf{A}\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}=\mathbf{0}$, which is impossible if $\mathbf{A}$ is invertible. ⌘

Example 6. Let $\mathbf{A}=\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$, then $\det \mathbf{A}=0$, and indeed, $\mathbf{B}=\begin{pmatrix} -3 & 6 & -3 \\ 6 & -12 & 6 \\ -3 & 6 & -3 \end{pmatrix}$ satisfies $\mathbf{AB}=\mathbf{BA}=\mathbf{0}$.

Let $\mathbf{A}=\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 10 \end{pmatrix}$, then $\det \mathbf{A}=-3$, and indeed, $\mathbf{B}=\begin{pmatrix} 2 & 2 & -3 \\ 4 & -11 & 6 \\ -3 & 6 & -3 \end{pmatrix}$ satisfies $\mathbf{AB}=\mathbf{BA}=-3\mathbf{I}$. Thus, $\mathbf{A}^{-1}=\frac{-1}{3}\mathbf{B}$.

Next we observe an unexpected connection between invertibility and polynomials a matrix satisfies.

> **Inverse Fact #10. Inverses & Polynomials.** Let $\mathbf{A}$ be a square matrix. Let $p(x)$ be a polynomial that $\mathbf{A}$ satisfies, $p(\mathbf{A})=\mathbf{0}$. If $p(0)\neq 0$, then $\mathbf{A}$ is invertible.

Proof. Suppose $p(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$, and since $p(0)\neq 0$, $a_0\neq 0$. Then since $p(\mathbf{A})=\mathbf{0}$, we have $\mathbf{0}=a_0\mathbf{I}+a_1\mathbf{A}+a_2\mathbf{A}^2+\cdots+a_n\mathbf{A}^n$. Dividing by a_0 and isolating $\mathbf{I}$, we have $\mathbf{I}=-\frac{a_1}{a_0}\mathbf{A}-\frac{a_2}{a_0}\mathbf{A}^2-\cdots-\frac{a_n}{a_0}\mathbf{A}^n=\mathbf{AX}$ where $\mathbf{X}=-\frac{a_1}{a_0}\mathbf{I}-\frac{a_2}{a_0}\mathbf{A}-\cdots-\frac{a_n}{a_0}\mathbf{A}^{n-1}$. Moreover since $\mathbf{X}$ is a polynomial in $\mathbf{A}$, they commute, and so $\mathbf{X}=\mathbf{A}^{-1}$. ⌘

Note that the theorem not only tells us the inverse exists, but also how to find it.

Example 7. Let $\mathbf{A}$ be the adjacency matrix of the Petersen graph. So we know that $\mathbf{A}^2+\mathbf{A}=2\mathbf{I}_{10}+\mathbf{J}_{10}$ and also $\mathbf{AJ}_{10}=3\mathbf{J}_{10}=\mathbf{J}_{10}\mathbf{A}$ since there are 3 ones in each row and each column of $\mathbf{A}$. Multiplying $\mathbf{A}^2+\mathbf{A}=2\mathbf{I}_{10}+\mathbf{J}_{10}$ by $\mathbf{A}-3\mathbf{I}$, since $(\mathbf{A}-3\mathbf{I})\mathbf{J}=\mathbf{AJ}-3\mathbf{J}=\mathbf{0}$, we get that $(\mathbf{A}-3\mathbf{I})(\mathbf{A}^2+\mathbf{A})=(\mathbf{A}-3\mathbf{I})2\mathbf{I}$, and so $\mathbf{A}^3+\mathbf{A}^2-3\mathbf{A}^2-3\mathbf{A}-2\mathbf{A}+6\mathbf{I}=\mathbf{0}$, or $\mathbf{A}^3-2\mathbf{A}^2-5\mathbf{A}+6\mathbf{I}=\mathbf{0}$, so

$$\mathbf{A}^{-1}=-\tfrac{1}{6}\left(\mathbf{A}^2-2\mathbf{A}-5\mathbf{I}\right)=-\tfrac{1}{6}\left(2\mathbf{I}+\mathbf{J}-\mathbf{A}-2\mathbf{A}-5\mathbf{I}\right)=-\tfrac{1}{6}\left(\mathbf{J}-3\mathbf{A}-3\mathbf{I}\right).$$

The last claim can also be readily verified given that we know that $\mathbf{A}^2+\mathbf{A}=2\mathbf{I}_{10}+\mathbf{J}_{10}$.

We have encountered upper triangular matrices before, we now pursue their invertibility properties. The next lemma is very useful

> **Lemma.** Let $\mathbf{M}=\begin{pmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{0} & \mathbf{C}\end{pmatrix}$ be block upper triangular where $\mathbf{A}$ and $\mathbf{C}$ are square (not necessarily of the same size). If $\mathbf{A}$ and $\mathbf{C}$ are invertible, then so is $\mathbf{M}$, and then $\mathbf{M}^{-1}=\begin{pmatrix}\mathbf{A}^{-1} & -\mathbf{A}^{-1}\mathbf{BC}^{-1}\\ \mathbf{0} & \mathbf{C}^{-1}\end{pmatrix}$.

Proof. The proof is straightforward. Start by assuming that $\mathbf{A}$ and $\mathbf{C}$ are invertible. Observe that if $\mathbf{A}$ is $n\times n$ and $\mathbf{C}$ is $m\times m$, then $\mathbf{B}$ is $n\times m$, and the expression $\mathbf{A}^{-1}\mathbf{BC}^{-1}$ makes sense. But, then $\mathbf{M}\begin{pmatrix}\mathbf{A}^{-1} & -\mathbf{A}^{-1}\mathbf{BC}^{-1}\\ \mathbf{0} & \mathbf{C}^{-1}\end{pmatrix}=\mathbf{I}=\begin{pmatrix}\mathbf{A}^{-1} & -\mathbf{A}^{-1}\mathbf{BC}^{-1}\\ \mathbf{0} & \mathbf{C}^{-1}\end{pmatrix}\mathbf{M}$ are both trivially verified. ⌘

Example 8. Let $\mathbf{A}$ be the adjacency matrix of the Petersen graph. Let $\mathbf{M}=\begin{pmatrix}\mathbf{A} & \mathbf{J}_{10\times 2}\\ \mathbf{0} & \mathbf{I}_2\end{pmatrix}$.

Then $\mathbf{M}$ is invertible, and $\mathbf{M}^{-1}=\begin{pmatrix}\mathbf{A}^{-1} & -\mathbf{A}^{-1}\mathbf{B}\mathbf{C}^{-1}\\ \mathbf{0} & \mathbf{C}^{-1}\end{pmatrix}=\begin{pmatrix}\frac{1}{2}\mathbf{A}+\frac{1}{2}\mathbf{I}-\frac{1}{6}\mathbf{J} & -\frac{1}{3}\mathbf{J}\\ \mathbf{0} & \mathbf{I}\end{pmatrix}$.

Below we will prove the converse to this lemma, which is also of great utility. Of course, the lemma only extends easily to a very useful theorem. This theorem is a simple generalization of the diagonal matrix example above—it is the extension to block diagonal.

> **Theorem. (Block Upper Triangular).** Let $\mathbf{M}=\begin{pmatrix}\mathbf{A}_{11} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1t}\\ \mathbf{0} & \mathbf{A}_{22} & \cdots & \mathbf{A}_{2t}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{A}_{tt}\end{pmatrix}$ be in balanced block upper triangular form. If each of the diagonal blocks is invertible, then so is $\mathbf{M}$. Moreover, if that is the case, then $\mathbf{M}^{-1}$ is also block upper triangular and its diagonal entries are the respective inverses of the diagonal entries.

Proof. Not surprisingly, the proof is by induction on the number of blocks, t. If $t=1$, there is nothing to prove. The very important case of $t=2$ was dealt with in the lemma. But actually, the lemma does all the work. Suppose the theorem hold for $t-1$, then visualize $\mathbf{M}$ in the form $\mathbf{M}=\begin{pmatrix}\mathbf{X} & \mathbf{Y}\\ \mathbf{0} & \mathbf{Z}\end{pmatrix}$ where $\mathbf{X}=\begin{pmatrix}\mathbf{A}_{11} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1t-1}\\ \mathbf{0} & \mathbf{A}_{22} & \cdots & \mathbf{A}_{2t-1}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{A}_{t-1t-1}\end{pmatrix}$, $\mathbf{Y}=\begin{pmatrix}\mathbf{A}_{1t}\\ \mathbf{A}_{2t}\\ \vdots\\ \mathbf{A}_{tt}\end{pmatrix}$ and $\mathbf{Z}=\mathbf{A}_{tt}$. Once we do that the result will follow readily from the lemma by induction. ⌘

Again, the converse of this theorem is true and will be proven below.

Example 17 above exemplifies the next corollary. One direction of the corollary is just the theorem applied to the case when the diagonal blocks are 1×1. The other direction follows from the **one side suffices** theorem below.

> **Corollary (Upper Triangular and Inverses).** An upper triangular matrix $\mathbf{A}$ is invertible exactly when all of its diagonal entries are nonzero. Moreover, if that is the case, $\mathbf{A}^{-1}$ is also upper triangular and its diagonal will consist of the reciprocals of the diagonal entries of $\mathbf{A}$.

In the diagonal case,

Corollary (Diagonal Matrices). A diagonal matrix $\mathbf{A}$ is invertible if and only if all of its diagonal entries are nonzero. Moreover, if that is the case, $\mathbf{A}^{-1}$ is just the diagonal matrix of the reciprocals of the diagonal entries of $\mathbf{A}$.

And we now arrive at the deepest theorem of the section, which is truly surprising in the sense that all we need is to multiply on one side to check whether something is the inverse of something else.

Theorem (One Side Suffices). Let $\mathbf{A}$ be square. If $\mathbf{AX}=\mathbf{I}$, then $\mathbf{A}$ is invertible and, as before, $\mathbf{X}=\mathbf{A}^{-1}$.

The challenging proof of this theorem can be found in the Appendix.

Corollary (Either Side). Let $\mathbf{A}$ be square. If $\mathbf{XA}=\mathbf{I}$, then $\mathbf{A}$ is invertible and $\mathbf{X}=\mathbf{A}^{-1}$.

Proof. Since $\mathbf{X}$ is square and $\mathbf{XA}=\mathbf{I}$, we can apply the theorem to $\mathbf{X}$, and so we know that $\mathbf{X}$ is invertible, and $\mathbf{A}=\mathbf{X}^{-1}$. ⌘

Example 9. The purpose of this example is to show that the square hypothesis is necessary to make full sense of the theorem. Let $\mathbf{A}=\begin{pmatrix}1&0&0\\0&1&0\end{pmatrix}$ and let $\mathbf{B}=\begin{pmatrix}1&0\\0&1\\0&0\end{pmatrix}$. Then $\mathbf{AB}=\mathbf{I}_2$, but, of course, $\mathbf{BA}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}$. More importantly, there does not exist a matrix $\mathbf{C}$ such that $\mathbf{CA}=\mathbf{I}_3$.

Now we are in a position to prove the converses of the triangularity lemmas and theorem before.

Corollary. Let $\mathbf{M}=\begin{pmatrix}\mathbf{A}&\mathbf{B}\\\mathbf{O}&\mathbf{C}\end{pmatrix}$ be block upper triangular where $\mathbf{A}$ and $\mathbf{C}$ are square (not necessarily of the same size). If $\mathbf{M}$ is invertible, then so are $\mathbf{A}$ and $\mathbf{C}$.

Proof. Assume that $\mathbf{M}$ is invertible. We need to show that $\mathbf{A}$ and $\mathbf{C}$ are invertible. Let $\mathbf{M}^{-1}=\begin{pmatrix}\mathbf{X}&\mathbf{Y}\\\mathbf{Z}&\mathbf{W}\end{pmatrix}$. Then by multiplying $\mathbf{MM}^{-1}$, we get that $\begin{pmatrix}\mathbf{AX}+\mathbf{BZ}&\mathbf{AY}+\mathbf{BW}\\\mathbf{CZ}&\mathbf{CW}\end{pmatrix}=\mathbf{I}$. By looking at the second row, we get $\mathbf{CW} = \mathbf{I}$ and $\mathbf{CZ} = \mathbf{0}$. So, by the theorem, we have that $\mathbf{C}$ is invertible, and so $\mathbf{Z} = \mathbf{0}$ (by **Fact 7** above). But now $\mathbf{AX} = \mathbf{I}$, and we are done. ⌘

We finish the section with a frivolous but entertaining application of inverses.

Example 10. ***Cryptography: An application of inverses.*** One can use matrices to encode messages by the simple act of multiplying by a given matrix. The idea is very simple. Suppose we are given a message:

MENA IS FABULOUS.

then one can use the simple conversion of letter to number to encode it:

1	2	3	4	5	6	7	8	9	10	11	12	13
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
14	15	16	17	18	19	20	21	22	23	24	25	26
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

and 0 is a blank.

So the message becomes (if one is tight in space or memory, one could ignore blanks since those are usually easily deducible from context):

13 5 14 1 0 9 19 0 6
1 2 21 12 15 21 19

The problem with this simple encoding is that everyone can figure what the message was.

A little more interesting is that given any matrix (which is of course supposed to be hidden from the enemy), one simply multiplies by that matrix to encode.
For example, suppose we use the matrix

2	5	2	1
3	1	4	7
1	2	1	1
1	1	1	1

Then we would multiply the matrix by the message, which when **transformed into column vectors** becomes:

13	0	6	12
5	9	1	15
14	19	2	21
1	0	21	19

and we would obtain the encoded message

80 107 38 33 83 85 37 28 42 174
31 30 160 268 82 67

which already is not readily decipherable without the matrix. But one can go further, and do what is called modular arithmetic[1] and reduce these numbers mod 27 (26 letters and a space), and obtain the modified message

26 26 11 6 2 4 10 1 15
12 4 3 25 25 1 13

which in turn can be changed to letters, and therefore would be even more confusing to the enemy:

Z Z K F B D J A O L
D C Y Y A M.

To decode the message, one would have to reverse the process—change the received letters to numbers, multiply them by the inverse of the original matrix, reduce them mod 27, and then change the numbers back to letters—only then we would receive our original message. Of course, without knowing the matrix it is rather difficult.

Specifically, we would get the received message:

26	2	15	25
26	4	12	25
11	10	4	1
6	1	3	13

and multiply it by the inverse of our original matrix:

-3	-1	6	4
0	0	1	-1
4	1	-10	-1
-1	0	3	-1

to obtain the sent message before running through the mod 27 reduction:

-14	54	-21	-42
5	9	1	-12
14	-89	29	102
1	27	-6	-35

[1] To do arithmetic mod 27, one simply divides by 27 and obtains the remainder, *e.g.*, 89=3*27+8—Most calculators have the mod function built into them, the usual syntax is, *e.g.*, mod(89, 27)=8.

❻ Row Reduction & Linear Equations

So far we have discussed the arithmetic of matrices. In this section we begin to discuss the` algebra of matrices. What is the simplest equation in everybody's past? Probably something like $15x = 60$. And what was the process of solving it? Simple, both sides of the equation get multiplied by $\frac{1}{15}$, and we arrive at the simple solution $x = 4$. We intend to solve the same level of equation for matrices, but because we have size now to consider it we discuss it further.

In fact the most basic equation of matrices (as with numbers) is the linear equation, and so the most basic matrix equation is

$$\mathbf{Ax} = \mathbf{b}$$

where $\mathbf{A}$ is an $m \times n$ matrix and $\mathbf{b}$ is an $m \times 1$ vector. Of course $\mathbf{x}$ is our unknown. In fact we refer to them as follows, $\mathbf{A}$ is the **matrix of coefficients**, $\mathbf{x}$ is the **unknown** and $\mathbf{b}$ is the **constant vector**.

The acute reader may suggest we are short-charging ourselves by not looking at the more general true matrix equation

$$\mathbf{AX} = \mathbf{B}$$

where $\mathbf{A}$ is an $m \times n$ matrix and $\mathbf{B}$ is an $m \times p$ matrix, and thus our unknown would be an $n \times p$ matrix. But the even more acute reader would realize that by solving $\mathbf{Ax} = \mathbf{b}$ for each of the columns of $\mathbf{B}$ we would (by simple matrix multiplication) be solving the more general equation $\mathbf{AX} = \mathbf{B}$ since we would be finding the columns of $\mathbf{X}$ one at a time.

For example, in order to solve $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}\mathbf{X} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, we would equivalently have to solve the two simpler equations $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}\mathbf{x} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}\mathbf{x} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$, and if $\mathbf{u} = \frac{1}{3}\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ and $\mathbf{v} = \frac{1}{3}\begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix}$, for example, are respective solutions to these two equations, then the 3×2 matrix $\begin{pmatrix} \mathbf{u} & \mathbf{v} \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 1 & 1 \\ 1 & -2 \\ 0 & 3 \end{pmatrix}$ will be a solution to the original system.

And of course if one wanted to solve an equation of the form $\mathbf{XA} = \mathbf{B}$, transposing would lead us to a previous form—finally, if we wanted to solve the more general linear equation on one unknown $\mathbf{AX} + \mathbf{C} = \mathbf{B}$, that immediately reduces to $\mathbf{AX} = \mathbf{B} - \mathbf{C}$. Thus we come to the conclusion that by being able to solve the ancient

$$\mathbf{Ax} = \mathbf{b},$$

one is able to solve any linear matrix equation in one unknown.

But even more is true. Suppose $\mathbf{A}$ is $m\times n$ and $\mathbf{B}$ is $m\times p$ and $\mathbf{C}$ is $m\times q$. We could consider the linear equation on two unknowns,

$$\mathbf{AX}+\mathbf{BY}=\mathbf{C}$$

where $\mathbf{X}$ is an $n\times q$ unknown and $\mathbf{Y}$ is $p\times q$ unknown. But the equation $\mathbf{AX}+\mathbf{BY}=\mathbf{C}$ is equivalent to the equation $\mathbf{DZ}=\mathbf{C}$ where $\mathbf{D}$ is the horizontal stacking of $\mathbf{A}$ and $\mathbf{B}$, $\mathbf{D}=\begin{pmatrix}\mathbf{A} & \mathbf{B}\end{pmatrix}$, and thus $\mathbf{Z}$ becomes an $(n+p)\times q$ unknown, the vertical stacking of our two previous unknowns, $\mathbf{Z}=\begin{pmatrix}\mathbf{X}\\ \mathbf{Y}\end{pmatrix}$. And in turn $\mathbf{DZ}=\mathbf{C}$ can be reduced to an equation of the form $\mathbf{Ax}=\mathbf{b}$. Thus the ability to solve the equation $\mathbf{Ax}=\mathbf{b}$ entitles us to solve any linear equation involving matrices.

Thus we concentrate on the equation $\mathbf{Ax}=\mathbf{b}$.

The most important first observation follows from the analysis of the equation for numbers. Namely the equation following $15x=60$ carries the same information as $-15x=-60$, or $30x=120$, or $150x=600$. Of course, of all of these, we chose $x=4$ as to represent the solution since it is the one where the information is most transparent, clearest. But in fact all of these equations are the same equation. Of course, the one number we could not have multiplied by is 0 since then we would obtain $0x=0$, which carries no information—multiplying by 0 has destroyed all the information.

From the abstract point of view, the first claim is trivial, but everlasting, since all is built into it.

> **Theorem (Equations and Inverses).** Let $\mathbf{P}$ be an invertible matrix. Then the equation $\mathbf{Ax}=\mathbf{b}$ and the equation $\mathbf{PAx}=\mathbf{Pb}$ have exactly the same solutions.

Proof. Clearly, if $\mathbf{Ax}=\mathbf{b}$, then $\mathbf{PAx}=\mathbf{Pb}$, and conversely, if $\mathbf{PAx}=\mathbf{Pb}$, then

$$\mathbf{Ax}=\left(\mathbf{P}^{-1}\mathbf{P}\right)\mathbf{Ax}=\mathbf{P}^{-1}\left(\mathbf{PAx}\right)=\mathbf{P}^{-1}\left(\mathbf{Pb}\right)=\left(\mathbf{P}^{-1}\mathbf{P}\right)\mathbf{b}=\mathbf{b}$$

and so we are done. ⌘

Example 1. The simplest equation to solve is simply $\mathbf{Ix}=\mathbf{b}$, which of course, has the unique solution $\mathbf{x}=\mathbf{b}$.

By the same reasoning, if $\mathbf{P}$ is invertible, then $\mathbf{Px}=\mathbf{b}$ has a unique solution, $\mathbf{x}=\mathbf{P}^{-1}\mathbf{b}$. Concretely suppose we wanted to solve $\mathbf{Px}=\mathbf{b}$, $\begin{pmatrix}1&4&7\\2&5&8\\3&6&10\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}3\\-3\\4\end{pmatrix}$, then since $\mathbf{P}^{-1}=\dfrac{-1}{3}\begin{pmatrix}2&2&-3\\4&-11&6\\-3&6&-3\end{pmatrix}=\dfrac{1}{3}\begin{pmatrix}-2&-2&3\\-4&11&-6\\3&-6&3\end{pmatrix}$, we have that $\mathbf{x}=\begin{pmatrix}4\\-23\\13\end{pmatrix}$ is the unique solution.

Note that what has actually occurred in this last example is the changing of the matrix of coefficients from **A** to **I**. In fact, that is what we will systematically pursue below as much as it can be done—in the invertible case, this is of course accomplished via the inverse. But also observe we do not have yet a general technique for finding the inverse of an invertible matrix.

Above, we referred to the equation $\mathbf{Ax} = \mathbf{b}$ as ancient, and indeed it is at least 2,000 years old in China, and the process of solving linear equations goes back in China to at least **The Nine Chapters of the Arithmetic Art** which dates from the first century AD.

The method was called of **rectangular arrays**. One of their problems was the following—we should remark a **dou** is a unit of volume.

Example 2. Three bundles of top-grade ears of rice, together with two bundles of medium grade, and one bundle of low-grade ears of rice make 39 dou of rice. Also two bundles of top-grade ears of rice with three bundles of medium grade and one bundle of low-grade ears of rice make 34 dou of rice. Finally, one bundle of top-grade ears of rice, and two bundles of medium grade with three bundles of grade ears of rice make 26 dou of rice. How many dou are there in a bundle of top-grade, of medium grade, and of low-grade ears of rice?

Except that the Chinese would write the system vertically and from right to left, there is very little difference between the ancient method and our modern day method. However they do differ in age, there is more than fifteen centuries between them. Today, we would write this problem as a system of three equations on three unknowns:

$$3x + 2y + z = 39$$
$$2x + 3y + z = 34$$
$$x + 2y + 3z = 26$$

or, in matrix form, $\begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 39 \\ 34 \\ 26 \end{pmatrix}$, $\mathbf{Ax} = \mathbf{b}$, where $\mathbf{A} = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$, $\mathbf{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ and $\mathbf{b} = \begin{pmatrix} 39 \\ 34 \\ 26 \end{pmatrix}$.

In a similar fashion to the Chinese, we would now solve it using the three steps of the procedure known as **Gaussian Elimination**:

① Permuting rows;

② Multiplying a row by a nonzero number,

and most importantly

③ Adding a multiple of a row to another row.

Why are we allowed to use these three steps? Because each of them is nothing but multiplication on the left by an appropriate invertible matrix, and by the theorem above, we can do so without changing the solutions to the system.

But note that the multiplication of $\mathbf{Ax} = \mathbf{b}$ by $\mathbf{P}$ leads to $\mathbf{PAx} = \mathbf{Pb}$, and the information can easily be stored in the horizontal stacking of $\mathbf{A}$ and $\mathbf{b}$, $\begin{pmatrix}\mathbf{A} & \mathbf{b}\end{pmatrix}$, since when we multiply this matrix by $\mathbf{P}$ we get $\begin{pmatrix}\mathbf{PA} & \mathbf{Pb}\end{pmatrix}$, which is the desired information for the transformed equation. This horizontal stacking is called the **augmented matrix** of the system, and in our particular case it is given by: $\begin{pmatrix} 3 & 2 & 1 & 39 \\ 2 & 3 & 1 & 34 \\ 1 & 2 & 3 & 26 \end{pmatrix}$.

Row reduction, or simply **reduction**, is often used as a synonym for Gaussian Elimination. So we now proceed to **reduce** the matrix $\begin{pmatrix} 3 & 2 & 1 & 39 \\ 2 & 3 & 1 & 34 \\ 1 & 2 & 3 & 26 \end{pmatrix}$:

What we multiply by	Language Description of the Product	End Result
$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	Permuting the first and third rows	$\begin{pmatrix} 1 & 2 & 3 & 26 \\ 2 & 3 & 1 & 34 \\ 3 & 2 & 1 & 39 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	Subtracting twice the first row from the second row	$\begin{pmatrix} 1 & 2 & 3 & 26 \\ 0 & -1 & -5 & -18 \\ 3 & 2 & 1 & 39 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix}$	Subtracting thrice the first row from the third row	$\begin{pmatrix} 1 & 2 & 3 & 26 \\ 0 & -1 & -5 & -18 \\ 0 & -4 & -8 & -39 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	Multiplying the second row by -1	$\begin{pmatrix} 1 & 2 & 3 & 26 \\ 0 & 1 & 5 & 18 \\ 0 & -4 & -8 & -39 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix}$	Adding four times the second row to the third row	$\begin{pmatrix} 1 & 2 & 3 & 26 \\ 0 & 1 & 5 & 18 \\ 0 & 0 & 12 & 33 \end{pmatrix}$
$\begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	Subtracting twice the second row from the first:	$\begin{pmatrix} 1 & 0 & -7 & -10 \\ 0 & 1 & 5 & 18 \\ 0 & 0 & 12 & 33 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{12} \end{pmatrix}$	Dividing the third row by 12:	$\begin{pmatrix} 1 & 0 & -7 & -10 \\ 0 & 1 & 5 & 18 \\ 0 & 0 & 1 & \frac{11}{4} \end{pmatrix}$

$\begin{pmatrix}1&0&7\\0&1&0\\0&0&1\end{pmatrix}$	**Adding seven times the third row to the first:**	$\begin{pmatrix}1&0&0&\frac{37}{4}\\0&1&5&18\\0&0&1&\frac{11}{4}\end{pmatrix}$
$\begin{pmatrix}1&0&0\\0&1&-5\\0&0&1\end{pmatrix}$	**Subtracting five times the third row from the second:**	$\begin{pmatrix}1&0&0&\frac{37}{4}\\0&1&0&\frac{17}{4}\\0&0&1&\frac{11}{4}\end{pmatrix}$

Providing us with the unique solution: $\begin{pmatrix}x\\y\\z\end{pmatrix}=\frac{1}{4}\begin{pmatrix}37\\17\\11\end{pmatrix}$ since now the coefficients are nothing but the identity matrix.

Again we emphasize that this process of reduction is that of multiplication (on the left) by the appropriate matrices, and each of the three steps of Gaussian Elimination corresponds to multiplication (on the left) by a special type matrix.

The end result is that **Gaussian Elimination is equivalent to multiplication on the left by an invertible matrix**. In our example above:

$$\begin{pmatrix}1&0&0&\frac{37}{4}\\0&1&0&\frac{17}{4}\\0&0&1&\frac{11}{4}\end{pmatrix}=\frac{1}{12}\begin{pmatrix}7&-4&-1\\-5&8&-1\\1&-4&5\end{pmatrix}\begin{pmatrix}3&2&1&39\\2&3&1&34\\1&2&3&26\end{pmatrix}$$

and the matrix $\frac{1}{12}\begin{pmatrix}7&-4&-1\\-5&8&-1\\1&-4&5\end{pmatrix}$ is the sequential product of the row operations described above:

$$\frac{1}{12}\begin{pmatrix}7&-4&-1\\-5&8&-1\\1&-4&5\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&-5\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&7\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&\frac{1}{12}\end{pmatrix}\begin{pmatrix}1&-2&0\\0&1&0\\0&0&1\end{pmatrix}$$
$$\begin{pmatrix}1&0&0\\0&1&0\\0&4&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&-1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\-3&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\-2&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$$

One of the key ingredients in the process of reducing the matrix was that of transforming a nonzero column to a column of the identity. The most common way to accomplish this is to select a nonzero entry in that column, making it a 1 by dividing that row by the entry, and then zeroing all other entries in that column by adding multiples of that row to all other rows. This is called **pivoting** in that position.

Example 3. Consider the matrix $\mathbf{A}=\begin{pmatrix}1&4&7\\2&5&8\\3&6&9\end{pmatrix}$. If we pivot in the 3-2 position, we will obtain the matrix $\begin{pmatrix}-1&0&1\\-\frac{1}{2}&0&\frac{1}{2}\\\frac{1}{2}&1&\frac{3}{2}\end{pmatrix}$. The sequence of steps is as follows

Factor	Result	Factor	Result	Factor	Result
$\begin{pmatrix}1&0&0\\0&1&0\\0&0&\frac{1}{6}\end{pmatrix}$	$\begin{pmatrix}1&4&7\\2&5&8\\\frac{1}{2}&1&\frac{3}{2}\end{pmatrix}$	$\begin{pmatrix}1&0&-4\\0&1&0\\0&0&1\end{pmatrix}$	$\begin{pmatrix}-1&0&1\\2&5&8\\\frac{1}{2}&1&\frac{3}{2}\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&1&-5\\0&0&1\end{pmatrix}$	$\begin{pmatrix}-1&0&1\\-\frac{1}{2}&0&\frac{1}{2}\\\frac{1}{2}&1&\frac{3}{2}\end{pmatrix}$

so the invertible matrix that will accomplish the pivoting is:

$$\begin{pmatrix}1&0&0\\0&1&-5\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&-4\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&\frac{1}{6}\end{pmatrix}=\begin{pmatrix}1&0&-\frac{4}{6}\\0&1&-\frac{5}{6}\\0&0&\frac{1}{6}\end{pmatrix}.$$

A general observation is that **when pivoting on a position the matrix that accomplishes that reduction is the identity except for one column.**

Example 4. Not all systems have solutions. Let $\mathbf{A}=\begin{pmatrix}1\\1\\1\end{pmatrix}$ and $\mathbf{b}=\begin{pmatrix}1\\2\\3\end{pmatrix}$. Then obviously, since $\begin{pmatrix}1\\2\\3\end{pmatrix}$ is not a multiple of $\begin{pmatrix}1\\1\\1\end{pmatrix}$ the equation $\mathbf{Ax}=\mathbf{b}$ has no solution.

A little more interesting is the following.

Before we saw that $\mathbf{M}=\begin{pmatrix}1&4&7\\2&5&8\\3&6&10\end{pmatrix}$ is an invertible matrix. Consider the system $\mathbf{Ax}=\mathbf{b}$ where $\mathbf{A}=\begin{pmatrix}1&4\\2&5\\3&6\end{pmatrix}$, the first two columns of $\mathbf{M}$ and $\mathbf{b}=\begin{pmatrix}7\\8\\10\end{pmatrix}$, the third column of $\mathbf{M}$. If there were a solution to $\mathbf{Ax}=\mathbf{b}$, say $\mathbf{x}=\begin{pmatrix}a\\b\end{pmatrix}$, then we would have that $\begin{pmatrix}7\\8\\10\end{pmatrix}=a\begin{pmatrix}1\\2\\3\end{pmatrix}+b\begin{pmatrix}4\\5\\6\end{pmatrix}$, but that would imply that $\mathbf{M}\begin{pmatrix} a \\ b \\ -1 \end{pmatrix} = \mathbf{0}$, which we have seen is impossible for invertible matrix. Thus, we can claim that $\mathbf{Ax} = \mathbf{b}$ has no solutions.

In the example above we arrived at a unique solution, which, as we will see, can only happen if we had at least as many equations as unknowns. In some of our problems, this will not be the case, and thus we want to review what happens with a system in general.

A matrix **A** is said to be in (**row**) **reduced form** (or **row echelon form**, or **row reduced echelon form**) if the following 4 conditions are satisfied:

① The first nonzero term of any row is a 1. This entry is called a **pivot**, and thus every row is either all zeros or it has a unique pivot. Hence a nonzero row will be called **pivotal**, and such a row will have exactly one pivot. Conversely, every pivot is in a pivotal row.

② A column that contains a pivot, a pivotal column, has all zeroes except for the pivot. Hence any pivotal column is identical to a column of the identity matrix, and a **pivotal column** has exactly one pivot, and every pivot is in a pivotal column.

③ Any zero row is below any pivotal row.

④ The pivots in the matrix lie from upper left to lower right.

Note that the number of pivots equals both the number of nonzero rows of the reduced matrix as well as the number of pivotal columns.

Example 5. Any matrix of the form $\begin{pmatrix} 1 & * & 0 & * & 0 \\ 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ where * are arbitrary is reduced. Here the first three rows are pivotal while the pivotal columns are 1, 3 and 5. On the other hand, none of the following is in row echelon form:

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Note that requirements ③ and ④ of the reduced form are easily accomplished by simple row permutations, while ① may require multiplication by a diagonal matrix. It is requirement ② that demands the most effort, most of it being the addition of a multiple of a row to another row.

Example 6. Consider the matrix $\mathbf{A}=\begin{pmatrix}1 & * & 0 & * & 0\\ 0 & 0 & 1 & * & 0\\ 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0\end{pmatrix}$, which is reduced. For which **b**'s does the system $\mathbf{Ax}=\mathbf{b}$ have a solution? Let $\mathbf{b}=\begin{pmatrix}a\\ b\\ c\\ d\end{pmatrix}$. If we were to write the system of equations we would get (if we let our respective unknowns be x, y, z, w and u)

$$x+*y+*w=a$$
$$z+*w=b$$
$$u=c$$
$$0x+0y+0z+0w+0u=d$$

and we have a clear necessary and sufficient conditions for a solution to exist: d has to be 0, or equivalently $\mathbf{Ax}=\mathbf{b}$ will have a solution if and only if the fourth coordinate of **b** is 0. The necessity is obvious from the last equation, but the sufficiency is also clear since all we need to do is let $y=w=0$ and $x=a$, $z=b$ and $u=c$.

The example shows that for a reduced matrix the only time that we do not have a solution is when we have a row of zeroes in the matrix of coefficients but a nonzero entry in the constant vector. This example is generic as the following lemma shows, which will be needed for the major theorem below.

> **Lemma (Existence of Solutions).** Let $\mathbf{A}$ be row reduced. Take any vector **b**. Then $\mathbf{Ax}=\mathbf{b}$ has a solution if and only if **b** has a zero in every zero row of **A**.

Proof. Since **A** is reduced, we know **A** is of the form $\mathbf{A}=\begin{pmatrix}\mathbf{M}\\ \mathbf{0}\end{pmatrix}$ where actually the **0** block may be nonexistent since every row of **A** may be nonzero (if $\mathbf{A}=\mathbf{0}$, then **b** has to be **0** too, a very uninteresting case). Block **b** in the same fashion as **A**, so $\mathbf{b}=\begin{pmatrix}\mathbf{c}\\ \mathbf{d}\end{pmatrix}$. Then the claim becomes that $\mathbf{Ax}=\mathbf{b}$ has a solution if and only if $\mathbf{d}=\mathbf{0}$. One direction is clear, if $\mathbf{d}\neq\mathbf{0}$, then we are attempting to solve an equation where all the coefficients are 0, but the constant term is not 0, and that is clearly impossible. Assume then conversely, that $\mathbf{d}=\mathbf{0}$. But then for every position of **c**, we have a pivot in that row of **A**, so choose the vector **x** that has the same entry as **c** in a given row, but we put that entry in the row that corresponds to the pivotal column where the pivot from that row of **A** is. Then the vector **x** is a solution to the equation $\mathbf{Ax}=\mathbf{b}$. ⌘

This abstract description is much harder than what actually occurs. One example should suffice.

Example 7. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, and let $\mathbf{b} = \begin{pmatrix} a \\ b \\ c \\ 0 \end{pmatrix}$. Then $\mathbf{x} = \begin{pmatrix} a \\ 0 \\ b \\ 0 \\ c \end{pmatrix}$ is a solution to the equation.

Ultimately, the theorem is the **Uniqueness of the Row Echelon Form:**

> **Theorem (Uniqueness of the form).** Let **A** be an arbitrary $m \times n$ matrix. Then **A** is row equivalent to a unique matrix in row echelon form.

The proof can be found in the **Appendix of Proofs**. This is indeed a fundamental fact with many important consequences. In fact, the proof is actually algorithmic in the sense that we arrive at the reduced form by reducing one column at a time.

There are several algorithm for arriving at the reduced from of a matrix. But because of the uniqueness it is irrelevant what algorithm we adopt. One of them is as follows:

❶ Make the first column if nonzero into the first column of the identity by pivoting.

❷ Go to the next row that is not 0, and find the first column that has a nonzero entry in that row and pivot in that position.

❸ Keep repeating ❷ until there are no nonzero rows without a pivot.

❹ If necessary permute rows so properties ③ and ④ of the reduced form are taken care of.

Example 8. Let us considering reducing $\begin{pmatrix} 1 & 2 & 3 & 5 & 6 \\ 1 & 2 & 3 & 5 & 7 \\ 1 & 2 & 3 & 5 & 7 \\ 1 & 2 & 3 & 6 & 7 \\ 1 & 2 & 4 & 6 & 8 \end{pmatrix}$. Since we have a 1 in the $1,1-$position, we can start by pivoting there to obtain $\begin{pmatrix} 1 & 2 & 3 & 5 & 6 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 2 \end{pmatrix}$. Now we will pivot in the $2,5-$position, and get $\begin{pmatrix} 1 & 2 & 3 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$. Now we skip row 3 since it is all zeroes, and choose to pivot in the $4,4-$position: $\begin{pmatrix} 1 & 2 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$, and finally pivot in the $5,3-$entry, and get $\begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$, and permuting rows: $\begin{pmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

Example 9. Let $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 2 & 6 & 4 & 2 \\ 2 & 5 & 3 & 1 \\ 2 & 4 & 2 & 0 \end{pmatrix}$. Suppose we consider the systems $\mathbf{Ax} = \mathbf{b}$ and $\mathbf{Ax} = \mathbf{c}$ where $\mathbf{b} = \begin{pmatrix} -1 \\ 34 \\ 25 \\ 16 \end{pmatrix}$ and $\mathbf{c} = \begin{pmatrix} 3 \\ 13 \\ 12 \\ 10 \end{pmatrix}$. Since we are about to reduce $\begin{pmatrix} \mathbf{A} & \mathbf{b} \end{pmatrix}$ and $\begin{pmatrix} \mathbf{A} & \mathbf{c} \end{pmatrix}$ and the end result will be $\begin{pmatrix} \mathbf{PA} & \mathbf{Pb} \end{pmatrix}$ and $\begin{pmatrix} \mathbf{PA} & \mathbf{Pc} \end{pmatrix}$, where the matrix $\mathbf{P}$ is the same matrix that reduces $\mathbf{A}$, we can accomplish all the work by reducing both system at once in the form $\begin{pmatrix} \mathbf{A} & \mathbf{b} & \mathbf{c} \end{pmatrix}$. But even better, if we wanted to actually compute the matrix $\mathbf{P}$ as we do the reduction, then we should reduce the matrix $\begin{pmatrix} \mathbf{A} & \mathbf{b} & \mathbf{c} & \mathbf{I} \end{pmatrix}$, for then when we are finished we will have the matrix $\begin{pmatrix} \mathbf{PA} & \mathbf{Pb} & \mathbf{Pc} & \mathbf{P} \end{pmatrix}$, and we will know the reducing matrix. And that is what we do. We start with $\begin{pmatrix} 1 & 1 & 0 & -1 & -1 & 3 & 1 & 0 & 0 & 0 \\ 2 & 6 & 4 & 2 & 34 & 13 & 0 & 1 & 0 & 0 \\ 2 & 5 & 3 & 1 & 25 & 12 & 0 & 0 & 1 & 0 \\ 2 & 4 & 2 & 0 & 16 & 10 & 0 & 0 & 0 & 1 \end{pmatrix}$, which after pivoting in the $1,1-$position we get $\begin{pmatrix} 1 & 1 & 0 & -1 & -1 & 3 & 1 & 0 & 0 & 0 \\ 0 & 4 & 4 & 4 & 36 & 7 & -2 & 1 & 0 & 0 \\ 0 & 3 & 3 & 3 & 27 & 6 & -2 & 0 & 1 & 0 \\ 0 & 2 & 2 & 2 & 18 & 4 & -2 & 0 & 0 & 1 \end{pmatrix}$, and then if we pivot in the $2,2-$position, we have $\begin{pmatrix} 1 & 0 & -1 & -2 & -10 & 1.25 & 1.5 & -0.25 & 0 & 0 \\ 0 & 1 & 1 & 1 & 9 & 1.75 & -0.5 & 0.25 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.75 & -0.5 & -0.75 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & -1 & -0.5 & 0 & 1 \end{pmatrix}$. And although the matrix we see is not reduced we stop, because $\mathbf{A}$ is reduced. Moreover, we can see that the system $\mathbf{Ax} = \mathbf{b}$ has a solution, $\begin{pmatrix} -10 \\ 9 \\ 0 \\ 0 \end{pmatrix}$. Also $\mathbf{Ax} = \mathbf{c}$ does not since there is a nonzero entry in the third row of $\mathbf{c}$, and that row is all zeroes in $\mathbf{A}$. Moreover, we know that the matrix $\mathbf{P} = \frac{1}{4}\begin{pmatrix} 6 & -1 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ -2 & -3 & 4 & 0 \\ -4 & -2 & 0 & 4 \end{pmatrix}$ will reduce the matrix $\mathbf{A}$. In the next section we will see how to find all solutions to $\mathbf{Ax} = \mathbf{b}$.

We finish this section with another example of a reduction of a matrix.

Example 10. Reducing by Hand. When reducing a matrix without a sophisticated machine, one needs to keep track of the step being performed as one moves across the row. Thus it is recommended to develop some notation that will remind one of the operation being performed. One possible set of symbols is now exemplified in the reduction of the matrix $\begin{pmatrix} 2 & -2 & 2 & 10 & 2 & 4 \\ 7 & -7 & 4 & 26 & 11 & 12 \\ 9 & -9 & 6 & 36 & 13 & 16 \\ 3 & -3 & 2 & 12 & 4 & 5 \end{pmatrix}$.

$$-1\begin{pmatrix} 2 & -2 & 2 & 10 & 2 & 4 \\ 7 & -7 & 4 & 26 & 11 & 12 \\ 9 & -9 & 6 & 36 & 13 & 16 \\ 3 & -3 & 2 & 12 & 4 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & -2 & 2 & 10 & 2 & 4 \\ 7 & -7 & 4 & 26 & 11 & 12 \\ 9 & -9 & 6 & 36 & 13 & 16 \\ 1 & -1 & 0 & 2 & 2 & 1 \end{pmatrix} \rightarrow -7\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 7 & -7 & 4 & 26 & 11 & 12 \\ 9 & -9 & 6 & 36 & 13 & 16 \\ 2 & -2 & 2 & 10 & 2 & 4 \end{pmatrix}$$

$$-9\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 4 & 12 & -3 & 5 \\ 9 & -9 & 6 & 36 & 13 & 16 \\ 2 & -2 & 2 & 10 & 2 & 4 \end{pmatrix} \rightarrow -2\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 4 & 12 & -3 & 5 \\ 0 & 0 & 6 & 18 & -5 & 7 \\ 2 & -2 & 2 & 10 & 2 & 4 \end{pmatrix} \rightarrow \begin{array}{c} \\ \\ \\ \tfrac{1}{2}\Rightarrow \end{array}\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 4 & 12 & -3 & 5 \\ 0 & 0 & 6 & 18 & -5 & 7 \\ 0 & 0 & 2 & 6 & -2 & 2 \end{pmatrix}$$

$$-4\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 4 & 12 & -3 & 5 \\ 0 & 0 & 6 & 18 & -5 & 7 \\ 0 & 0 & 1 & 3 & -1 & 1 \end{pmatrix} \rightarrow -6\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 6 & 18 & -5 & 7 \\ 0 & 0 & 1 & 3 & -1 & 1 \end{pmatrix} \rightarrow -1\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 & -1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 3 & -1 & 1 \end{pmatrix} \rightarrow 1\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 3 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow -2\begin{pmatrix} 1 & -1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and we arrive at the reduced form of the matrix $\begin{pmatrix} 1 & -1 & 0 & 2 & 0 & -1 \\ 0 & 0 & 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

❼ Rank & Systems

The number of pivots in the row reduced echelon form of **A**, or equivalently, the number of nonzero rows of the reduced matrix, is a very important invariant of **A** and is called the **rank** of **A**, which we will abbreviate by $r(\mathbf{A})$.

Clearly, by definition if **A** is $m \times n$, then $r(\mathbf{A}) \leq m$ and $r(\mathbf{A}) \leq n$ since any row can only have at most one pivot, and the same applies to any column. A matrix is said to be of **full rank** if its rank is as large as possible. Sometimes when clarification is needed one can describe a matrix as being of **full row rank**, or of **full column rank** as the occasion calls for. Thus a 5×6 is of full rank if its rank is 5 (as large as possible). Naturally, the reason why row equivalence play a role in the study of linear equations is the elementary fact that the solutions of $\mathbf{Ax} = \mathbf{b}$ are exactly the same as the solutions to $\mathbf{PAx} = \mathbf{Pb}$ if **P** is any invertible matrix as proven above.

The following is basically a corollary to the uniqueness of the reduced form.

> **Theorem (Invertible Matrices).** Let **A** be a square matrix. Then the following are equivalent:
> ❶ **A** is invertible;
> ❷ **A** has full rank;
> ❸ **A** reduces to **I**.

Proof. Assume **A** is invertible. Then we argue when **A** is reduced there cannot be any zero rows. For suppose there were, if we let **P** denote the reducing matrix, then **PA** would also be invertible and would have a row of zeroes. But that is impossible since a row zeroes will always produce a row of zeroes in any product, so one could never multiply to **I**. But without a row of zeroes, every row is pivotal, so the rank is full. If ❷ holds, then we must have a pivot in every row, and since the matrix is square, we must have a pivot in every column, and so the reduced form is **I**. Finally if ❸ holds, then $\mathbf{PA} = \mathbf{I}$ for the reducing matrix **P**, so **A** is invertible. ⌘

This allows us to just define two matrices **A** and **B** to be **row equivalent** if there exists an invertible matrix **P** such that $\mathbf{PA} = \mathbf{B}$, since every invertible matrix can be obtained by a sequence of row operations by the corollary. Of course, we could have also said that **two matrices are row equivalent if and only if they have the same reduced form**.

The previous theorem also permits us to produce an algorithm based on reduction for computing the inverse of any invertible matrix.

> **Corollary (Gauss-Jordan).** Let **A** be an invertible matrix. Then when we reduce the matrix $(\mathbf{A} \quad \mathbf{I})$ we will obtain $(\mathbf{I} \quad \mathbf{A}^{-1})$.

Proof. We know from above that $\mathbf{A}$ will reduce to the identity, and so when we multiply, we get the result. ⌘

Example 1. Take the matrix $\mathbf{A}=\begin{pmatrix}1&2&3&5&0\\2&2&1&2&1\\3&1&10&14&-2\\4&2&1&1&0\\5&3&1&1&0\end{pmatrix}$. The sequence of pivotings is:

$$\begin{pmatrix}\mathbf{1}&2&3&5&0&1&0&0&0&0\\2&2&1&2&1&0&1&0&0&0\\3&1&10&14&-2&0&0&1&0&0\\4&2&1&1&0&0&0&0&1&0\\5&3&1&1&0&0&0&0&0&1\end{pmatrix}\qquad\begin{pmatrix}1&2&3&5&0&1&0&0&0&0\\0&-\mathbf{2}&-5&-8&1&-2&1&0&0&0\\0&-5&1&-1&-2&-3&0&1&0&0\\0&-6&-11&-19&0&-4&0&0&1&0\\0&-7&-14&-24&0&-5&0&0&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&-2&-3&1&-1&1&0&0&0\\0&1&\frac{5}{2}&4&-\frac{1}{2}&1&-\frac{1}{2}&0&0&0\\0&0&\mathbf{\frac{27}{2}}&19&-\frac{9}{2}&2&-\frac{5}{2}&1&0&0\\0&0&4&5&-3&2&-3&0&1&0\\0&0&\frac{7}{2}&4&-\frac{7}{2}&2&-\frac{7}{2}&0&0&1\end{pmatrix}\qquad\begin{pmatrix}1&0&0&\frac{-5}{27}&\frac{1}{3}&\frac{-19}{27}&\frac{17}{27}&\frac{4}{27}&0&0\\0&1&0&\frac{13}{27}&\frac{1}{3}&\frac{17}{27}&\frac{-1}{27}&\frac{-5}{27}&0&0\\0&0&1&\frac{38}{27}&\frac{-1}{3}&\frac{4}{27}&\frac{-5}{27}&\frac{2}{27}&0&0\\0&0&0&\mathbf{\frac{-17}{27}}&\frac{-5}{3}&\frac{38}{27}&\frac{-61}{27}&\frac{-8}{27}&1&0\\0&0&0&\frac{-25}{27}&\frac{-7}{3}&\frac{40}{27}&\frac{-77}{27}&\frac{-7}{27}&0&1\end{pmatrix}$$

$$\begin{pmatrix}1&0&0&0&\frac{14}{17}&\frac{-19}{17}&\frac{22}{17}&\frac{4}{17}&\frac{-5}{17}&0\\0&1&0&0&\frac{-16}{17}&\frac{29}{17}&\frac{-30}{17}&\frac{-7}{17}&\frac{13}{17}&0\\0&0&1&0&\frac{-69}{17}&\frac{56}{17}&\frac{-89}{17}&\frac{-10}{17}&\frac{38}{17}&0\\0&0&0&1&\frac{45}{17}&\frac{-38}{17}&\frac{61}{17}&\frac{8}{17}&\frac{-27}{17}&0\\0&0&0&0&\mathbf{\frac{2}{17}}&\frac{-10}{17}&\frac{8}{17}&\frac{3}{17}&\frac{-25}{17}&1\end{pmatrix}\qquad\begin{pmatrix}1&0&0&0&0&3&-2&-1&10&-7\\0&1&0&0&0&-3&2&1&11&8\\0&0&1&0&0&17&11&\frac{11}{2}&\frac{-97}{2}&\frac{69}{2}\\0&0&0&1&0&11&-7&\frac{-7}{2}&\frac{63}{2}&\frac{-45}{2}\\0&0&0&0&1&-5&4&\frac{3}{2}&\frac{-25}{2}&\frac{17}{2}\end{pmatrix}$$

So

$$\mathbf{A}^{-1}=\begin{pmatrix}3&-2&-1&10&-7\\-3&2&1&11&8\\17&11&\frac{11}{2}&\frac{-97}{2}&\frac{69}{2}\\11&-7&\frac{-7}{2}&\frac{63}{2}&\frac{-45}{2}\\-5&4&\frac{3}{2}&\frac{-25}{2}&\frac{17}{2}\end{pmatrix}$$

Since the reduced form of the matrix $\begin{pmatrix}\mathbf{A} & \mathbf{B}\end{pmatrix}$ starts with the reduced form of $\mathbf{A}$, it is clear that every position occupied by a pivot in $\mathbf{A}$ will be occupied by a pivot of $\begin{pmatrix}\mathbf{A} & \mathbf{B}\end{pmatrix}$, and thus trivially we have that

$$r\begin{pmatrix}\mathbf{A} & \mathbf{B}\end{pmatrix}\geq r(\mathbf{A})$$

for any matrices $\mathbf{A}$ and $\mathbf{B}$ (that can be horizontally stacked).

And we have an easy, but important consequence of the concept of rank:

Theorem (Rank & Equations). Let $\mathbf{u}_1$, $\mathbf{u}_2,\ldots,\mathbf{u}_n$ and $\mathbf{b}$ be vectors of size m. Let $\mathbf{A}=\begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n\end{pmatrix}$ be the $m\times n$ matrix whose columns are the $\mathbf{u}$'s. Then the following are equivalent:

❶ The system $\mathbf{Ax}=\mathbf{b}$ has a solution.

❷ The vector $\mathbf{b}$ is a linear combination of $\mathbf{u}_1$, $\mathbf{u}_2,\ldots,\mathbf{u}_n$.

❸ $r(\mathbf{A})=r\begin{pmatrix}\mathbf{A} & \mathbf{b}\end{pmatrix}$.

Proof. The equivalence of ❶ and ❷ was observed long ago in the section on matrix multiplication, but it is worth repeating. If ❶ holds, and $\mathbf{x}=\begin{pmatrix}a_1\\ a_2\\ \vdots\\ a_n\end{pmatrix}$, then $\mathbf{b}=a_1\mathbf{u}_1+a_2\mathbf{u}_2+\cdots+a_n\mathbf{u}_n$, and vice versa, from the linear combination, we obtain a solution. So ❶ $\Leftrightarrow$ ❷. Now since $r(\mathbf{A})\le r\begin{pmatrix}\mathbf{A} & \mathbf{b}\end{pmatrix}$, the only way they may not be equal is for a pivot to appear in the last column of $\begin{pmatrix}\mathbf{A} & \mathbf{b}\end{pmatrix}$, but again the only way that can happen if to have a row of zeroes on the matrix of coefficients side, but a 1 in the last column, which is equivalent to $\mathbf{Ax}=\mathbf{b}$ not having a solution. ⌘

Example 2. Consider the system $\mathbf{Ax}=\mathbf{b}$ where $\mathbf{A}=\begin{pmatrix}1&1&0&-1\\2&6&4&2\\2&5&3&1\\2&4&2&0\end{pmatrix}$ and $\mathbf{b}=\begin{pmatrix}-1\\34\\25\\16\end{pmatrix}$. When we reduce $\begin{pmatrix}\mathbf{A} & \mathbf{b}\end{pmatrix}$ we get $\begin{pmatrix}1&0&-1&2&-10\\0&1&1&1&9\\0&0&0&0&0\\0&0&0&0&0\end{pmatrix}$, and we see that $r(\mathbf{A})=r\begin{pmatrix}\mathbf{A} & \mathbf{b}\end{pmatrix}=2$, and of course we have the solution $\begin{pmatrix}-10\\9\\0\\0\end{pmatrix}$, and in fact $-10\begin{pmatrix}1\\2\\2\\2\end{pmatrix}+9\begin{pmatrix}1\\6\\5\\4\end{pmatrix}=\begin{pmatrix}-1\\34\\25\\16\end{pmatrix}$.

Corollary (Full Row Rank & Equations). Let $\mathbf{A}$ be an $m\times n$ matrix. Then the following are equivalent:

❶ $\mathbf{A}$ has full row rank, $r(\mathbf{A})=m$.

❷ The system $\mathbf{Ax}=\mathbf{b}$ has at least one solution for any vector $\mathbf{b}$ of size m.

❸ Any vector $\mathbf{b}$ of size m can be written as a linear combination of the columns of $\mathbf{A}$.

❹ There exists a $n\times m$ matrix $\mathbf{X}$ such that $\mathbf{AX}=\mathbf{I}_m$.

Proof. By the previous theorem, since $r(\mathbf{A} \quad \mathbf{b}) \leq m$ for any $\mathbf{b}$, we have that ❶ implies ❷. Conversely, suppose that ❶ does not hold. So the reduced form of $\mathbf{A}$, $\mathbf{PA}$ has a row of zeroes. But then readily we can find a vector $\mathbf{c}$ that has a 1 in that row, so $\mathbf{PAx} = \mathbf{c}$ does not have a solution, and consequently neither does $\mathbf{Ax} = \mathbf{P}^{-1}\mathbf{c}$, and ❷ is then false. So ❶ ⇔ ❷. The equivalence of ❷ and ❸ is clear by matrix multiplication. Assume ❷. Then we can solve any system, so one can solve $\mathbf{Ax} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, the first column of the identity $\mathbf{I}_m$. Let $\mathbf{v}_1$ be a solution. Similarly, one can solve $\mathbf{Ax} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, the second column of the identity. Let $\mathbf{v}_2$ be a solution. Proceeding that way, we get vectors $\mathbf{v}_1$, $\mathbf{v}_2, \ldots, \mathbf{v}_m$, and if we let $\mathbf{X} = (\mathbf{v}_1 \quad \mathbf{v}_2 \quad \cdots \quad \mathbf{v}_m)$, then $\mathbf{AX} = \mathbf{I}_m$. Conversely, suppose $\mathbf{X}$ exists so that $\mathbf{AX} = \mathbf{I}$, but then to solve $\mathbf{Ax} = \mathbf{b}$, we know that $\mathbf{b} = \mathbf{Ib} = \mathbf{AXb}$, so $\mathbf{x} = \mathbf{Xb}$ is a solution.⌘

Note that in the square case, this is nothing but the Gauss-Jordan algorithm.

Example 3. Consider $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$. Its reduced form is $\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$, so $\mathbf{A}$ is of rank 2. And $\mathbf{X} = \frac{1}{3}\begin{pmatrix} -5 & 2 \\ 4 & -1 \\ 0 & 0 \end{pmatrix}$. Thus to solve $\mathbf{Ax} = \mathbf{b}$ with $\mathbf{b} = \begin{pmatrix} 7 \\ 1 \end{pmatrix}$, we simply take $\mathbf{Xb} = \begin{pmatrix} -11 \\ 9 \\ 0 \end{pmatrix}$.

Before we pursue the full column rank statement, we need a key observation about a reduced matrix, and the process of Gaussian Elimination.

> **Lemma (Nonpivotal Columns).** Let $\mathbf{u}_1$, $\mathbf{u}_2, \ldots, \mathbf{u}_n$ be vectors of size m and let $\mathbf{A} = (\mathbf{u}_1 \quad \mathbf{u}_2 \quad \cdots \quad \mathbf{u}_n)$ be the $m \times n$ matrix whose columns are the $\mathbf{u}$'s. Then every nonpivotal column of $\mathbf{A}$ can be written uniquely as a linear combination of the pivotal columns.

Proof. Let $\mathbf{M}$ be the reduced form of $\mathbf{A}$, $\mathbf{M} = (\mathbf{v}_1 \quad \mathbf{v}_2 \quad \cdots \quad \mathbf{v}_n)$. Then it is obvious that the theorem holds for any reduced matrix since the pivotal are columns of the identity matrix. We just need an extra observation. Any way one can write a $\mathbf{u}$ as a linear combination of the other $\mathbf{u}$'s is tantamount to writing the corresponding $\mathbf{v}$ as the same linear combination of the other $\mathbf{v}$'s. For example, suppose $\mathbf{u}_n = a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_{n-1}\mathbf{u}_{n-1}$. This means

$\mathbf{A}\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ -1 \end{pmatrix} = \mathbf{0}$, but $\mathbf{Ax} = \mathbf{0}$ and $\mathbf{Mx} = \mathbf{0}$ have the same solutions (since $\mathbf{M} = \mathbf{PA}$ for some invertible matrix $\mathbf{P}$). And the reverse argument is also clear. ⌘

Example 4. Let $\mathbf{u}_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \\ 2 \end{pmatrix}$, $\mathbf{u}_2 = \begin{pmatrix} 1 \\ 6 \\ 5 \\ 4 \end{pmatrix}$, $\mathbf{u}_3 = \begin{pmatrix} 0 \\ 4 \\ 3 \\ 2 \end{pmatrix}$, and $\mathbf{u}_4 = \begin{pmatrix} -1 \\ 2 \\ 1 \\ 0 \end{pmatrix}$, and $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 2 & 6 & 4 & 2 \\ 2 & 5 & 3 & 1 \\ 2 & 4 & 2 & 0 \end{pmatrix}$. The reduced form of $\mathbf{A}$ is $\mathbf{M} = \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. It is clear that any nonpivotal column in $\mathbf{M}$ can be written as a linear combination of the pivotal columns preceding it. And the relationship between the columns is preserved in the reduced form: $\mathbf{u}_3 = -\mathbf{u}_1 + \mathbf{u}_2$ and $\mathbf{u}_4 = -2\mathbf{u}_1 + \mathbf{u}_2$. But note that the reduction has a definite prejudice on which columns will be chosen as pivotal, since it always prefers the leading ones if at all possible.

Corollary (Full Column Rank & Equations). Let $\mathbf{A}$ be an $m \times n$ matrix. Then the following are equivalent:

❶ $\mathbf{A}$ has full column rank, $r(\mathbf{A}) = n$.

❷ The system $\mathbf{Ax} = \mathbf{b}$ has at most one solution for any vector $\mathbf{b}$ of size m.

❸ Any vector $\mathbf{b}$ of size m can be written in at most one way as a linear combination of the columns of $\mathbf{A}$.

❹ There exists a $n \times m$ matrix $\mathbf{X}$ such that $\mathbf{XA} = \mathbf{I}_m$.

Proof. Start by assuming ❶. Since $\mathbf{A}$ is of full column rank, the reduced form of the augmented matrix $(\mathbf{A} \quad \mathbf{b})$ has to be of the form $\begin{pmatrix} \mathbf{I} & \mathbf{c} \\ \mathbf{0} & \mathbf{d} \end{pmatrix}$ (where the $\mathbf{0}$-block and the $\mathbf{d}$ may be nonexistent). If $\mathbf{d}$ has an entry that is not zero, then we know that the system has no solution, but otherwise we know the unique solution is $\mathbf{x} = \mathbf{c}$, and we have ❷. That ❷ and ❸ are equivalent follows easily by matrix multiplication since every solution to $\mathbf{Ax} = \mathbf{b}$ is a is a way of writing $\mathbf{b}$ as linear combination of the columns of $\mathbf{A}$. Assume now that ❶ is not true. But then by the lemma, we can write a nonpivotal column as a linear combination of the pivotal ones, but that same nonpivotal column can simply be written as a linear combination of itself alone (with all other coefficients equal to 0), and so there is more than one way to write a vector as a linear combination of the columns of $\mathbf{A}$. Thus ❸ is not true. Now assume ❹ holds and let $\mathbf{u}$ be a solution to $\mathbf{Ax} = \mathbf{b}$, so $\mathbf{Au} = \mathbf{b}$. Then multiplying by $\mathbf{X}$, we get $\mathbf{u} = \mathbf{Xb}$, so $\mathbf{u}$ is uniquely determined. Thus all we have left to do is to prove $\mathbf{X}$ exists if we assume ❶. We know the reduced form of $\mathbf{A}$ is of the form $\begin{pmatrix} \mathbf{I} \\ \mathbf{0} \end{pmatrix}$ any of the first three statements. Let $\mathbf{P}$ be the reducing matrix, so P is $m \times m$ where necessarily $m \geq n$. Let $\mathbf{P} = \begin{pmatrix} \mathbf{Q} \\ \mathbf{R} \end{pmatrix}$ where $\mathbf{Q}$ consists of its first n rows. Then $\mathbf{QA} = \mathbf{I}_n$, and we have ❹. ⌘

Example 5. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \\ 13 & 14 & 18 \end{pmatrix}$. Then $\mathbf{A}$ is indeed of rank 3 with reducing matrix $\mathbf{P} = \frac{1}{3}\begin{pmatrix} -2 & -2 & 0 & 0 & 1 \\ -2 & 7 & 0 & 0 & -2 \\ 3 & -4 & 0 & 0 & 1 \\ 3 & -6 & 3 & 0 & 0 \\ 6 & -9 & 0 & 3 & 0 \end{pmatrix}$. So $\mathbf{X} = \frac{1}{3}\begin{pmatrix} -2 & -2 & 0 & 0 & 1 \\ -2 & 7 & 0 & 0 & -2 \\ 3 & -4 & 0 & 0 & 1 \end{pmatrix}$, satisfies $\mathbf{XA} = \mathbf{I}_3$. Thus to solve $\mathbf{Ax} = \mathbf{b}$ where $\mathbf{b} = \begin{pmatrix} 14 \\ 32 \\ 50 \\ 68 \\ 95 \end{pmatrix}$, all we would need to do is compute $\mathbf{u} = \mathbf{Xb} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$. However, that would only be correct if we knew we had a solution to start with—if instead we had taken $\mathbf{b} = \begin{pmatrix} 14 \\ 32 \\ ? \\ ? \\ 95 \end{pmatrix}$, our answer would not change, but on the other hand $\mathbf{Au}$ would not be correct. We will pursue this in another section in a latter chapter.

The last corollary addresses only half of the issue—what happens to $\mathbf{Ax} = \mathbf{b}$ when $\mathbf{A}$ does not have full column rank? Of course, we may not have a solution since if $\mathbf{A}$ does not have full row rank, that will indubitably be the case for some $\mathbf{b}$'s. But suppose then that $\mathbf{A}$ does not have full column rank and at the same time that $\mathbf{Ax} = \mathbf{b}$ has a solution. Then we know by the previous lemma that each nonpivotal column can be written as a linear combination of the pivotal ones.

Since $\mathbf{Ax} = \mathbf{b}$ has a solution we know that $\mathbf{b}$ is a linear combination of the columns of $\mathbf{A}$, say $\mathbf{A} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$ and $\mathbf{b} = k_1\mathbf{u}_1 + k_2\mathbf{u}_2 + \cdots + k_n\mathbf{u}_n$. Without loss of generality, let us say that $\mathbf{u}_n$ is not pivotal. Then we claim that we can find a solution to $\mathbf{Ax}=\mathbf{b}$ where the value of the n^{th} unknown is arbitrary—in other words, we can write $\mathbf{b}$ as a linear combination of the columns of $\mathbf{A}$ where the coefficient of $\mathbf{u}_n$ is arbitrarily chosen. This is just a simple substitution, since $\mathbf{u}_n = a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_{n-1}\mathbf{u}_{n-1}$, we have that

$$a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_{n-1}\mathbf{u}_{n-1} - \mathbf{u}_n = \mathbf{0},$$

and so we can chose any *t*, and $ta_1\mathbf{u}_1 + ta_2\mathbf{u}_2 + \cdots + ta_{n-1}\mathbf{u}_{n-1} - t\mathbf{u}_n = \mathbf{0}$, so

$$\mathbf{b} = k_1\mathbf{u}_1 + k_2\mathbf{u}_2 + \cdots + k_n\mathbf{u}_n + ta_1\mathbf{u}_1 + ta_2\mathbf{u}_2 + \cdots + ta_{n-1}\mathbf{u}_{n-1} - t\mathbf{u}_n,$$

and

$$\mathbf{b} = (k_1 + ta_1)\mathbf{u}_1 + (k_2 + ta_2)\mathbf{u}_2 + \cdots + (k_n - t)\mathbf{u}_n,$$

and since t is arbitrary, so is $k_n - t$. This shows that the moment there is a nonpivotal column and a solution exists, then the system has infinitely many solutions, and we have finished proving:

Corollary (Choices). Let $\mathbf{A}$ be $m \times n$, and consider any system $\mathbf{Ax}=\mathbf{b}$. Then exactly one of the following can happen:

❶ It has no solution, which happens if and only $r(\mathbf{A} \quad \mathbf{b}) = r(\mathbf{A}) + 1$;

❷ It has exactly one solution, which happens if and only $r(\mathbf{A} \quad \mathbf{b}) = r(\mathbf{A}) = n$;

❸ It has infinitely many solutions, which happens if and only if $r(\mathbf{A} \quad \mathbf{b}) = r(\mathbf{A}) < n$.

We will pursue a more geometric understanding of the nature of all the solutions to a linear system in the next chapter. Presently we develop an algorithmic way to describe all solutions. Two of the proofs above used a special system, $\mathbf{Ax}=\mathbf{0}$. This is known as the **homogeneous system** (for the matrix of coefficients $\mathbf{A}$).

Corollary (Homogeneous Systems). Let $\mathbf{A}$ be $m \times n$ where $n > m$. Then the system $\mathbf{Ax}=\mathbf{0}$ has a nontrivial solution.

Proof. Since $r(\mathbf{A}) \le m < n$, we have a free variable, and so we have infinitely many solutions to $\mathbf{Ax}=\mathbf{0}$. ⌘

A more abstract way to describe what occurred in the last argument is as follows: let $\mathbf{u}$ be a solution to the system $\mathbf{Ax}=\mathbf{b}$, and let $\mathbf{w}$ be a solution to the homogeneous system $\mathbf{Ax}=\mathbf{0}$. Then $\mathbf{u}+\mathbf{w}$ is also a solution to $\mathbf{Ax}=\mathbf{b}$ since

$$\mathbf{A}(\mathbf{u}+\mathbf{w}) = \mathbf{Au} + \mathbf{Aw} = \mathbf{b} + \mathbf{0} = \mathbf{b},$$

and conversely, if $\mathbf{u}$ and $\mathbf{v}$ are solutions to $\mathbf{Ax}=\mathbf{b}$, then $\mathbf{w}=\mathbf{u}-\mathbf{v}$ is a solution to the homogeneous system since

$$\mathbf{Aw} = \mathbf{A}(\mathbf{u}-\mathbf{v}) = \mathbf{Au} - \mathbf{Av} = \mathbf{b} - \mathbf{b} = \mathbf{0}.$$

Thus, we have the following

Theorem (Linear Systems). Consider the system $\mathbf{Ax} = \mathbf{b}$. Suppose $\mathbf{u}$ is a particular solution to $\mathbf{Ax} = \mathbf{b}$. Then all solutions are of the form $\mathbf{u} + \mathbf{w}$ where $\mathbf{w}$ is a solution to the homogeneous system $\mathbf{Ax} = \mathbf{0}$.

Thus we have to start by understanding the homogeneous systems—but from our discussion above we saw that the nonpivotal variables can take any value, and that is the essence of all solutions to the homogeneous case.

Example 6. Let $\mathbf{A} = \begin{pmatrix} 1 & 3 & 2 & 4 & 1 \\ 2 & 6 & 1 & 5 & -4 \\ 3 & 9 & 3 & 9 & -3 \\ 4 & 12 & 4 & 12 & -4 \end{pmatrix}$. Then consider $\mathbf{Ax} = \mathbf{0}$. The reduced form of the augmented matrix is $\begin{pmatrix} 1 & 3 & 0 & 2 & -3 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. Note that the last column of the augmented matrix of a homogeneous system will never change since $\mathbf{P0} = \mathbf{0}$ for any matrix. So all our information has come down to two equations:

$$x_1 + 3x_2 + 2x_4 - 3x_5 = 0 \text{ and } x_3 + x_4 + 2x_5 = 0.$$

What are the solutions to these equations? Simply solve for each pivotal unknown in terms of the nonpivotals:

$$x_1 = -3x_2 - 2x_4 + 3x_5 \text{ and } x_3 = -x_4 - 2x_5.$$

Then clearly the vector

$$\mathbf{w} = \begin{pmatrix} -3x_2 - 2x_4 + 3x_5 \\ x_2 \\ -x_4 - 2x_5 \\ x_4 \\ x_5 \end{pmatrix}$$

will satisfy $\mathbf{Ax} = \mathbf{0}$ since it obviously satisfies the reduced system. But what are x_2, x_4 and x_5? First we should observe they are the nonpivotal unknowns (or columns). Second, we do not require them to be anything, they can be arbitrary, and they are known then as **free variables**. So all solutions to the homogeneous system are captured in the expression

$$\mathbf{w} = x_2 \begin{pmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} -2 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + x_5 \begin{pmatrix} 3 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix} = a \begin{pmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} -2 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + c \begin{pmatrix} 3 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix}$$

where a, b and c are arbitrary scalars. This expression is arrived at when we separate the previous vector into the x_2-vector, the x_4-vector and the x_5-vector.

But in fact in order to solve any system one does not need to solve for the homogeneous separately as the following example shows.

Example 7. Let $\mathbf{A}=\begin{pmatrix}1&3&2&4&1\\2&6&1&5&-4\\3&9&3&9&-3\\4&12&4&12&-4\end{pmatrix}$. Then consider the following systems $\mathbf{Ax}=\mathbf{b}$, $\mathbf{Ax}=\mathbf{c}$ and $\mathbf{Ax}=\mathbf{d}$ where $\mathbf{b}=\begin{pmatrix}-1\\1\\0\\0\end{pmatrix}$, $\mathbf{c}=\begin{pmatrix}4\\5\\9\\12\end{pmatrix}$ and $\mathbf{d}=\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$. As observed in the theorem, to find all solutions to each of those systems (if any), we will need the solutions to the homogeneous system. But reducing any system will always give us that since a column of 0's will remain so through the reduction as observed before. Thus, we will reduce the matrix $\begin{pmatrix}\mathbf{A} & \mathbf{b} & \mathbf{c} & \mathbf{d}\end{pmatrix}$. When we do so we get the matrix $\begin{pmatrix}1&3&0&2&-3&1&2&0\\0&0&1&1&2&-1&1&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&0\end{pmatrix}$, which immediately tell us that $\mathbf{Ax}=\mathbf{d}$ does not have a solution.

To solve $\mathbf{Ax}=\mathbf{b}$ we proceed as we did on the homogeneous system. All we have left are the two equations $x_1+3x_2+2x_4-3x_5=1$ and $x_3+x_4+2x_5=-1$. Proceed to solve for the pivotal unknowns in terms of the nonpivotal ones—note that this can always be done since each pivotal unknown occurs in exactly one equation (with all other unknowns being nonpivotal). When we do we get $x_1=1-3x_2-2x_4+3x_5$ and $x_3=-1-x_4-2x_5$. So clearly the vector

$$\mathbf{u}=\begin{pmatrix}1-3x_2-2x_4+3x_5\\x_2\\-1-x_4-2x_5\\x_4\\x_5\end{pmatrix}.$$

is a solution to the system regardless what values x_2, x_4 and x_5 take. Separating the vector as we did in the homogeneous case, we get that

$$\mathbf{u}=\begin{pmatrix}1\\0\\-1\\0\\0\end{pmatrix}+a\begin{pmatrix}-3\\1\\0\\0\\0\end{pmatrix}+b\begin{pmatrix}-2\\0\\-1\\1\\0\end{pmatrix}+c\begin{pmatrix}3\\0\\-2\\0\\1\end{pmatrix}$$

where a, b and c are arbitrary real numbers is an arbitrary solution to the system $\mathbf{Ax}=\mathbf{b}$.

Note that the solutions look like the particular solution $\begin{pmatrix}1\\0\\-1\\0\\0\end{pmatrix}$ added to an arbitrary homogeneous solution—and the particular solution was obtained by letting the free variables be 0.

Similarly, for $\mathbf{Ax}=\mathbf{c}$, we can read from the reduced form a specific solution, $\begin{pmatrix}2\\0\\1\\0\\0\end{pmatrix}$, and so we get all solutions $\begin{pmatrix}2\\0\\1\\0\\0\end{pmatrix}+a\begin{pmatrix}-3\\1\\0\\0\\0\end{pmatrix}+b\begin{pmatrix}-2\\0\\-1\\1\\0\end{pmatrix}+c\begin{pmatrix}3\\0\\-2\\0\\1\end{pmatrix}$. Note that since **c** is nothing but the fourth column of **A**, one solution is given trivially by $\begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}$, and indeed if we let $a=0$, $b=1$ and $c=0$ in the general expression we will get that specific solution. But even more importantly we could have written all solutions as being of the form

$$\begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}+a\begin{pmatrix}-3\\1\\0\\0\\0\end{pmatrix}+b\begin{pmatrix}-2\\0\\-1\\1\\0\end{pmatrix}+c\begin{pmatrix}3\\0\\-2\\0\\1\end{pmatrix}$$

since they both represent the same collection of vectors.

Appropriately we end this important section with another historical Chinese problem. The example is from the book, (Zhang Qiujian) **Mathematical Manual**, which dates from the sixth century.

> One rooster is worth five copper cash; one hen is worth three copper cash; three young chicks are worth one copper cash. Buying 100 fowls with 100 cash, how many roosters, hens and chicks?

If we let R stand for the number of roosters, H for the number of hens and C for the number of chickens, then the conditions of the problem easily translate to the following two equations:

$$R + H + C = 100$$
$$5R + 3H + \tfrac{1}{3}C = 100$$

Or in matrix notation this becomes $\begin{pmatrix} 1 & 1 & 1 & 100 \\ 5 & 3 & \frac{1}{3} & 100 \end{pmatrix}$, which reduces to $\begin{pmatrix} 1 & 0 & \frac{-4}{3} & -100 \\ 0 & 1 & \frac{7}{3} & 200 \end{pmatrix}$ so we have that $R = \frac{4}{3}C - 100$ and $H = 200 - \frac{7}{3}C$, so all solutions are given by

$$\begin{pmatrix} R \\ H \\ C \end{pmatrix} = \begin{pmatrix} -100 \\ 200 \\ 0 \end{pmatrix} + \frac{C}{3}\begin{pmatrix} 4 \\ -7 \\ 1 \end{pmatrix}.$$

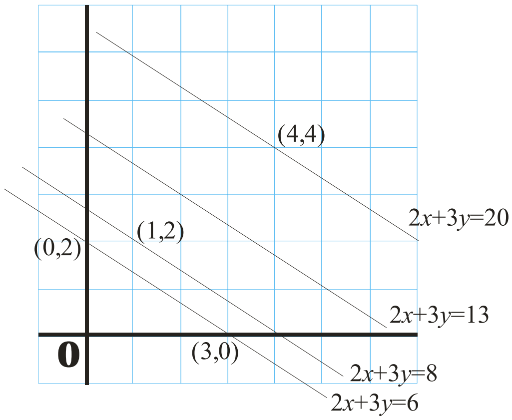
In order for the solutions to make sense (be integers), we need to have C to be a multiple of 3, and also since $R \geq 0$ and $H \geq 0$, we must have $C \geq 75$ and $C \leq 85$, so the only possibilities for C are 75, 78, 81 and 84. In fact, the solutions are

R	H	C
12	4	84
8	11	81
4	18	78
0	25	75

Although the method of solution was not included, the book gives the three positive solutions. Today we would probably list all 4, including the one with one of the unknowns taking the value 0.

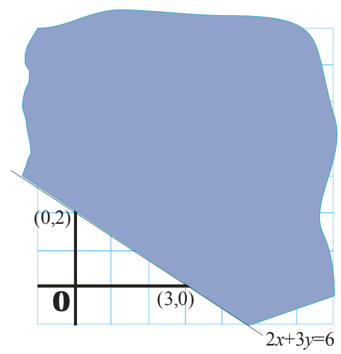
❽ Inequalities

So far, we have had an extensive discussion on linear equations. In this section we look briefly at inequalities, starting naturally in $\mathbb{R}^2$. What does the inequality $2x+3y \geq 6$ represent, in other words what points in the plane satisfy this inequality. Simply, we know that $2x+3y=6$ represents a line. In fact for any number c,



$$2x+3y=c$$

represents a line, and if we choose $c \geq 6$, then all the lines are on one side of the original line, so that the original inequality represents one half of the plane, as in the picture.



When we have more than one inequality, we see that we need to intersect all the half-planes as in the following example.

Example 1. (Mixing). To feed her stock a farmer can purchase two kinds of feed, ① and ②. The farmer has determined that her herd requires 60, 84 and 72 units of the nutritional elements **A**, **B**, and **C**, respectively, per day. The contents per pound of each of the two feeds are given in the following table:

Nutritional Elements (units/lb)

	A	**B**	**C**
Feed ①	3	7	3
Feed ②	2	2	6

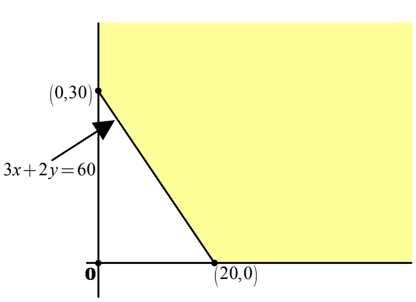
If we let x and y denote the amount (in pounds) of feed ① and ②, respectively, then the conditions of the problem translate into the following **constraints**:

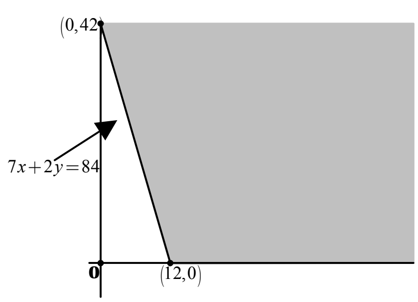
$$3x+2y \geq 60 \ (\mathbf{A}) \qquad 7x+2y \geq 84 \ (\mathbf{B}) \qquad 3x+6y \geq 72 \ (\mathbf{C})$$

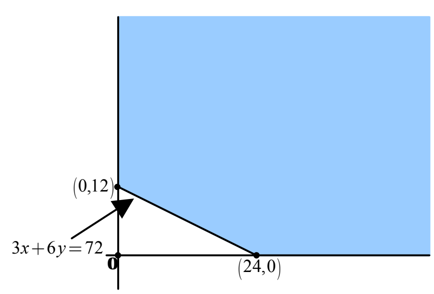
However, we have another set of constraints, which are implicit in the problem:

$$x \geq 0,\ y \geq 0.$$

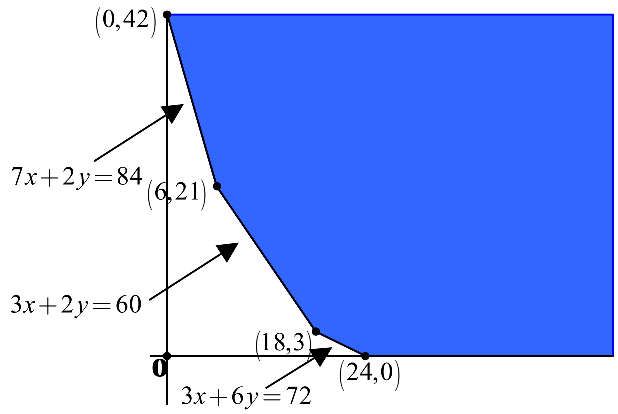
If we were to graph all possible solutions to this system of inequalities, we would see that there are infinitely many solutions to it. In fact, if we graph the region for each of the inequalities, we obtain three unbounded regions:





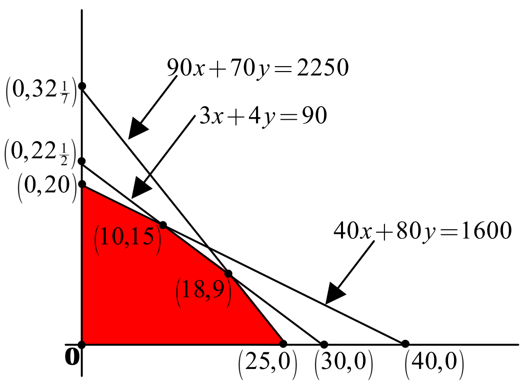


and when we look at the intersection of the three regions we get a region of infinitely many points and with four corners: $(0,42)$, $(6,21)$, $(18,3)$ and $(24,0)$.



A very different region occurs in the following

Example 2. (Building). A building contractor builds two types of houses, 3-bedroom and 4-bedroom. A 3-bedroom home requires 3 units of glass, 40 units of wood and 90 units of block. A 4-bedrooom home requires 4 units of glass, 80 units of wood and 70 units of block. The contractor has available to him a total of 90 units of glass, 1600 units of wood and 2250 units of block. What productions are possible?



If we let x and y denote the number of houses with 3 bedrooms and 4 bedrooms respectively, then the conditions of the problem translate into:

$$3x+4y \le 90 \text{ (glass)}$$
$$40x+80y \le 1600 \text{ (wood)}$$
$$90x+70y \le 2250 \text{ (block)}$$

Of course, we again have $x \ge 0$, $y \ge 0$.

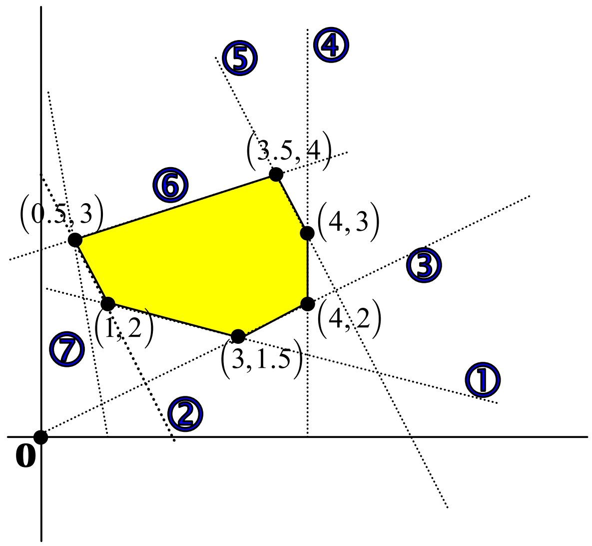
Here the feasibility region is very bounded with five corners: $(0,0)$, $(25,0)$, $(18,9)$, $(10,15)$ and $(0,20)$. But observe we needed the visual to aid in deciding that the intersection of the two lines $40x+80y \le 1600$ and $90x+70y \le 2250$ lies outside our region. An alternative would have been to find the point of intersection $\left(15\tfrac{5}{11},12\tfrac{3}{11}\right)$ and observe it does not satisfy the third inequality, $45\tfrac{15}{11}+48\tfrac{9}{11}>90$.

One more simple example

Example 3. Consider the following set of 7 inequalities:

①	$x+4y \ge 9$	②	$2x+y \ge 4$
③	$x-2y \le 0$	④	$x \le 4$
⑤	$2x+y \le 11$	⑥	$6y-2x \le 17$

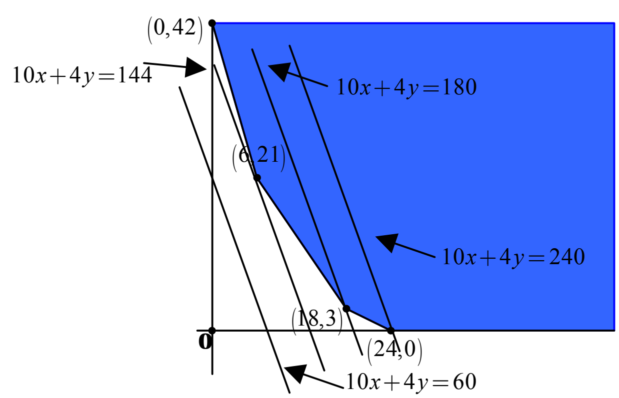
⑦ $6x+y \ge 6$.



The graph is as given with consecutive corners: $(1,2)$, $(3,1.5)$, $(4,2)$, $(4,3)$, $(3.5,4)$ and $(0.5,3)$. It is worth observing that the picture has the corner $(0.5,3)$ in which the three lines, ②, ⑥ and ⑦ meet.

Of course, what happens in 3-space is very similar to what occurred in the plane. If we are given a linear inequality such as $2x+3y+4z\geq 9$, then the set of points that satisfy this inequality is a **half-space**, all the points on the appropriate side of the plane given by the equation $2x+3y+4z=9$. And similarly, in higher dimensions, each linear inequality represents a half-space as delineated by the hyperplane given by the equation.

There is an interesting problem associated with inequalities, one of optimizing (either minimizing or maximizing) a linear function, and there are two charming theorems associated with this problem—one is very easy to see graphically, while the other is rather deep, and much harder to prove.



We will revisit the three examples above. To start with suppose that in **Example 1**, each unit of feed ① costs 10¢ while each unit of feed ② costs 4¢. Then we would be interested in minimizing the cost function, **C**, which is given by:

$$\mathbf{C}=10x+4y.$$

Of course, for any specific value of **C** that we choose, the graph of $\mathbf{C}=10x+4y$ is a line, but since we want our constraints satisfied we need a line that intersects the region, but that gives as low a value of **C** as possible. Of course, all the lines we get by giving different value to **C**, are parallel, and as the picture indicates, we will obtain a **minimum** at the corner $(6,21)$. In fact, if we compute the cost at each of the four corners, we get:

x	y	**C**
0	42	168
6	21	144
18	3	192
24	0	240

And the minimum cost would be achieved with 6 pounds of feed ① and 21 pounds of feed ②.

This simple example illustrates one of the two theorems mentioned above:

that a minimum or a maximum—if it exists—will occur at one of the corners of the region.

Certainly, if we had asked for the maximum cost, there is no point that will give us that.

The second theorem, more subtle and harder to prove is that :

next to each corner, there is a corner that is smaller unless one is at the minimum already.

In other words,

if you are better than your neighbors, you are better than anybody else.

Note a crucial omission on the statement of the first theorem, the word **ONLY**. The minimum can occur at other points as well—for example if the cost had rather been given by $\mathbf{C} = 6x + 4y$, then the minimum value of $\mathbf{C} = 120$ not only would have occurred at the same corner $(6,21)$, but also at the corner $(18,3)$ as well as any point in between such as $(12,12)$.

We illustrate these two theorems in the other two examples.

Suppose that in **Example 2**, the profit in a 3-bedroom house is \$40,000 while the profit in a 4-bedroom is \$60,000. Then the profits at the corners (in thousands of dollars) are given by the table on the right, and we see the second theorem illustrated again—next to the maximum corner $(10,15)$, there are corners that are less profitable.

x	y	**P**
0	0	0
0	20	1,200
10	**15**	**1,300**
18	9	1,260
25	0	1,000

Of course, any nonnegative function would have a minimum at the corner $(0,0)$.

Finally, in **Example 3**, no matter what function $\mathbf{F} = ax + by$ we pick, the minimum and maximum will exist at one of the corners. And by choosing different values for *a* and *b*, one can make different corners be the optimal points, as the following two simple examples illustrate:

$a = -4$		$b = 10$	
x	y	**F**	
0.5	3	28	max
1	2	16	
3	1.5	3	min
4	2	4	
4	3	14	
3.5	4	26	

$a = 2$		$b = 6$	
x	y	**F**	
0.5	3	19	
1	2	14	min
3	1.5	15	
4	2	20	
4	3	26	
3.5	4	31	max

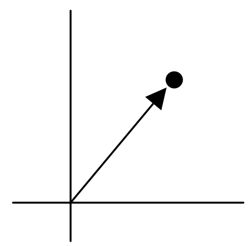
Naturally, to extend the understanding to higher dimensions, the notion of **corner** had to be carefully defined, and the notion of **neighboring corners** be suitably extended. This belongs to a higher course than this one, but it does involve pivoting.

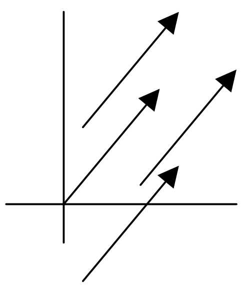
❾ The Geometry of Vectors

As often happens in mathematics, the power of analytic and algebraic tools is only enhanced via the visualization of geometric thought, and that is exactly what we pursue in this section. Thus we concentrate on vectors of size 2 and 3 in order to gain understanding that then will be extended to arbitrary vectors.

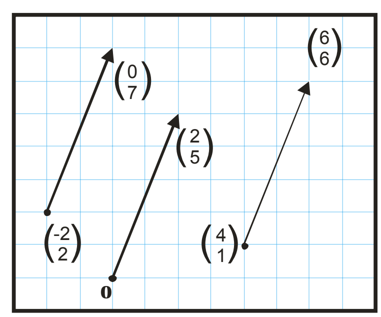
Some notation: $\mathbb{R}^2$ denotes the set of vectors of size 2, $\mathbb{R}^3$ the collection of vectors of size 3, $\mathbb{R}^4$ those of size 4, etcetera. Abstractly, $\mathbb{R}^n$ will denote those vectors of size n.

Naturally, we start with the well-known plane that we inherited from **Descartes** and **Fermat**, but we see it not from a 17th century point of view, but from a 19th century perspective. In contrast to Cartesian (or complex number) notation, we will now use vectors (of size 2) of real numbers to denote points in the plane, thus $\begin{pmatrix}0\\0\end{pmatrix}$ denotes the origin, $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$ the unit points of the axes, respectively. Not much has changed from the Cartesian perspective, but we are really discussing the vector plane. We view points not only statically, but also dynamically, as an arrow starting at the origin and ending at the point. But more generally, a vector, which has both direction and magnitude, is not necessarily anchored at the origin, and we think of it as the same vector no matter where it starts as long as its direction is the same and its length (or magnitude) is the same. In other words, one often thinks of a vector as **a change from one point to another**, and two changes are the same if their direction and magnitude are the same.

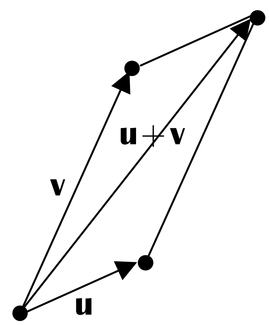




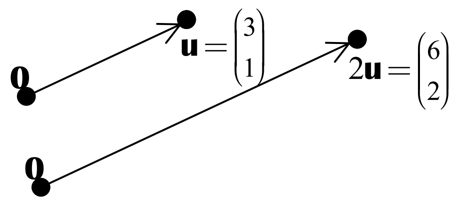
Example 1. $\begin{pmatrix}2\\5\end{pmatrix}$ is the vector from the origin to that point, but it is also the vector from $\begin{pmatrix}4\\1\end{pmatrix}$ to $\begin{pmatrix}6\\6\end{pmatrix}$, since $\begin{pmatrix}6\\6\end{pmatrix}-\begin{pmatrix}4\\1\end{pmatrix}=\begin{pmatrix}2\\5\end{pmatrix}$ and similarly $\begin{pmatrix}2\\5\end{pmatrix}$ is the vector from $\begin{pmatrix}-2\\2\end{pmatrix}$ to $\begin{pmatrix}0\\7\end{pmatrix}$ for the same reasons.



In a more formal way, a vector is really a pair of points, the starting point and the end point, and two pairs are considered equal if there is a translation taking the one pair to the other. We will refrain from using this formal approach. For us **vectors will be anchored at the origin. If we were to encounter $\begin{pmatrix}2\\5\end{pmatrix}$, do we think of it as the simple static point, or do we think of it as a vector? It is important that at all times we keep in mind both possibilities, and decide which fits the situation best.**

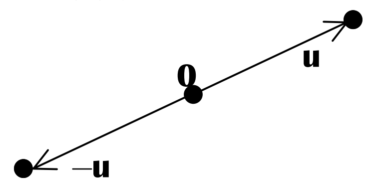


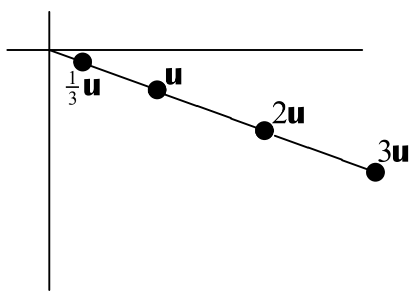
Of course, vector (or matrix) addition is well suited for geometry. It represents the parallelogram law: $\begin{pmatrix}3\\1\end{pmatrix}+\begin{pmatrix}1\\5\end{pmatrix}=\begin{pmatrix}4\\6\end{pmatrix}$.



Scalar multiplication is also very well suited for geometry. It amounts to a vector in the same direction but whose magnitude has been multiplied by the scalar factor.

Of course, a negative scalar reverses the direction since $\mathbf{u}+(-\mathbf{u})=\mathbf{0}$.





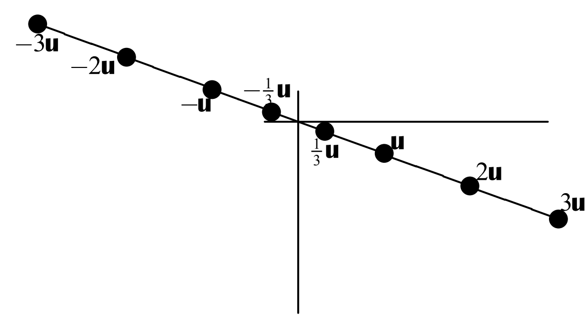
This simple idea of scalar multiplication leads to one of the important concepts in geometry, that of a line. If $\mathbf{u}$ is a nonzero vector, then, **the ray of** $\mathbf{u}=\{t\mathbf{u} \mid t\geq 0\}$. That our definition agrees with our intuition is easily seen from the picture.

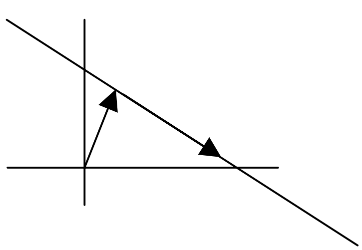
Note that the points between the origin and $\mathbf{u}$ have t's that are between 0 and 1, while those passed $\mathbf{u}$ have $t>1$.

Also, by considering **all real** values of t, $[\mathbf{u}]=\{t\mathbf{u} \mid t\in\mathbb{R}\}$, in other words, by taking all multiples of $\mathbf{u}$, we obtain

the line in the direction of $\mathbf{u}$,

or the line that goes through $\mathbf{u}$ and the origin. Note that from this point of view you can think of $\mathbf{u}$ as both a point and a vector because both the point $\mathbf{u}$ is on the line, and the vector $\mathbf{u}$ lies on the line—both are true.



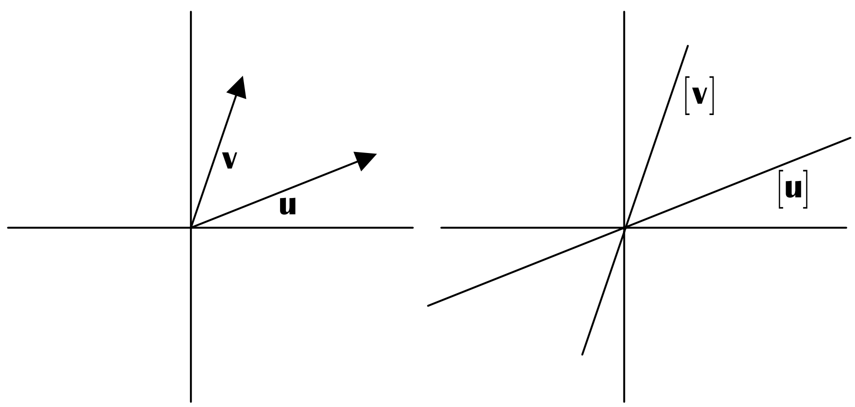


In this course we will be mostly interested in collections of vectors with the origin among them, so our lines will be mostly of the type we have just described, **the multiples of a vector.** But we should observe that for a line not going through the origin, **the points that are on it are never the vectors that lie on it**—and often in other courses, where all kinds of lines are considered, that can lead to confusion. Observe that we have used $[\mathbf{u}]$ to denote the set of multiples of $\mathbf{u}$.

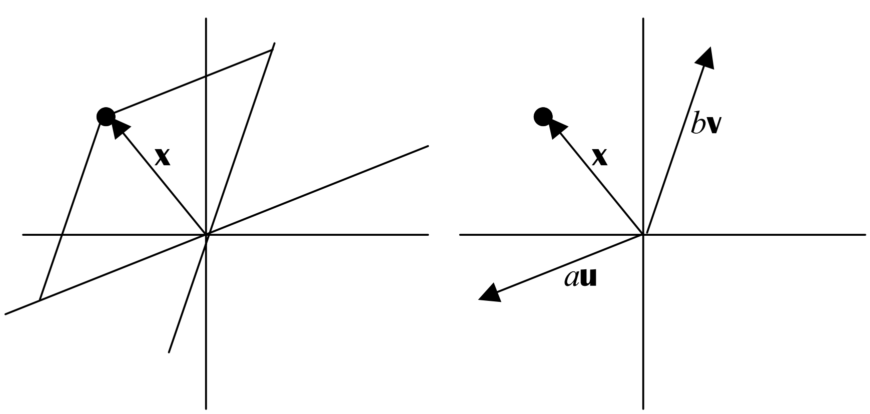
One of the great advantages of the vector approach to geometry is the uniformity of description of a line in space of any size: $\mathbb{R}^2$, $\mathbb{R}^3$, $\mathbb{R}^4$, etcetera. Namely, if we extend our thinking to vectors of size 3, we realize that the collection of all multiples of a vector form a line, but now, in space, and so by further extension, when we move to vectors of size 4, namely to $\mathbb{R}^4$, we then think of a line through the origin as all multiples of a nonzero vector.

And so in $\mathbb{R}^n$, **a line through the origin is the set of all multiples of a nonzero vector**. And thus **a line is always a one-dimensional object since it is generated by a single vector**.

Returning to $\mathbb{R}^2$, suppose we are given two nonzero vectors, $\mathbf{u}$ and $\mathbf{v}$. It could be that one of them is a multiple of the other, if that is the case they lie on the same line, they are parallel, then the set of **linear combinations** of the two of them $[\mathbf{u},\mathbf{v}] = \{a\mathbf{u} + b\mathbf{v} \mid a, b \in \mathbb{R}\}$ is nothing but the set of multiples of either, $[\mathbf{u},\mathbf{v}] = [\mathbf{u}] = [\mathbf{v}]$. But suppose the more interesting case occurs, when neither is a multiple of the other. Then we know that the set of all multiples of $\mathbf{u}$, $[\mathbf{u}] = \{a\mathbf{u}\}$ is the set of all points on the line through the point $\mathbf{u}$ and the origin, or equivalently, the line in the direction of $\mathbf{u}$. Similarly for $\mathbf{v}$, and so we are adding any vector in the one line to any vector in the other line, and as the picture illustrates, we are really filling in the plane.



The argument is as follows: let $\mathbf{x}$ be an arbitrary vector (point), and draw the two perpendiculars to the two respective lines through the new point, and draw them until they intersect the other line, then the two vectors obtained in this fashion are indeed multiples of $\mathbf{u}$ and $\mathbf{v}$, and they satisfy



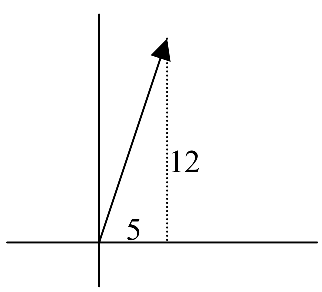
$$\mathbf{x} = a\mathbf{u} + b\mathbf{v}.$$

Thus, we realize the important fact that the collection of linear combinations of any two vectors in the plane either constitute a line (if the vectors happen to be multiples of each other), or they fill in the plane. But the geometric picture we have just seen extends easily to vectors in space, vectors of size 3, and so we have a way of again extending our intuition:

> let $\mathbf{u}$ and $\mathbf{v}$ be nonzero vectors in $\mathbb{R}^n$. Then the set of linear combinations of the two of them, also known as their **span**, $[\mathbf{u},\mathbf{v}]=\{a\mathbf{u}+b\mathbf{v}\mid a,b\in\mathbb{R}\}$ is either a line (if the vectors happen to be multiples of each other), or it is a plane (through the origin).

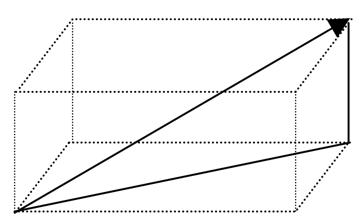
Again, one of the advantages of approaching the geometry of the plane from the vector point of view is that the notions discussed there readily extend to 3-space, and indeed they extend to vectors of any size. One of the key observations toward acceptance of these remarks is the fact that any time two points are given in 3-space (or higher), then there is a plane in 3-space containing those two points as well as the origin, and therefore we are reduced to considerations in the plane.

Enough has been said about lines and planes for the time being. Let us turn to other important notions from geometry: **lengths**, **areas** and **angles**.



What is the length of the vector $\begin{pmatrix}5\\12\end{pmatrix}$? Of course, with the aid of the great ancient Pythagorean Theorem, we see that the length of this vector is $\sqrt{5^2+12^2}=13$. In general, for any vector in $\mathbb{R}^2$, $\mathbf{u}=\begin{pmatrix}x\\y\end{pmatrix}$, its length is given by $\sqrt{x^2+y^2}$. The length of a vector is usually denoted by $|\mathbf{u}|$ or $\|\mathbf{u}\|$. We will use the first of the two, $|\mathbf{u}|$, to denote the length of $\mathbf{u}$. But we can make immediately an obvious, yet important, connection with matrix multiplication: **the square of the length is the dot product of a vector with itself**, or equivalently **the result of multiplying the transpose of the vector by the vector**,

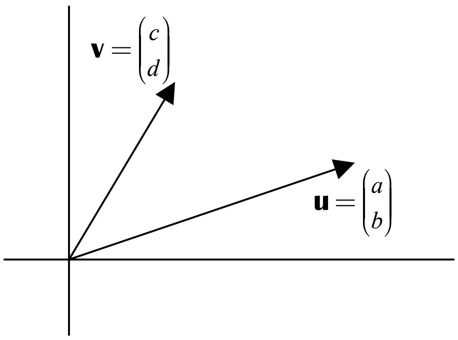
$$|\mathbf{u}|^2=\mathbf{u}\cdot\mathbf{u}=\mathbf{u}^{\mathrm{T}}\mathbf{u}\,.$$



By looking at a similar picture in $\mathbb{R}^3$, we arrive at the same result namely that for a 3-vector $\begin{pmatrix}x\\y\\z\end{pmatrix}$, its length is given by $\sqrt{x^2+y^2+z^2}$, and so once again we use what we know in the plane and in 3-space to extend to higher dimensions, and so we will agree that the **length of a vector $\mathbf{u}$** in $\mathbb{R}^n$ is given by

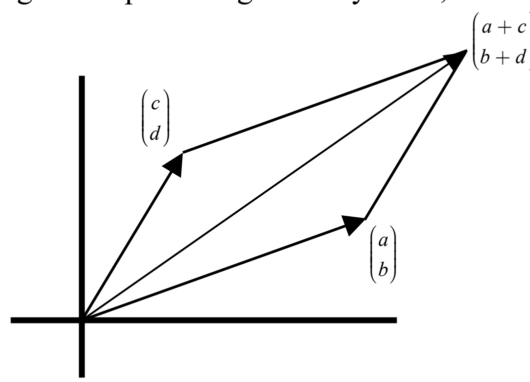
$$|\mathbf{u}|^2 = \mathbf{u} \cdot \mathbf{u} = \mathbf{u}^{\mathrm{T}} \mathbf{u}.$$

It is clear that the length is a positive quantity unless we are discussing the **0** vector which naturally has length 0. A vector is known as a **unit** vector if its length is 1, *e.g.*, $\begin{pmatrix} \frac{3}{5} \\ \frac{4}{5} \end{pmatrix}$ and $\frac{1}{11}\begin{pmatrix} 2 \\ 6 \\ 9 \end{pmatrix}$ are unit vectors. Clearly for any vector **u**, $\dfrac{\pm\mathbf{u}}{|\mathbf{u}|}$ is a unit vector.



We next look at area (and volume). Again we start in $\mathbb{R}^2$, and suppose we are given two vectors as in the picture. Then by looking at the parallelogram they form, we ask

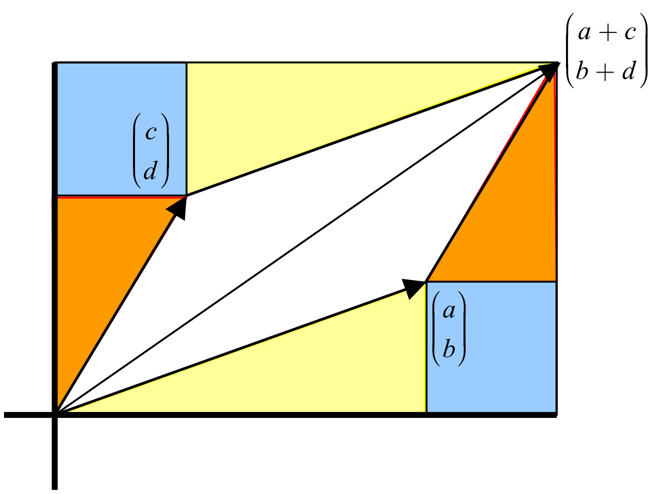
what is the area of that parallelogram?

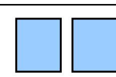
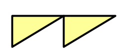
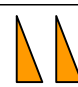


Certainly we can envelope the parallelogram in a rectangle with area

$$(a+c)(b+d) = ab + bc + ad + cd$$

and all we would have to do is subtract the shaded areas in the picture to get to the area of the parallelogram. But easily



Region	Area
	$2bc$
	ab
	cd

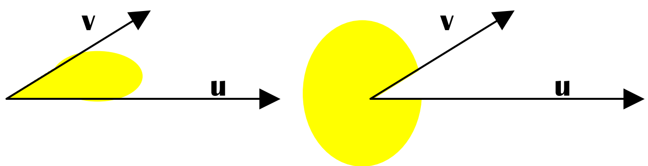
Thus, we have the area of the parallelogram is

$$\textbf{area} = ab + bc + ad + cd - 2bc - cd - ab = ad - bc$$

And we readily observe that this equals the determinant of the matrix formed from the two vectors. Namely, if $\mathbf{A} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, then the area formed by the two vectors equals determinant of **A**, abbreviated to $\det \mathbf{A}$. Thus, we can claim that

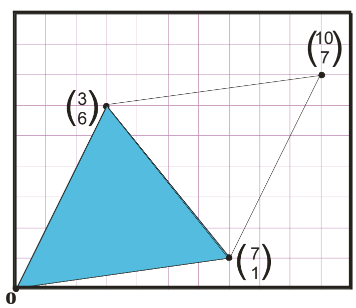
the area of the parallelogram formed from two vectors is equal to the determinant of the matrix formed with those vectors as its columns.

But the keen reader may appreciate the fact that there are two matrices that can be formed from two vectors, and thus we need to briefly discuss the **orientation** of two vectors in the plane.

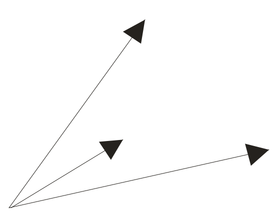


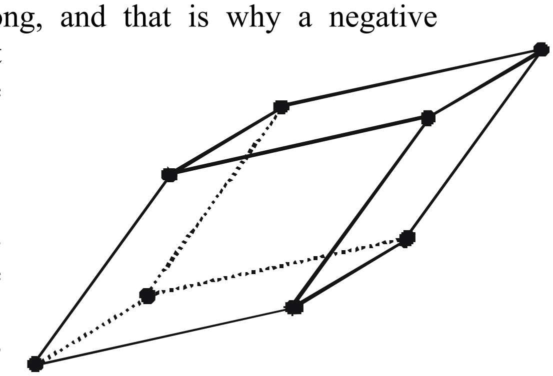
Given two nonzero, nonparallel vectors $\mathbf{u}$ and $\mathbf{v}$, then we see we can sweep from one vector to the other two ways, one which is more than 180°, and one which is less than 180°. We will always mean by the sweep from one vector to the other to be the one which is less than 180°. Thus in our picture, the sweep is the one on the left. The sweep from one vector to the other can go in one of two directions, clockwise or counterclockwise, and traditionally the former is **negative orientation** while the latter is **positive**. So in our picture the sweep from $\mathbf{u}$ to $\mathbf{v}$ is counterclockwise while the sweep from $\mathbf{v}$ to $\mathbf{u}$ is clockwise.

It is then an interesting geometric fact (but not of great consequence to us since we will be mainly discussing determinants of matrices), that the **determinant of a 2×2 matrix is positive if its columns are positively oriented and negative otherwise**.



Example 2. The area of the parallelogram with edges $\begin{pmatrix}7\\1\end{pmatrix}$ and $\begin{pmatrix}3\\6\end{pmatrix}$ is the determinant of $\begin{pmatrix}7&3\\1&6\end{pmatrix}$ which is 39, which means that the area of the triangle with vertices the origin, $\begin{pmatrix}7\\1\end{pmatrix}$ and $\begin{pmatrix}3\\6\end{pmatrix}$ is half of that, $\frac{39}{2}$. Note that if we had used the matrix $\begin{pmatrix}3&7\\6&1\end{pmatrix}$ we would have obtained -39 instead, and in fact then the angle between the vectors would be going clockwise instead of counterclockwise, and the orientation would be wrong, and that is why a negative determinant was obtained. Thus, the determinant not only computes area, but also the orientation of the vectors.





Now we move on to 3-space, and volume. Given three vectors in space, we easily visualize the parallelepiped that they form. This is similar to the parallelogram formed by two vectors in the plane. In the plane case, we saw that **the determinant of the matrix formed by the two vectors was in absolute value the**

area of the parallelogram formed by the two vectors. So we should not be surprised to find the theorem that states that the **volume of the box made by three vectors in space is the determinant with the orientation of the three vectors determining the sign.** We will not prove this theorem, but nevertheless we state it.

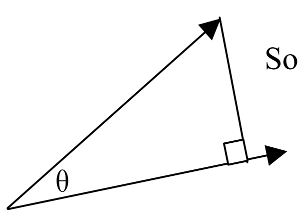
> **Theorem (Determinants and Volumes).** Let $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ be vectors in 3-space. Then the volume of the box they form is $\pm\det(\mathbf{A})$ where $\mathbf{A} = (\mathbf{u} \quad \mathbf{v} \quad \mathbf{w})$.

Of course, the sign depends of the **orientation** of the three vectors. In the plane we had two possible orientations: clockwise (-1) and counterclockwise (1). In 3-space we have 6 orientations, three of them positive and three of them negative. The basic positive one is *x*-*y*-*z* and its cyclical permutations: *y*-*z*-*x* and *z*-*x*-*y*.

Example 3. Let $\mathbf{u} = \begin{pmatrix} 1 \\ 4 \\ -7 \end{pmatrix}$, $\mathbf{v} = \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix}$ and $\mathbf{w} = \begin{pmatrix} 0 \\ -1 \\ 2 \end{pmatrix}$. Then $\det(\mathbf{u} \quad \mathbf{v} \quad \mathbf{w}) = 0$, which means the box has no height, or that the vector $\mathbf{w}$ is in the same plane as $\mathbf{u}$ and $\mathbf{v}$. Indeed, $9\mathbf{w} = \mathbf{v} - 2\mathbf{u}$. On the other hand, if $\mathbf{u} = \begin{pmatrix} 1 \\ 4 \\ -7 \end{pmatrix}$, $\mathbf{v} = \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix}$ and $\mathbf{w} = \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}$, then the volume of the box is 9.

We are not yet ready to define determinants in any size, so we will postpone further discussion of them. But of course, when we do, they will represent volumes in that dimension.

We are ready to discuss the third important geometric concern, **angle**. Again, we start in $\mathbb{R}^2$. Clearly, the angle between two vectors in the plane is the same as the angle between their rays, since it is really these that determine the angle. Thus, we can without loss of generality take the two vectors to be of length 1.



So let $\mathbf{u} = \begin{pmatrix} a \\ b \end{pmatrix}$, and $\mathbf{v} = \begin{pmatrix} c \\ d \end{pmatrix}$ be two **unit** vectors, so $a^2 + b^2 = 1$ and $c^2 + d^2 = 1$. We will let θ denote the angle between them.

We know that the area of the parallelogram that the two vectors form is the determinant $ad - bc$ (if we assume the vectors are positively oriented). But since the base of the parallelogram is 1, this determinant represents the height of the parallelogram. Thus from the picture, we know

$$\sin\theta = ad - bc .$$

But then since

$$1=(a^2+b^2)(c^2+d^2)=a^2c^2+a^2d^2+b^2c^2+b^2d^2,$$

we have that

$$\begin{aligned}\cos^2\theta=1-\sin^2\theta &= a^2c^2+a^2d^2+b^2c^2+b^2d^2-a^2d^2+2abcd-b^2c^2\\ &= a^2c^2+2abcd+b^2d^2=(ac+bd)^2\end{aligned}$$

And so we arrive at the fact

$$\cos\theta=\mathbf{u}\cdot\mathbf{v}=\mathbf{u}^{\mathrm{T}}\mathbf{v}.$$

If the vectors had not been unit vectors, then the equation would have been

$$\cos\theta=\frac{\mathbf{u}\cdot\mathbf{v}}{|\mathbf{u}||\mathbf{v}|}$$

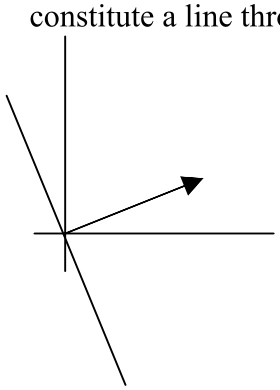
because from any vector **u**, we can obtain a unit vector in the same direction by simply dividing by its length.

Example 4. Let $\mathbf{u}=\begin{pmatrix}3\\-3\end{pmatrix}$ and $\mathbf{v}=\begin{pmatrix}3\\-2\end{pmatrix}$. Then $\cos\theta=\dfrac{15}{\sqrt{18}\sqrt{13}}$, so $\theta\approx 11.31^\circ$.

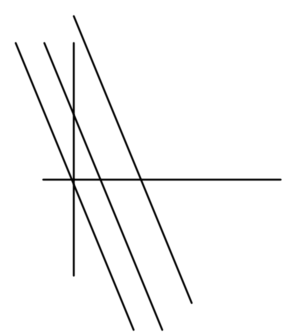
From the cosine expression, we immediately get that two vectors are **perpendicular** to each other, which means the angle between them is 90°, if and only if their dot product is 0. For us, vectors are **orthogonal** is a synonym to their being perpendicular. We will use $\mathbf{u}\perp\mathbf{v}$ to denote that $\mathbf{u}$ and $\mathbf{v}$ are orthogonal.

Example 5. Let $\mathbf{u}=\begin{pmatrix}a\\b\end{pmatrix}$. Then $\mathbf{v}=\begin{pmatrix}-b\\a\end{pmatrix}$ satisfies $\mathbf{u}\cdot\mathbf{v}=0$, and so $\mathbf{u}\perp\mathbf{v}$.

Example 6. Clearly in $\mathbb{R}^2$, if we take a nonzero vector **u**, then all vectors orthogonal to it constitute a line through the origin.



Specifically, let $\mathbf{u}=\begin{pmatrix}2\\3\end{pmatrix}$. Then when we ask for all vectors **x** orthogonal to it, we are asking for all vectors that satisfy $\mathbf{u}\cdot\mathbf{x}=0$. But as usual, it is smart to switch to matrix multiplication, so we are asking for all vectors $\mathbf{x}$ that satisfy the equation $\mathbf{u}^{\mathrm{T}}\mathbf{v}=0$, or equivalently, all solutions to the equation $\mathbf{A}\mathbf{x}=0$ where $\mathbf{A}=(\mathbf{u}^{\mathrm{T}})$. Thus, in our specific case, $\mathbf{A}=(2\quad 3)$, so then our vectors $\mathbf{x}=\begin{pmatrix}x\\y\end{pmatrix}$ must satisfy the equation $2x+3y=0$. Of course other linear equations with the same coefficients, such as $2x+3y=5$, represent lines parallel to $2x+3y=0$.



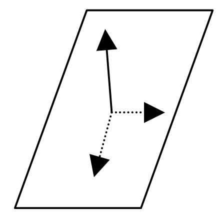
Moving on to 3-space is easy, since as aforementioned, every two vectors lie in a plane, the notion of angle is identical in 3-space and hence in any space as in the plane, for any two unit vectors, their angle is given by

$$\cos\theta = \mathbf{u}\cdot\mathbf{v} = \mathbf{u}^{\mathrm{T}}\mathbf{v}.$$

Thus, from our point of view, more importantly, two vectors are orthogonal if and only if their dot product is 0, or equivalently,

$$\mathbf{u}\cdot\mathbf{v} = \mathbf{u}^{\mathrm{T}}\mathbf{v} = 0.$$

But the geometry of all vectors perpendicular to a given vector changes although the algebraic expression remains the same.



Example 7. Let $\mathbf{u} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$. What is the shape of all vectors perpendicular to this vector? It is the plane of all vectors $\mathbf{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ that satisfy the linear equation $x + 2y + 3z = 0$. Equivalently these are the vectors that satisfy the matrix equation $\mathbf{Ax} = 0$ where $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$, *i.e.*, the equation $x + 2y + 3z = 0$.

Thus, a linear equation will no longer represent a line in 3-space, but rather it will be a **plane**, and in higher dimensions a linear equation with 0 constant, which represents all vectors perpendicular to a given vector, is referred to as a **hyperplane**.

Example 8. Consider a single nonzero vector $\mathbf{u}$ of size n, and its orthogonal complement, $\mathbf{u}^{\perp} = \{\mathbf{x} \mid \mathbf{u}^{\mathrm{T}}\mathbf{x} = 0\}$. We will view it in different situations:

n	$\mathbf{u}$	$\mathbf{x}$	$\mathbf{u}^{\perp}$	Geometric Shape
2	$\begin{pmatrix} a \\ b \end{pmatrix}$	$\begin{pmatrix} x \\ y \end{pmatrix}$	$ax + by = 0$	A line in the plane
3	$\begin{pmatrix} a \\ b \\ c \end{pmatrix}$	$\begin{pmatrix} x \\ y \\ z \end{pmatrix}$	$ax + by + cz = 0$	A plane in 3-space
4	$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$	$\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$	$ax + by + cz + dw = 0$	A hyperplane in 4-space
n	$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$	$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$	$a_1x_1 + \cdots + a_nx_n = 0$	A hyperplane in n-space

Thus, in general, the shape of $\mathbf{u}^{\perp} = \left\{\mathbf{x} \mid \mathbf{u}^{\mathrm{T}}\mathbf{x} = 0\right\}$ is what is referred to, as we saw above, as a **hyperplane**.

Then of course the geometric nature of all the solutions to a linear system is clear then as the intersection of various hyperplanes.

❿ The Subspaces of a Matrix

With a little bit of geometric understanding, we now return to one of the central themes of the course: **linear systems**. Let an $m \times n$ matrix $\mathbf{A}$ be given. Then there are two collections of vectors that are of interest:

❶ for which $\mathbf{b}$'s does the system $\mathbf{Ax} = \mathbf{b}$ have a solution?

❷ which $\mathbf{u}$'s are solutions to the homogeneous system $\mathbf{Ax} = \mathbf{0}$?

We discuss ❶ first. We already have an answer for it: $\mathbf{b}$ will be in this collection, that is, $\mathbf{Ax} = \mathbf{b}$ will have a solution, if and only if $\mathbf{b}$ is a linear combination of the columns of $\mathbf{A}$. Hence this collection of vectors is known as the **column space** of $\mathbf{A}$, and is denoted by $\mathcal{C}(\mathbf{A})$.

Certainly $\mathcal{C}(\mathbf{A})$ is a collection of vectors of size *m*, so $\mathcal{C}(\mathbf{A})$ is contained in $\mathbb{R}^m$, and we are ready to make three key observations about this set:

① $\mathbf{0}$ is in $\mathcal{C}(\mathbf{A})$ since $\mathbf{Ax} = \mathbf{0}$ can always be solved—at least trivially, $\mathbf{A0} = \mathbf{0}$.

② If $\mathbf{b}$ and $\mathbf{c}$ are in $\mathcal{C}(\mathbf{A})$, then so is their sum, $\mathbf{b} + \mathbf{c} \in \mathcal{C}(\mathbf{A})$[1]. The reason for this is easy. If $\mathbf{u}$ and $\mathbf{v}$ are respective solutions to $\mathbf{Ax} = \mathbf{b}$ and $\mathbf{Ax} = \mathbf{c}$, then $\mathbf{u} + \mathbf{v}$ is a solution to $\mathbf{Ax} = (\mathbf{b} + \mathbf{c})$: $\mathbf{A}(\mathbf{u} + \mathbf{v}) = \mathbf{Au} + \mathbf{Av} = \mathbf{b} + \mathbf{c}$.

The last property is similar to the previous one.

③ If $\mathbf{b}$ is in $\mathcal{C}(\mathbf{A})$, and a is any scalar, then $a\mathbf{b} \in \mathcal{C}(\mathbf{A})$ also. Let $\mathbf{u}$ be a solution to $\mathbf{Ax} = \mathbf{b}$, then $\mathbf{A}(a\mathbf{u}) = a\mathbf{Au} = a\mathbf{b}$.

Any collection of vectors in $\mathbb{R}^n$ that satisfy these three properties will be referred to as a **vector space** or **vector subspace** (or just **subspace**), and this is an important concept. That is why we call the previous example the column *space* of a matrix.

Thus $\mathcal{C}(\mathbf{A})$ consists of all linear combinations of the columns of $\mathbf{A}$, and it is also known as the **span** of the columns. The name makes sense if one recalls that the span of two vectors is a plane as we saw before.

Thus the **span** of any set of vectors is the set of linear combinations of them. In symbols if $\mathbf{w}_1$, $\mathbf{w}_2$, …, $\mathbf{w}_n$ are vectors in $\mathbb{R}^m$, their **span**, denoted by $[\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n]$, is the set of their linear combinations:

$$[\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n] = \{a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_n\mathbf{w}_n \mid a_1, a_2, \ldots, a_n \in \mathbb{R}\}.$$

---

[1] The symbol $\in$ reads *belongs to* or *is in*.

The connection is clear.

> **Theorem** (Column Spaces). Let $\mathbf{A} = (\mathbf{w}_1 \quad \mathbf{w}_2 \quad \cdots \quad \mathbf{w}_n)$ be an $m \times n$ matrix. Let $\mathbf{b} \in \mathbb{R}^m$. Then the following three conditions are equivalent,
>
> ① $\mathbf{b} \in \mathcal{C}(\mathbf{A})$.
>
> ② $\mathbf{b}$ is a linear combinations of the columns of $\mathbf{A}$, $\mathbf{b} \in [\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n]$.
>
> ③ There is a vector $\mathbf{u} \in \mathbb{R}^n$ such that $\mathbf{Au} = \mathbf{b}$, or in other words, the system $\mathbf{Ax} = \mathbf{b}$ has a solution.

Example 1. Of course, $[\mathbf{w}] = \{a\mathbf{w} \mid a \in \mathbb{R}\}$ is a line as long as $\mathbf{w} \neq \mathbf{0}$.

Consider now two vectors, $\mathbf{w}$ and $\mathbf{v}$, and let $\mathbf{A} = (\mathbf{w} \quad \mathbf{v})$. And assume neither vector is $\mathbf{0}$. If $\mathbf{v} \in [\mathbf{w}]$, then we know that $[\mathbf{w}, \mathbf{v}] = [\mathbf{w}]$ is just a line, while otherwise it is a plane. But observe that $[\mathbf{w}, \mathbf{v}] = [\mathbf{w}]$ only if $r(\mathbf{A}) = 1$ since $\mathbf{v}$ could not be pivotal if $\mathbf{v} \in [\mathbf{w}]$.

Let $\mathbf{w}$, $\mathbf{v}$ and $\mathbf{u}$ be nonzero vectors in $\mathbb{R}^m$, and $\mathbf{A} = (\mathbf{w} \quad \mathbf{v} \quad \mathbf{u})$. Then $\mathcal{C}(\mathbf{A})$ is either a line (if all the vectors happen to be multiples of each other), or it is a plane (if one of them is in the span of the others), or they generate a 3-dimensional type subspace in $\mathbb{R}^m$.

Example 2. What is the column space of the identity $\mathbf{I}_m$? Clearly if $m = 3$, every vector can be written as a linear combination of them: $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + c\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, so the columns span all of $\mathbb{R}^3$. One can readily see this is always the case, $\mathcal{C}(\mathbf{I}_m) = \mathbb{R}^m$. From the equation point of view this is also obvious since we are asking whether we can solve $\mathbf{Ix} = \mathbf{b}$ for any given $\mathbf{b}$.

Example 3. What is the column space of the matrix $\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}$? Equivalently, what is the span of $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$? Clearly, since the first three vectors already span all of $\mathbb{R}^3$, these four vectors will also span $\mathbb{R}^3$.

Example 4. Let $\mathbf{A} = \begin{pmatrix} 1 & 4 & 9 \\ 2 & 5 & 12 \\ 3 & 6 & 15 \end{pmatrix}$. Then of course $\mathcal{C}(\mathbf{A})$ is the span of $\mathbf{w} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $\mathbf{v} = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}$

and $\mathbf{u}=\begin{pmatrix}9\\12\\15\end{pmatrix}$. Since they are all nonzero, they each generate a line, and also since none of them is a multiple of another, we do have that any two of them span a plane. But what is not at all clear is whether they are all in one plane, or that indeed they generate or span all of $\mathbb{R}^3$. But $\mathbf{A}$ reduces to $\begin{pmatrix}1&0&1\\0&1&2\\0&0&0\end{pmatrix}$, so we know that $\mathbf{u}=\mathbf{w}+2\mathbf{v}$ (by the **Nonpivotal Columns Lemma** of the last section). Hence any linear combination of $\mathbf{w}$, $\mathbf{v}$ and $\mathbf{u}$, is simply a linear combination of just $\mathbf{w}$ and $\mathbf{v}$:

$$a\mathbf{w}+b\mathbf{v}+c\mathbf{u}=a\mathbf{w}+b\mathbf{v}+c\left(\mathbf{w}+2\mathbf{v}\right)=\left(a+c\right)\mathbf{w}+\left(b+2c\right)\mathbf{v}\,.$$

But also just as easily, $\mathbf{w}=\mathbf{u}-2\mathbf{v}$, or $\mathbf{v}=\frac{1}{2}\left(\mathbf{u}+\mathbf{w}\right)$. And so we have that the span of all three vectors is a plane in $\mathbb{R}^3$, $\mathcal{C}\left(\mathbf{A}\right)=\left[\mathbf{w},\mathbf{v},\mathbf{u}\right]=\left[\mathbf{w},\mathbf{v}\right]=\left[\mathbf{w},\mathbf{u}\right]=\left[\mathbf{v},\mathbf{u}\right]$.

Thus, if $\mathbf{B}=\begin{pmatrix}1&4\\2&5\\3&6\end{pmatrix}$, then $\mathcal{C}\left(\mathbf{A}\right)=\mathcal{C}\left(\mathbf{B}\right)$.

Yet if we were to ask which of these systems has a solution $\mathbf{Ax}=\begin{pmatrix}2\\5\\8\end{pmatrix}$, or $\mathbf{Ax}=\begin{pmatrix}2\\5\\6\end{pmatrix}$, or $\mathbf{Ax}=\begin{pmatrix}7\\8\\10\end{pmatrix}$, we would need to resort to reducing in order to answer the questions. That is because at present there is no clear way of writing a vector as a linear combination of the columns of a matrix. However, there is an exception to this. So we pause to consider a useful idea.

Let $\mathbf{w}_1$, $\mathbf{w}_2$, …, $\mathbf{w}_n$ be vectors in $\mathbb{R}^m$. We will refer to them as **transparent** if there is a set of positions among the rows of the $\mathbf{w}$'s, we can pick n of them to be $\mathbf{I}_n$. For example, $\begin{pmatrix}1\\0\\2\\0\\1\end{pmatrix}$, $\begin{pmatrix}3\\1\\7\\0\\0\end{pmatrix}$ and $\begin{pmatrix}0\\0\\4\\1\\0\end{pmatrix}$ is transparent since we can see the identity matrix $\mathbf{I}_3$ in rows 2, 4 and 5. But also observe that once a set is transparent it becomes trivial to write which vectors are linear combinations of them: they are the vectors of the form $\begin{pmatrix}3a+c\\a\\7a+4b+2c\\b\\c\end{pmatrix}$, and so we can instantly decide that $\begin{pmatrix}7\\2\\12\\-1\\1\end{pmatrix}=2\begin{pmatrix}3\\1\\7\\0\\0\end{pmatrix}-\begin{pmatrix}0\\0\\4\\1\\0\end{pmatrix}+\begin{pmatrix}1\\0\\2\\0\\1\end{pmatrix}$ is a linear combination of the three vectors. Equivalently, $\begin{pmatrix}1&3&0\\0&1&0\\2&7&4\\0&0&1\\1&0&0\end{pmatrix}\mathbf{x}=\begin{pmatrix}7\\2\\12\\-1\\1\end{pmatrix}$ has a solution, $\mathbf{u}=\begin{pmatrix}1\\2\\-1\end{pmatrix}$

Returning to our previous example where we consider $\mathbf{A}=\begin{pmatrix}1&4&9\\2&5&12\\3&6&15\end{pmatrix}$. Then we claim that $\begin{pmatrix}1\\0\\-1\end{pmatrix}$ and $\begin{pmatrix}0\\1\\2\end{pmatrix}$ is a transparent set that spans $\mathcal{C}(\mathbf{A})$, so an alternate description of the plane is $\begin{pmatrix}a\\b\\2b-a\end{pmatrix}$ where $a,b\in\mathbb{R}$. Then easily we could say that of $\mathbf{Ax}=\begin{pmatrix}2\\5\\8\end{pmatrix}$, or $\mathbf{Ax}=\begin{pmatrix}2\\5\\6\end{pmatrix}$, or $\mathbf{Ax}=\begin{pmatrix}7\\8\\10\end{pmatrix}$, only the first of the three systems has a solution. We will soon see how to arrive at the transparent set.

In a slight twist, let us now consider the span of the three vectors: $\begin{pmatrix}1\\4\\9\end{pmatrix}$, $\begin{pmatrix}2\\5\\12\end{pmatrix}$ and $\begin{pmatrix}3\\6\\15\end{pmatrix}$. Note that these are the columns of $\mathbf{A}^{\mathrm{T}}$, or equivalently the **rows** of $\mathbf{A}$. Since the reduced from of $\mathbf{A}^{\mathrm{T}}$ is $\begin{pmatrix}1&0&-1\\0&1&2\\0&0&0\end{pmatrix}$, we see again that $\mathcal{C}(\mathbf{A}^{\mathrm{T}})$ is also a plane. This is not a coincidence. Neither is the fact that the nonzero rows of this reduced matrix form the transparent set that spanned $\mathcal{C}(\mathbf{A})$ above.

To reaffirm this connection, since the reduced form of $\mathbf{A}$ was $\begin{pmatrix}1&0&1\\0&1&2\\0&0&0\end{pmatrix}$, $\begin{pmatrix}1\\0\\1\end{pmatrix}$ and $\begin{pmatrix}0\\1\\2\end{pmatrix}$ form a transparent set that spans $\mathcal{C}(\mathbf{A}^{\mathrm{T}})$.

These connections will be made clearer in the next section.

Example 5. Consider the matrix $\mathbf{M} = \begin{pmatrix} 1 & 4 & 5 & 6 & 2 \\ 2 & 7 & 7 & 10 & 3 \\ -1 & 3 & 16 & 8 & 5 \\ 3 & 12 & 15 & 18 & 6 \end{pmatrix}$. Then we know the column space $\mathcal{C}(\mathbf{M})$ is a subspace of $\mathbb{R}^4$, but it is not clear at all what it consists of. But actually, $\mathbf{u}_2 = 2\mathbf{u}_1 + \mathbf{u}_5$, $\mathbf{u}_3 = -\mathbf{u}_1 + 3\mathbf{u}_5$ and $\mathbf{u}_4 = 2\mathbf{u}_1 + 2\mathbf{u}_5$, and so $\mathcal{C}(\mathbf{M})$ is the plane spanned by $\mathbf{u}_1$ and $\mathbf{u}_5$. When we reduce $\mathbf{M}^{\mathrm{T}}$ we get $\begin{pmatrix} 1 & 0 & 13 & 3 \\ 0 & 1 & -7 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, so $\mathcal{C}(\mathbf{M})$ consists of all vectors of the form $\begin{pmatrix} a \\ b \\ 13a - 7b \\ 3a \end{pmatrix}$.

Example 6. The Column Space of a Reduced Matrix. Consider as a specific example, the matrix $\mathbf{A} = \begin{pmatrix} 1 & * & 0 & * & 0 \\ 0 & 0 & 1 & * & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, which is reduced. For which $\mathbf{b}$'s does the system $\mathbf{Ax} = \mathbf{b}$ have a solution? Or equivalently, what is the column space of $\mathbf{A}$? As we saw before, $\mathbf{Ax} = \mathbf{b}$ will have a solution if and only if the fourth coordinate of $\mathbf{b}$ is 0. Thus the column space of $\mathbf{A}$ consists of all vectors of the form $\begin{pmatrix} a \\ b \\ c \\ 0 \end{pmatrix}$. Note then that it is the subspace of $\mathbb{R}^4$ which is the span of the three pivotal columns of $\mathbf{A}$, $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, and $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, a transparent set.

The other two columns are not necessary since we can readily see that the second column is a multiple of the first one, and the fourth column is a linear combination of the first and the third. Again, this is not surprising since we saw before that the nonpivotal columns are always linear combinations of the pivotal ones.

Example 7. The Column Space of a Matrix. Consider now any matrix whose reduced form is of the type in the previous example—$\mathbf{A}=\begin{pmatrix}10&30&3&55&1\\16&48&5&89&2\\10&30&2&50&2\\13&39&3&67&1\end{pmatrix}$ is such a matrix, and its reduced form is $\mathbf{M}=\begin{pmatrix}1&3&0&4&0\\0&0&1&5&0\\0&0&0&0&1\\0&0&0&0&0\end{pmatrix}$. Then in the reduced form we observe trivially that the second column is three times the first one—but the same is true in the original matrix (recall the **Nonpivotal Columns Lemma**), and that is simply that $\mathbf{M}\begin{pmatrix}3\\-1\\0\\0\\0\end{pmatrix}=\mathbf{0}$ if and only if $\mathbf{A}\begin{pmatrix}3\\-1\\0\\0\\0\end{pmatrix}=\mathbf{0}$. Similarly, we see that the fourth column of $\mathbf{M}$ is 4 times the first one added to 5 times the third one, and the same is true for $\mathbf{A}$—again $\mathbf{M}\begin{pmatrix}4\\0\\5\\-1\\0\end{pmatrix}=\mathbf{0}$ if and only if $\mathbf{A}\begin{pmatrix}4\\0\\5\\-1\\0\end{pmatrix}=\mathbf{0}$. Thus, we know then that the first, third and fifth columns of $\mathbf{A}$ span its column space. And since the reduced form of $\mathbf{A}^{\mathrm{T}}$ is $\begin{pmatrix}1&0&0&4\\0&1&0&-2\\0&0&1&0.5\\0&0&0&0\\0&0&0&0\end{pmatrix}$, we know the column space $\mathcal{C}(\mathbf{A})$ consists of vectors that are of the form $\begin{pmatrix}a\\b\\c\\4a-2b+\frac{c}{2}\end{pmatrix}$

As an easy corollary to the definition of column space we add to our understanding of the existence of solutions:

Corollary (Existence of Solutions). Let $\mathbf{A}$ be $m \times n$. Then the following are equivalent:

❶ $\mathcal{C}(\mathbf{A}) = \mathbb{R}^m$;

❷ $\mathbf{Ax} = \mathbf{b}$ will have at least one solution for every $\mathbf{b} \in \mathbb{R}^m$;

❸ $\mathbf{A}$ has full row rank;

❹ $r(\mathbf{A}) = m$.

Thus, if $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, then since $r(\mathbf{A}) = 2$, we know $\mathcal{C}(\mathbf{A}) = \mathbb{R}^2$, so every system of the form $\mathbf{Ax} = \mathbf{b}$ will have a solution—in fact infinitely many.

The following is a useful fact that we have tacitly been using above.

Theorem. Let $\mathbf{w}_1$, $\mathbf{w}_2$, …, $\mathbf{w}_n$ be vectors in $\mathbb{R}^m$. If $\mathbf{v} \in \mathbb{R}^m$ is a linear combination of the $\mathbf{w}$'s, that is, if $\mathbf{v} = c_1\mathbf{w}_1 + c_2\mathbf{w}_2 + \cdots + c_n\mathbf{w}_n$ for some scalars $c_1, c_2, \ldots, c_n \in \mathbb{R}$, then

$$[\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n, \mathbf{v}] = [\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n].$$

Proof. Obviously, since

$$a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_n\mathbf{w}_n = a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_n\mathbf{w}_n + 0\mathbf{v},$$

we have that $[\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n]$ is contained in $[\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n, \mathbf{v}]$. Conversely, if we take an element of the latter subspace, $a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_n\mathbf{w}_n + a\mathbf{v}$, then by substituting by $\mathbf{v}$, we get

$$\begin{aligned} a_1\mathbf{w}_1 &+ a_2\mathbf{w}_2 + \cdots + a_n\mathbf{w}_n + a\mathbf{v} \\ &= a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_n\mathbf{w}_n + a(c_1\mathbf{w}_1 + c_2\mathbf{w}_2 + \cdots + c_n\mathbf{w}_n) \\ &= (a_1 + c_1)\mathbf{w}_1 + (a_2 + c_2)\mathbf{w}_2 + \cdots + (a_n + c_n)\mathbf{w}_n, \end{aligned}$$

which is clearly in $[\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n]$. ⌘

Basically what this theorem claims is that

a vector that is in the span of the others is not needed for the span.

By just taking one column at a time, we get

Corollary. Let $\mathbf{A}$ be $m \times n$ and let $\mathbf{B}$ be $m \times q$. Suppose $\mathcal{C}(\mathbf{B})$ is contained in $\mathcal{C}(\mathbf{A})$. Then if $\mathbf{M}$ is the horizontal stacking of $\mathbf{A}$ and $\mathbf{B}$, $\mathbf{M} = (\mathbf{A} \quad \mathbf{B})$, we have $\mathcal{C}(\mathbf{M}) = \mathcal{C}(\mathbf{A})$.

Now that we have thoroughly discussed the column space, we are ready to start with the second very important subspace associated with a matrix. As usual, we are given an $m\times n$ matrix **A**. Let us continue with question ❷:

which **u**'s are solutions to the homogeneous system $\mathbf{Ax}=\mathbf{0}$?

The collection of all such **u**'s is called the **null space** of $\mathbf{A}$, and it is denoted by $\mathrm{N}(\mathbf{A})$. Certainly given a vector, we can readily decide if it in this set or not by simply multiplying by **A**. If we get **0** it is, if we don't, it is not. We immediately justify the use of the word *space*.

> **Theorem (Null Spaces).** Let $\mathbf{A}$ be $m\times n$. Then its null space, $\mathrm{N}(\mathbf{A})$, is a subspace of $\mathbb{R}^n$.

Proof. We have to show the three properties of subspaces. Trivially, $\mathbf{0}$ is in the null space since $\mathbf{A0}=\mathbf{0}$. Suppose that **u** and **v** are both in the null space of **A**, that means that we have both $\mathbf{Au}=\mathbf{0}$ and $\mathbf{Av}=\mathbf{0}$. But then trivially, $\mathbf{A}(\mathbf{u}+\mathbf{v})=\mathbf{Au}+\mathbf{Av}=\mathbf{0}+\mathbf{0}=\mathbf{0}$, by distributivity, so $\mathbf{u}+\mathbf{v}$ is also in $\mathrm{N}(\mathbf{A})$. Similarly if a is any scalar, and $\mathbf{u}\in\mathrm{N}(\mathbf{A})$, then $\mathbf{A}(a\mathbf{u})=a(\mathbf{Au})=a\mathbf{0}=\mathbf{0}$, so $a\mathbf{u}\in\mathrm{N}(\mathbf{A})$. ⌘

But additionally, we already know how to find the solutions to any system, so we can describe the null space as the set of all linear combinations of a set of vectors—which is actually transparent.

Example 8. Let $\mathbf{A}=\begin{pmatrix}1&2&3\\1&1&1\end{pmatrix}$. Then its reduced form is $\begin{pmatrix}1&0&-1\\0&1&2\end{pmatrix}$, so $\mathrm{N}(\mathbf{A})$ consists of all vectors of the form $t\begin{pmatrix}1\\-2\\1\end{pmatrix}=\begin{pmatrix}t\\-2t\\t\end{pmatrix}$ where $t\in\mathbb{R}$. The shape of this subspace is that of a line, all multiples of the vector $\begin{pmatrix}1\\-2\\1\end{pmatrix}$.

Example 9. Let $\mathbf{A}=\begin{pmatrix}1&3&2&4&1\\2&6&1&5&-4\\3&9&3&9&-3\\4&12&4&12&-4\end{pmatrix}$. Then it reduces to $\begin{pmatrix}1&3&0&2&-3\\0&0&1&1&2\\0&0&0&0&0\\0&0&0&0&0\end{pmatrix}$ and so the set of solutions is the span of the vectors $\begin{pmatrix}-3\\1\\0\\0\\0\end{pmatrix}$, $\begin{pmatrix}-2\\0\\-1\\1\\0\end{pmatrix}$ and $\begin{pmatrix}3\\0\\-2\\0\\1\end{pmatrix}$, and as remarked before this is automatically a transparent set.

Again as an easy corollary to the definition we obtain the following:

> **Corollary (Uniqueness of Solutions).** Let $\mathbf{A}$ be $m \times n$. Then the following conditions are equivalent:
>
> ❶ $\mathrm{N}(\mathbf{A}) = \mathbf{0}$;
>
> ❷ $\mathbf{Ax} = \mathbf{b}$ will have at most one solution for every $\mathbf{b} \in \mathbb{R}^m$;
>
> ❸ $\mathbf{A}$ has full column rank;
>
> ❹ $r(\mathbf{A}) = n$.

For example, since $\mathbf{A} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$ has rank 2, every system of the form $\mathbf{Ax} = \mathbf{b}$ will have at most one solution, and since it is not of full row rank, there will be systems with no solutions.

In another version of an old result

> **Corollary (Linear Systems).** Consider the system $\mathbf{Ax} = \mathbf{b}$ and let $\mathbf{u}$ be a particular solution, then all solutions are given by the set $\mathbf{u} + \mathrm{N}(\mathbf{A})$.

Thus, the shape of solutions is that of a flat subspace of the same shape as $\mathrm{N}(\mathbf{A})$ since we are simply translating the subspace to pass through a specific solution to the system $\mathbf{Ax} = \mathbf{b}$. In particular, if $\mathrm{N}(\mathbf{A}) \neq 0$, then the system will have infinitely many solutions.

Of course, if S and T are both subsets of a vector space, then one defines their sum, $S + T = \{\mathbf{u} + \mathbf{v} | \mathbf{u} \in S, \mathbf{v} \in T\}$.

Example 10. Let $\mathbf{A} = \begin{pmatrix} 1 & 3 & 2 & 4 & 1 \\ 2 & 6 & 1 & 5 & -4 \\ 3 & 9 & 3 & 9 & -3 \\ 4 & 12 & 4 & 12 & -4 \end{pmatrix}$. Then since the vectors $\begin{pmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} -2 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 3 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix}$ span its null space, every system $\mathbf{Ax} = \mathbf{b}$ that has a solution $\mathbf{u}$, will have all solutions in the form $\mathbf{u} + a\begin{pmatrix} -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + b\begin{pmatrix} -2 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + c\begin{pmatrix} 3 \\ 0 \\ -2 \\ 0 \\ 1 \end{pmatrix}$.

Thus with every $m\times n$ matrix $\mathbf{A}$ we have associated two spaces of vectors, $\mathcal{C}(\mathbf{A})$, the column space, a subspace of $\mathbb{R}^m$, and $\mathrm{N}(\mathbf{A})$, the null space, a subspace of $\mathbb{R}^n$. If we now consider the same spaces but for the transpose matrix, we obtain another two spaces: $\mathcal{C}(\mathbf{A}^{\mathrm{T}})$, the column space, a subspace of $\mathbb{R}^n$, and $\mathrm{N}(\mathbf{A}^{\mathrm{T}})$, the null space, a subspace of $\mathbb{R}^m$.

A key observation is then that $\mathcal{C}(\mathbf{A}^{\mathrm{T}})$ and $\mathrm{N}(\mathbf{A})$ are both subspaces of the same space $\mathbb{R}^n$. Similarly, $\mathcal{C}(\mathbf{A})$ and $\mathrm{N}(\mathbf{A}^{\mathrm{T}})$ live in the same place, $\mathbb{R}^m$. There is a very intimate relation between the two pairs of subspaces.

Recall that we say that two vectors $\mathbf{u}$ and $\mathbf{v}$ are perpendicular if $\mathbf{u}\cdot\mathbf{v}=\mathbf{u}^{\mathrm{T}}\mathbf{v}=0$, and we denote this fact by $\mathbf{u}\perp\mathbf{v}$. Then:

> **Theorem** (Orthogonal Complements). Let $\mathbf{A}$ be $m\times n$. Let $\mathbf{u}$ be a vector of size n and let $\mathbf{w}$ be a vector of size m. Then the following are true:
>
> ❶ $\mathbf{u}\in\mathrm{N}(\mathbf{A})$ if and only if $\mathbf{u}\perp\mathbf{v}$ for every $\mathbf{v}\in\mathcal{C}(\mathbf{A}^{\mathrm{T}})$.
>
> ❷ $\mathbf{w}\in\mathrm{N}(\mathbf{A}^{\mathrm{T}})$ if and only if $\mathbf{w}\perp\mathbf{v}$ for every $\mathbf{v}\in\mathcal{C}(\mathbf{A})$.
>
> ❸ $\mathbf{u}\in\mathcal{C}(\mathbf{A}^{\mathrm{T}})$ if and only if $\mathbf{u}\perp\mathbf{v}$ for every $\mathbf{v}\in\mathrm{N}(\mathbf{A})$.
>
> ❹ $\mathbf{w}\in\mathcal{C}(\mathbf{A})$ if and only if $\mathbf{w}\perp\mathbf{v}$ for every $\mathbf{v}\in\mathrm{N}(\mathbf{A}^{\mathrm{T}})$.

Proof. Clearly, ❷ is the same statement as ❶ but applied to the matrix $\mathbf{A}^{\mathrm{T}}$, and similarly for ❹ versus ❸. Now $\mathbf{v}\in\mathcal{C}(\mathbf{A}^{\mathrm{T}})$ if and only if $\mathbf{A}^{\mathrm{T}}\mathbf{y}=\mathbf{v}$ for some $\mathbf{y}\in\mathbb{R}^m$. Let us consider $\mathbf{A}^{\mathrm{T}}\mathbf{y}\cdot\mathbf{u}=(\mathbf{A}^{\mathrm{T}}\mathbf{y})^{\mathrm{T}}\mathbf{u}=\mathbf{y}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}^{\mathrm{T}}}\mathbf{u}=\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{u}$. Clearly if $\mathbf{A}\mathbf{u}=\mathbf{0}$, then $\mathbf{A}^{\mathrm{T}}\mathbf{y}\cdot\mathbf{u}=0$. Conversely, $\mathbf{A}\mathbf{u}\neq\mathbf{0}$, let $\mathbf{y}=\mathbf{A}\mathbf{u}$, then $\mathbf{A}^{\mathrm{T}}\mathbf{y}\cdot\mathbf{u}=\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{u}=\mathbf{A}\mathbf{u}\cdot\mathbf{A}\mathbf{u}\neq 0$, and so $\mathbf{u}\not\perp\mathbf{v}$ for $\mathbf{v}=\mathbf{A}^{\mathrm{T}}\mathbf{A}\mathbf{u}$ and $\mathbf{v}\in\mathcal{C}(\mathbf{A}^{\mathrm{T}})$. So ❶ (and hence ❷) has been proven. Switching perspectives, $\mathbf{v}\in\mathrm{N}(\mathbf{A})$ if and only if $\mathbf{A}\mathbf{v}=\mathbf{0}$, so if $\mathbf{u}\in\mathcal{C}(\mathbf{A}^{\mathrm{T}})$, then $\mathbf{u}=\mathbf{A}^{\mathrm{T}}\mathbf{y}$, and so

$$\mathbf{u}\cdot\mathbf{v}=(\mathbf{A}^{\mathrm{T}}\mathbf{y})\cdot\mathbf{v}=\mathbf{y}^{\mathrm{T}}\mathbf{A}\mathbf{v}=\mathbf{y}^{\mathrm{T}}\mathbf{0}=0.$$

Conversely, suppose $\mathbf{u}\notin\mathcal{C}(\mathbf{A}^{\mathrm{T}})$. Then we know that $r\begin{pmatrix}\mathbf{A}^{\mathrm{T}} & \mathbf{u}\end{pmatrix}=r(\mathbf{A}^{\mathrm{T}})+1$, in other words, there is a pivot in the last column the reduced form of $\begin{pmatrix}\mathbf{A}^{\mathrm{T}} & \mathbf{u}\end{pmatrix}$. Let $\mathbf{P}$ be the reducing matrix for $\begin{pmatrix}\mathbf{A}^{\mathrm{T}} & \mathbf{u}\end{pmatrix}$. Thus, without loss, we can assume that the last row of $\mathbf{P}\mathbf{A}^{\mathrm{T}}$ is all zeroes while the last row of $\mathbf{P}\mathbf{u}=1$. So if we let $\mathbf{y}=\begin{pmatrix}0 & \cdots & 0 & 1\end{pmatrix}$, then $\mathbf{y}\mathbf{P}\mathbf{A}^{\mathrm{T}}=\mathbf{0}$ but $\mathbf{y}\mathbf{P}\mathbf{u}=1$. Let then $\mathbf{v}=\mathbf{P}^{\mathrm{T}}\mathbf{y}^{\mathrm{T}}$, then $\mathbf{v}\in\mathrm{N}(\mathbf{A})$ and $\mathbf{v}\cdot\mathbf{u}=1$, so we are done. ⌘

Example 11. Let $\mathbf{A}=\begin{pmatrix}1&3&2&4&1\\2&6&1&5&-4\\3&9&3&9&-3\\4&12&4&12&-4\end{pmatrix}$. It reduces to $\begin{pmatrix}1&3&0&2&-3\\0&0&1&1&2\\0&0&0&0&0\\0&0&0&0&0\end{pmatrix}$ as we saw before. Thus, a transparent set for $\boldsymbol{C}\left(\mathbf{A}^{\mathrm{T}}\right)$ consists of $\begin{pmatrix}1\\3\\0\\2\\-3\end{pmatrix}$ and $\begin{pmatrix}0\\0\\1\\1\\2\end{pmatrix}$. We saw before that $\begin{pmatrix}-3\\1\\0\\0\\0\end{pmatrix}$, $\begin{pmatrix}-2\\0\\-1\\1\\0\end{pmatrix}$ and $\begin{pmatrix}3\\0\\-2\\0\\1\end{pmatrix}$ is a transparent spanning set for $\mathbf{N}(\mathbf{A})$. We readily observe that any vector of the first set is perpendicular to any vector of the second set.

Similarly the transpose reduces to $\begin{pmatrix}1&0&1&\frac{4}{3}\\0&1&1&\frac{4}{3}\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$. Thus a transparent spanning set for $\boldsymbol{C}(\mathbf{A})$ is $\begin{pmatrix}1\\0\\1\\\frac{4}{3}\end{pmatrix}$ and $\begin{pmatrix}0\\1\\1\\\frac{4}{3}\end{pmatrix}$ while a transparent set for the null space is given by $\begin{pmatrix}-1\\-1\\1\\0\end{pmatrix}$ and $\begin{pmatrix}\frac{-4}{3}\\\frac{-4}{3}\\0\\1\end{pmatrix}$, and we can just as readily observe the orthogonality.

When two subspaces V and W are related as the ones in the previous theorems, namely the vectors in one of them are exactly the vectors perpendicular to each vector of the other, they are known as **orthogonal complements**. One can indicate this by $V^{\perp}=W$ and $W^{\perp}=V$.

Thus with any $m\times n$ matrix $\mathbf{A}$ we have two pairs of orthogonal complement subspaces, one pair, $\boldsymbol{C}(\mathbf{A})$ and $\mathbf{N}\left(\mathbf{A}^{\mathrm{T}}\right)$ in $\mathbb{R}^m$ and $\boldsymbol{C}\left(\mathbf{A}^{\mathrm{T}}\right)$ and $\mathbf{N}(\mathbf{A})$ in $\mathbb{R}^n$. Since the columns of $\mathbf{A}^{\mathrm{T}}$ are the rows of $\mathbf{A}$, one also refers to $\boldsymbol{C}\left(\mathbf{A}^{\mathrm{T}}\right)$ as the **row space** of $\mathbf{A}$, and is denoted by $\mathbf{R}(\mathbf{A})$. Then the orthogonality of $\mathbf{R}(\mathbf{A})$ and $\mathbf{N}(\mathbf{A})$ is clear—every row is necessarily orthogonal to anything in the null space by simple matrix multiplication.

Also since every vector $\mathbf{N}\left(\mathbf{A}^{\mathrm{T}}\right)$ satisfies (by transposing), $\mathbf{y}^{\mathrm{T}}\mathbf{A}=\mathbf{0}$, we can also refer to it as the **left null space** of $\mathbf{A}$, and it can be denoted by $\mathbf{L}(\mathbf{A})$.

Thus we have

$$\mathcal{C}(\mathbf{A})^{\perp} = \mathbf{L}(\mathbf{A}) \text{ and } \mathbf{L}(\mathbf{A})^{\perp} = \mathcal{C}(\mathbf{A}),$$

and

$$\mathbf{N}(\mathbf{A})^{\perp} = \mathbf{R}(\mathbf{A}) \text{ and } \mathbf{R}(\mathbf{A})^{\perp} = \mathbf{N}(\mathbf{A}).$$

We will further clarify and fine-tune these ideas in the next section.

❶❶ The Notion of Dimension

In this section, we discuss one of the fundamental parameters of a vector space, the notion of **dimension**.

Recall that a collection of vectors V (of any given fixed size) is a **vector space** (or **subspace**, for most of our purposes) if the following three requirements are met:

① $\mathbf{0}$ is in V;
② if $\mathbf{u}$ and $\mathbf{v}$ are in V, then so is $\mathbf{u}+\mathbf{v}$ (closure under addition);
③ if $\mathbf{u}$ is in V, then so is $a\mathbf{u}$ where a is an arbitrary scalar (closure under scalar multiplication).

We have already associated four subspaces with any given matrix.

However, since every matrix can be thought of as a very tall vector (by stacking its columns vertically), we can also discuss vector spaces of matrices. We look at several examples of these at present.

Example 1. The Space of Symmetric Matrices. Consider the set V of all symmetric matrices of size n. Thus an $n\times n$ matrix $\mathbf{A}$ is in V if and only if $\mathbf{A}^{\mathrm{T}}=\mathbf{A}$. Certainly $\mathbf{0}^{\mathrm{T}}=\mathbf{0}$ is symmetric. Also by the transpose of a sum is the sum of the transposes, so we get the sum of two symmetric matrices is symmetric, $(\mathbf{A}+\mathbf{B})^{\mathrm{T}}=\mathbf{A}^{\mathrm{T}}+\mathbf{B}^{\mathrm{T}}=\mathbf{A}+\mathbf{B}$. Similarly, a scalar multiple of a symmetric matrix is also symmetric: $(a\mathbf{A})^{\mathrm{T}}=a\mathbf{A}^{\mathrm{T}}=a\mathbf{A}$, and so we can consider the set of symmetric matrices of size n as a subspace of the space of all square matrices of size n.

Example 2. The Space of Skew-Symmetric Matrices. A square matrix $\mathbf{A}$ is called **skew-symmetric** if it satisfies $\mathbf{A}^{\mathrm{T}}=-\mathbf{A}$. For example, $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ is such a matrix. Easily, if we let W be the set of all skew-symmetric matrices of size n, then $\mathbf{0}\in W$, and if $\mathbf{A},\mathbf{B}\in W$, then $(\mathbf{A}+\mathbf{B})^{\mathrm{T}}=\mathbf{A}^{\mathrm{T}}+\mathbf{B}^{\mathrm{T}}=-\mathbf{A}+-\mathbf{B}=-(\mathbf{A}+\mathbf{B})$, and easily $(a\mathbf{A})^{\mathrm{T}}=-a\mathbf{A}$. So we have another vector space of matrices.

The following is more unusual:
Example 3. The Powers of a Matrix. Let $\mathbf{A}$ be an $n\times n$ matrix. Consider the span of its powers starting with $\mathbf{I}=\mathbf{A}^0$, namely consider the vector space $\langle\mathbf{A}\rangle=[\mathbf{I},\mathbf{A},\mathbf{A}^2,\mathbf{A}^3,\ldots]$. Clearly, an $n\times n$ matrix $\mathbf{B}$ is in $\langle\mathbf{A}\rangle$ exactly when there exists a polynomial $p(x)$ such that $p(\mathbf{A})=\mathbf{B}$. Note that the set $\langle\mathbf{A}\rangle$ is not only closed under addition and scalar multiplication, but also multiplication, since $p(\mathbf{A})q(\mathbf{A})=r(\mathbf{A})$ where $r(x)=p(x)q(x)$.

Specific examples, $\langle \mathbf{I} \rangle = [\mathbf{I}] = \{a\mathbf{I} \mid a \in \mathbb{R}\}$, and $\langle \mathbf{J} \rangle = [\mathbf{I}, \mathbf{J}] = \{a\mathbf{I} + b\mathbf{J} \mid a, b \in \mathbb{R}\}$ since $\mathbf{J}_n^2 = n\mathbf{J}_n$.

As it turns out with every vector space V one can associate a positive integer called the **dimension** of V, and denoted by $\dim V$. We proceed next on how to find the dimension of any vector space.

Let us start with a previous example. Consider the matrix $\mathbf{A} = \begin{pmatrix} 1 & 3 & 2 & 4 & 1 \\ 2 & 6 & 1 & 5 & -4 \\ 3 & 9 & 3 & 9 & -3 \\ 4 & 12 & 4 & 12 & -4 \end{pmatrix}$. We know of course that its five columns form a spanning set for $\mathcal{C}(\mathbf{A})$, but at the same time there could be fewer columns that span that column space, or on the other hand we could add more columns and still have the same column space. In brief, **there is no constancy in the number of vectors in a spanning set for a vector space**.

However since we know $\mathbf{A}$ reduces to $\begin{pmatrix} 1 & 3 & 0 & 2 & -3 \\ 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, we know that first and the third column form of $\mathbf{A}$, $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ 1 \\ 3 \\ 4 \end{pmatrix}$ constitute a spanning set for $\mathcal{C}(\mathbf{A})$ which is minimal, in the sense that one can not delete one of the two vectors and span the column space. At the same time we saw before that $\begin{pmatrix} 1 \\ 0 \\ 1 \\ \frac{4}{3} \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \\ 1 \\ \frac{4}{3} \end{pmatrix}$ was a transparent spanning set for $\mathcal{C}(\mathbf{A})$. Clearly, a transparent set is also minimal since one cannot get a column of the identity from the other columns—**one cannot get 1 from 0's**. The key observation is that then both of these collections have the same number of vectors in them, in this case 2 vectors. Thus one says the dimension of $\mathcal{C}(\mathbf{A})$ is 2. Note the agreement with the geometric language as we referred to this column space as a plane before.

So the critical idea is that of spanning sets that are **minimal**, and the notion of **linear independence** is helpful. The basic facts about linear independence is captured in the following:

> **Theorem (Linear Independence).** Let $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_n$ be vectors of size m, and let $\mathbf{A} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_t \end{pmatrix}$. Then the following are equivalent:

	Statement about the Vectors	Statement about the Matrix
①	$\mathbf{u}_1 \neq \mathbf{0}$ and for each $i = 2,\ldots,n$, $\mathbf{u}_i \notin [\mathbf{u}_1,\ldots,\mathbf{u}_{i-1}]$.	Every column of **A** is pivotal.
②	There exists an invertible matrix **P** such that $\mathbf{Pu}_1$, $\mathbf{Pu}_2,\ldots,\mathbf{Pu}_n$ is transparent.	**A** is of full column rank, $r(\mathbf{A}) = n$
③	Whenever $a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n = \mathbf{0}$, we must have $a_1 = a_2 = \cdots = a_n = 0$.	If $\mathbf{Au} = \mathbf{0}$, then $\mathbf{u} = \mathbf{0}$, *i.e.*, $\mathrm{N}(\mathbf{A}) = \mathbf{0}$.
④	For any scalars, if $a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n = b_1\mathbf{u}_1 + b_2\mathbf{u}_2 + \cdots + b_n\mathbf{u}_n$, we must have $a_1 = b_1$, $a_2 = b_2$, …, $a_n = b_n$.	If $\mathbf{Au} = \mathbf{Av}$, then $\mathbf{u} = \mathbf{v}$
⑤	There exists an invertible matrix **P** whose first n columns are $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_n$.	There exists a matrix **B** such that $(\mathbf{A} \quad \mathbf{B})$ is invertible

Proof. Since the two statements in each row are basically just restatements of each other, the equivalence across each row should be clear. The equivalence of ① and ② is clear from the matrix point of view, and so is the equivalence of ② and ③. Assume ③ and let $\mathbf{Au} = \mathbf{Av}$. But then $\mathbf{A}(\mathbf{u} - \mathbf{v}) = \mathbf{0}$, and so $\mathbf{u} - \mathbf{v} = \mathbf{0}$, and ④ follows. Conversely if ④ holds and $\mathbf{Au} = \mathbf{0} = \mathbf{A0}$, so $\mathbf{u} = \mathbf{0}$, and ③ is done. Easily if ⑤ holds, then every column in $(\mathbf{A} \quad \mathbf{B})$ is pivotal, so every column in **A** is also. Conversely assume ②, then we may assume $\mathbf{PA} = \begin{pmatrix} \mathbf{I}_n \\ \mathbf{0} \end{pmatrix}$, so $\mathbf{P}^{-1}$ is an invertible matrix whose first n columns are **A**. ⌘

Let $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_n$ be vectors of size m satisfying the conditions of the theorem. Then they are called **linearly independent**. Note that always $n \leq m$ if this is the case.

It is logically consistent to refer to the empty collection of vectors as linearly independent. Note that if $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_n$ are linearly independent, then

none of them is in the span of the others,

and although this seems stronger than ①, it is logically equivalent to it.

We exemplify ⑤.

Example 4. Consider the following 3 elements of $\mathbb{R}^5$: $\mathbf{w} = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 3 \\ 1 \end{pmatrix}$, $\mathbf{v} = \begin{pmatrix} -4 \\ 5 \\ 5 \\ -2 \\ 5 \end{pmatrix}$ and $\mathbf{u} = \begin{pmatrix} 1 \\ 2 \\ 2 \\ 2 \\ 2 \end{pmatrix}$.

Then in order to find the reducing matrix $\mathbf{P}$, we reduce $\begin{pmatrix} 2 & -4 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 5 & 2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 5 & 2 & 0 & 0 & 1 & 0 & 0 \\ 3 & -2 & 2 & 0 & 0 & 0 & 1 & 0 \\ 1 & 5 & 2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, and obtain $\mathbf{P} = \begin{pmatrix} -2.8 & 0 & 0 & 2.6 & -1.2 \\ -0.8 & 0 & 0 & 0.6 & -0.2 \\ 3.4 & 0 & 0 & -2.8 & 1.6 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$. Thus $\mathbf{P}\begin{pmatrix} \mathbf{w} & \mathbf{v} & \mathbf{u} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_3 \\ \mathbf{0} \end{pmatrix}$, and so $\mathbf{P}^{-1}$ is the desired matrix. Indeed $\mathbf{P}^{-1} = \begin{pmatrix} 2 & -4 & 1 & 0 & 0 \\ 1 & 5 & 2 & 1 & 0 \\ 1 & 5 & 2 & 0 & 1 \\ 3 & -2 & 2 & 0 & 0 \\ 1 & 5 & 2 & 0 & 0 \end{pmatrix}$.

And we are ready for a fundamental concept. Let V be a vector space. A linearly independent spanning subset of V is called a **basis**. The main fact about bases is contained in the fundamental theorem whose proof can be found in the **Appendix of Proofs**.

> **Theorem** (**Basis**). Let V be a vector space. Then V has a basis. Furthermore, any two bases of V have the same number of elements.

The size of any basis for V then is a well-defined number and is known as the **dimension** of V and is denoted by $\dim V$. As an important and useful corollary to the theorem we obtain:

> **Corollary** (**Dimension**). Let V be a vector space with a nonzero vector. Let $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ be elements of V. Then the following are true:
>
> ❶ $\dim V$ is a positive integer.
>
> ❷ Any basis of V has $\dim V$ elements.
>
> ❸ If $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ is a linearly independent subset of V, then $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ can be extended to a basis of V. Hence $t \le \dim V$ and if $t = \dim V$, then $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ is a basis.
>
> ❹ If $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ is a spanning set for V, then $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ can be reduced to a basis of V. Hence $t \ge \dim V$ and if $t = \dim V$, then $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ is a basis.
>
> ❺ If W is a subspace of V, then $\dim W \le \dim V$, and if $\dim W = \dim V$, then $W = V$.

Proof. Both ❶ and ❷ are trivial consequences of the theorem. For ❸, let $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ be a linearly independent subset of *V* and let $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_n$ be a basis for *V*. Moreover, let *W* be the span of $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$. If each **v** is in *W*, then $W = V$, and $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ is also a spanning set, and we are done. If it is not the case that each **v** is in *W*, then let $\mathbf{u}_{t+1} = \mathbf{v}_i$, where $\mathbf{v}_i$ is the first **v** that is not in *W*. Then the set $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$, $\mathbf{u}_{t+1}$ is still linearly independent, and their span contains one more **v** than before. If all the **v**'s are contained in the span of $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$, $\mathbf{u}_{t+1}$, then we are done again. If not repeat the process we just went through, and eventually we will have a basis for *V* containing the set $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$. For the last claim of ❸, note that the only way we do not get a $\mathbf{u}_{t+1}$ is for the **u**'s to be a spanning set already, namely a basis. On to ❹, let $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ be a spanning set for *V*. If they are linearly independent, we are done. If not, let $\mathbf{u}_i$ be the first **u** such that $\mathbf{u}_i \in [\mathbf{u}_1, \ldots, \mathbf{u}_{i-1}]$, and drop it from the collection. Now we still have a spanning set , but with fewer elements. If the smaller collection is linearly independent, we are done. If not repeat the process. Eventually, we will arrive at a spanning set that is also linearly independent—namely a basis. The last remark of ❹ follows easily, and ❺ is a trivial consequence of ❸. ⌘

Example 5. Consider the space of all vectors of size *m*, $\mathbb{R}^m$, then the columns of the identity are referred to as the **standard basis** for $\mathbb{R}^m$. Clearly it has *m* elements, so the dimension of $\mathbb{R}^m$ is *m*, $\dim \mathbb{R}^m = m$. One usually denotes these vectors by ξ_1, $\xi_2, \ldots$.

Similarly, if we consider the space of all $m \times n$ matrices, then the members of its standard basis are usually denoted by $\mathbf{E}_{ij}$, which is the matrix with 0's everywhere except in the $i, j-$position, where there is a 1. For example $m = 3$, $n = 4$, then $\mathbf{E}_{23} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.
Therefore, the dimension is mn. This is not surprising since one can always think of an $m \times n$ matrix as a tall mn vector.

Example 6. Consider the vectors in $\mathbb{R}^3$ that are perpendicular to the vector $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$. This is tantamount to the solutions of $a + b + c = 0$. Then easily $\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$ constitute a basis, so the dimension of this space is 2.

Now we revisit some of the examples ate the beginning of this section:

Example 7. Symmetric Matrices. We saw before that the collection of symmetric matrices of size n is a subspace of the space of all square matrices of size n, which has dimension n^2. What is the dimension then of the space of symmetric matrices? Let us consider the 2×2 symmetric matrices—it is easy to check $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ and $\begin{pmatrix}0&0\\0&1\end{pmatrix}$ form a basis, so it is 3-dimensional. For the case $n=3$, an arbitrary symmetric case is $\begin{pmatrix}a&b&c\\b&d&e\\c&e&f\end{pmatrix}$, so we can see that a basis will consist of 6 elements: $\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$, $\begin{pmatrix}0&1&0\\1&0&0\\0&0&0\end{pmatrix}$, $\begin{pmatrix}0&0&1\\0&0&0\\1&0&0\end{pmatrix}$, $\begin{pmatrix}0&0&0\\0&1&0\\0&0&0\end{pmatrix}$, $\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix}$ and $\begin{pmatrix}0&0&0\\0&0&0\\0&0&1\end{pmatrix}$. For arbitrary n, the dimension is $\dfrac{n(n+1)}{2}$.

The following is even more unusual:
Example 8. The Powers of a Matrix. We saw before that if $\mathbf{A}$ is an $n\times n$ matrix, then the span of its powers starting with $\mathbf{I}=\mathbf{A}^0$, $\langle\mathbf{A}\rangle=\left[\mathbf{I},\mathbf{A},\mathbf{A}^2,\mathbf{A}^3,\ldots\right]$ is a vector space. What is the dimension of this vector space? Certainly we know it is at most n^2 since that is the dimension of the space of all $n\times n$ matrices. Actually, we will see below that it is at most n, but in many cases is much lower than that. We look at several examples.

First, $\langle\mathbf{I}\rangle=[\mathbf{I}]$, which is clearly of dimension 1. Second, $\langle\mathbf{J}_n\rangle=[\mathbf{I},\mathbf{J}_n]$ since $\mathbf{J}_n^2=n\mathbf{J}_n$, so it is of dimension 2.

Let $\mathbf{C}=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$. Then $\mathbf{C}^2=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$, and $\mathbf{C}^3=\mathbf{I}$, so $\langle\mathbf{C}\rangle=\left[\mathbf{I},\mathbf{C},\mathbf{C}^2\right]$, of dimension 3.

Let now $\mathbf{A}=\begin{pmatrix}\mathbf{0}&\mathbf{J}_{10}\\\mathbf{J}_{10}&\mathbf{0}\end{pmatrix}$. Then $\mathbf{A}^2=\begin{pmatrix}10\mathbf{J}_{10}&\mathbf{0}\\\mathbf{0}&10\mathbf{J}_{10}\end{pmatrix}$ and $\mathbf{A}^3=100\mathbf{A}$, so $\mathbf{A}^3\in\left[\mathbf{I},\mathbf{A},\mathbf{A}^2\right]$, and thus, $\mathbf{A}^4\in\left[\mathbf{I},\mathbf{A},\mathbf{A}^2,\mathbf{A}^3\right]=\left[\mathbf{I},\mathbf{A},\mathbf{A}^2\right]$, and so on, so the dimension of $\langle\mathbf{A}\rangle=3$ in this case.

Before we enter the main topic of the dimensions of the spaces of a matrix, we do one more matrix example.

Example 9. Consider all 3×3 $\mathbf{A}$'s that commute with $\mathbf{J}_3$, namely, all $\mathbf{A}$'s such that $\mathbf{AJ}_3=\mathbf{J}_3\mathbf{A}$. It is easy to show that this a subspace of the space of all 3×3 matrices, which as we saw has dimension 9. If $\mathbf{A}=\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}$ is such a matrix, then

$$\mathbf{AJ}_3=\begin{pmatrix} a+b+c & a+b+c & a+b+c \\ d+e+f & d+e+f & d+e+f \\ g+h+i & g+h+i & g+h+i \end{pmatrix}$$

while $\mathbf{J}_3\mathbf{A}=\begin{pmatrix} a+d+g & b+e+h & c+f+i \\ a+d+g & b+e+h & c+f+i \\ a+d+g & b+e+h & c+f+i \end{pmatrix}$, therefore we have equality exactly when

$$a+b+c=d+e+f=g+h+i=a+d+g=b+e+h=c+f+i\,.$$

So the row sums and column sums are all equal. But then if we solve this system by using the free variables *a*, *b*, *d*, *e* and *r* (where *r* denotes an arbitrary row or column sum), we get $\mathbf{A}=\begin{pmatrix} a & b & r-a-b \\ d & e & r-d-e \\ r-a-d & r-b-e & a+b+d+e-r \end{pmatrix}$, so a basis for this space is given by

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 0 \\ -1 & 0 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & -1 \end{pmatrix}.$$

And we have the dimension of this space is 5. Note that the first four matrices constitute a basis for the space of matrices that satisfy $\mathbf{AJ}_3=\mathbf{J}_3\mathbf{A}=\mathbf{0}$.

As aforementioned for the remainder of this section we consider an $m\times n$ matrix $\mathbf{A}$ and the four spaces associated with it: $\mathcal{C}(\mathbf{A})$, $\mathrm{N}(\mathbf{A})$, $\mathcal{R}(\mathbf{A})$ and $\mathrm{L}(\mathbf{A})$, and pursue their dimensions. We need to understand how these spaces are related to the reduced form of $\mathbf{A}$, and the following begins to address this issue.

Theorem (Row and Null Spaces). Let $\mathbf{A}$ be $m\times n$, and let $\mathbf{M}$ be its reduced form. Then the nonzero rows of $\mathbf{M}$ form a transparent basis for $\mathcal{R}(\mathbf{A})$. Thus, $\mathcal{R}(\mathbf{A})=\mathcal{R}(\mathbf{M})$ is of dimension $r(\mathbf{A})$. Naturally, $\mathrm{N}(\mathbf{A})=\mathrm{N}(\mathbf{M})$, and a transparent basis is obtained by solving the system $\mathbf{Mx}=\mathbf{0}$. Thus, $\dim\mathrm{N}(\mathbf{A})=n-r(\mathbf{A})$.

Proof. It suffices to show that if $\mathbf{P}$ is an invertible matrix, then $\mathcal{R}(\mathbf{PA})=\mathcal{R}(\mathbf{A})$ and $\mathrm{N}(\mathbf{PA})=\mathrm{N}(\mathbf{A})$. But since the relation is symmetric, $\mathbf{P}^{-1}(\mathbf{PA})=\mathbf{A}$, it suffices to show containment of one side into the other. For a vector to be in the row space of $\mathbf{A}$, it needs to be a liner combination of its rows, or equivalently it needs to be a linear combination of the columns of $\mathbf{A}^{\mathrm{T}}$, that is of the form $\mathbf{A}^{\mathrm{T}}\mathbf{y}$. But

$$\mathbf{A}^{\mathrm{T}}\mathbf{y}=\mathbf{A}^{\mathrm{T}}\mathbf{P}^{\mathrm{T}}\left(\mathbf{P}^{\mathrm{T}}\right)^{-1}\mathbf{y}=(\mathbf{PA})^{\mathrm{T}}\left(\left(\mathbf{P}^{\mathrm{T}}\right)^{-1}\mathbf{y}\right)=(\mathbf{PA})^{\mathrm{T}}\mathbf{w}\,,$$

so $\mathbf{A}^{\mathrm{T}}\mathbf{y}\in\mathcal{R}(\mathbf{PA})$, and thus by the symmetry, $\mathcal{R}(\mathbf{PA})=\mathcal{R}(\mathbf{A})$. Let $\mathbf{u}\in\mathrm{N}(\mathbf{A})$. Then $\mathbf{Au}=\mathbf{0}$. So $\mathbf{PAu}=\mathbf{P0}=\mathbf{0}$, so $\mathbf{u}\in\mathrm{N}(\mathbf{PA})$. Astute readers may recognize this as a restatement that **two row equivalent systems have the same solutions**. Once we have established that $\mathsf{R}(\mathbf{PA}) = \mathsf{R}(\mathbf{A})$ and $\mathsf{N}(\mathbf{PA}) = \mathsf{N}(\mathbf{A})$, then since we know there is an invertible matrix $\mathbf{P}$ such that $\mathbf{PA} = \mathbf{M}$, we have that $\mathsf{R}(\mathbf{A}) = \mathsf{R}(\mathbf{M})$ and $\mathsf{N}(\mathbf{A}) = \mathsf{N}(\mathbf{M})$. The rest of the claims are obvious from these: the nonzero rows of $\mathbf{M}$ are clearly transparent by the reduced form and since all the others are $\mathbf{0}$, they form a transparent basis for $\mathsf{N}(\mathbf{M})$. We have already observed the claims about the null space. ⌘

The dimension of the null space of **A** is called the **nullity** of **A**.

Example 10. Let $\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 2 & 6 & 4 & 2 \\ 2 & 5 & 3 & 1 \end{pmatrix}$ which has reduced form $\mathbf{M} = \begin{pmatrix} 1 & 0 & -1 & -2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Then we can see every row of **A** is in the span of the two vectors $\mathbf{u}_1^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & -1 & -2 \end{pmatrix}$ and $\mathbf{u}_2^{\mathrm{T}} = \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix}$. In fact, because of their transparency, every row is easily written as a linear combination of them: $\begin{pmatrix} 1 & 1 & 0 & -1 \end{pmatrix} = \mathbf{u}_1^{\mathrm{T}} + \mathbf{u}_2^{\mathrm{T}}$, $\begin{pmatrix} 2 & 6 & 4 & 2 \end{pmatrix} = 2\mathbf{u}_1^{\mathrm{T}} + 6\mathbf{u}_2^{\mathrm{T}}$, and $\begin{pmatrix} 2 & 5 & 3 & 1 \end{pmatrix} = 2\mathbf{u}_1^{\mathrm{T}} + 5\mathbf{u}_2^{\mathrm{T}}$. Also we can observe that the two null spaces are the same, but it is much easier to tell the null space of **M** than that of **A.** Of course since we are solving the homogeneous system $\mathbf{Ax} = \mathbf{0}$, this last remark is obvious—**reducing is the way to solve systems**. Namely when does a vector $\mathbf{x} = \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$ belong to $\mathsf{N}(\mathbf{M})$, when $x = z + 2w$ and $y = -z - w$, that is when $\mathbf{x} = \begin{pmatrix} z+2w \\ -z-w \\ z \\ w \end{pmatrix}$, which means $\mathbf{x} = z\begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix} + w\begin{pmatrix} 2 \\ -1 \\ 0 \\ 1 \end{pmatrix}$, so we have that the two vectors $\begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ -1 \\ 0 \\ 1 \end{pmatrix}$ span $\mathsf{N}(\mathbf{M})$, and hence $\mathsf{N}(\mathbf{A})$. Note that $\dim \mathsf{R}(\mathbf{A}) = 2 = r(\mathbf{A})$ and also its nullity is 2. Note that $2+2=4$, the number of columns of **A**. Observe also the mutual orthogonality of the two spaces.

However, as the following very simple example illustrates, **the column space of a matrix does change as one reduces it**.

Example 11. Let $\mathbf{A} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then it is clear that its column space is $\mathcal{C}(\mathbf{A}) = \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right]$, which is also known as the *y*-axis in more familiar terms. Its null space is $\mathsf{N}(\mathbf{A}) = \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right]$, the *y*-

axis also. Finally, its row space is the x-axis, $\mathbf{R}(\mathbf{A}) = \left[\begin{pmatrix}1\\0\end{pmatrix}\right]$, which is spanned by the second row of **A** since the first row is all 0's. Note as observed before, anything in the null space is perpendicular to anything in the row space.

What is the reduced form of **A**? Trivially, it is $\mathbf{M} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$. Note that of course, the row space is still the x-axis, but now the row is the first row, so we could not go back to the first row of the original matrix because that would gives us just the zero vector. The null space has of course not changed either. But look at the column space now—it is the x-axis, not the y-axis, it has changed.

> **Theorem (Column and Left Null Spaces).** Let $\mathbf{A}$ be $m \times n$, and let **M** be its reduced form. Then the columns of **A** that occupy the pivotal positions in **M** form a basis for $\mathbf{C}(\mathbf{A})$. Thus, $\dim \mathbf{C}(\mathbf{A}) = r(\mathbf{A})$. Equivalently, the nonzero rows of the reduced form of $\mathbf{A}^{\mathrm{T}}$ form a transparent basis for $\mathbf{C}(\mathbf{A})$. The dimension of $\mathbf{L}(\mathbf{A})$, the left null space, is $m - r(\mathbf{A})$.

Proof. By the **Nonpivotal Column Lemma**, we know the relations between the columns of **A** are exactly the same as the relations between the columns of **M**. In the reduced matrix, it is clear that the pivotal columns form a transparent basis, so the pivotal columns of **A** must also be a basis (although it is not transparent). But we also know that the nonzero rows of the reduced form of $\mathbf{A}^{\mathrm{T}}$ form a transparent basis for $\mathbf{R}(\mathbf{A}^{\mathrm{T}})$, which is the same as $\mathbf{C}(\mathbf{A})$. Since $\mathbf{L}(\mathbf{A})$ is the same as $\mathbf{N}(\mathbf{A}^{\mathrm{T}})$, the last remark follows from the previous theorem. ⌘

Example 12. As before $\mathbf{A} = \begin{pmatrix}1 & 1 & 0 & -1\\2 & 6 & 4 & 2\\2 & 5 & 3 & 1\end{pmatrix}$ and $\mathbf{M} = \begin{pmatrix}1 & 0 & -1 & -2\\0 & 1 & 1 & 1\\0 & 0 & 0 & 0\end{pmatrix}$. So we know that the first two columns of **A**, $\begin{pmatrix}1\\2\\2\end{pmatrix}$ and $\begin{pmatrix}1\\6\\5\end{pmatrix}$ form a basis for $\mathbf{C}(\mathbf{A})$ since these columns are in the pivotal positions of **M**. And just like in the **Nonpivotal Column Lemma**, since the third column of $\mathbf{M} = \begin{pmatrix}1 & 0 & -1 & -2\\0 & 1 & 1 & 1\\0 & 0 & 0 & 0\end{pmatrix}$ equals the second column minus the first columns, the same is true of $\mathbf{A} = \begin{pmatrix}1 & 1 & 0 & -1\\2 & 6 & 4 & 2\\2 & 5 & 3 & 1\end{pmatrix}$. Similarly, the fourth column of **M** is the second minus twice the first, so the same is true in **A**. But in another approach, consider

$\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 6 & 5 \\ 0 & 4 & 3 \\ -1 & 2 & 1 \end{pmatrix}$ and its reduced form $\begin{pmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & \frac{3}{4} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. So $\mathbf{w}_1 = \begin{pmatrix} 1 \\ 0 \\ \frac{1}{2} \end{pmatrix}$ and $\mathbf{w}_2 = \begin{pmatrix} 0 \\ 1 \\ \frac{3}{4} \end{pmatrix}$ form a transparent basis for $\mathcal{C}(\mathbf{A})$. Indeed, $\begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} = \mathbf{w}_1 + 2\mathbf{w}_2$, $\begin{pmatrix} 1 \\ 6 \\ 5 \end{pmatrix} = \mathbf{w}_1 + 6\mathbf{w}_2$, $\begin{pmatrix} 0 \\ 4 \\ 3 \end{pmatrix} = 4\mathbf{w}_2$ and $\begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} = -\mathbf{w}_1 + 2\mathbf{w}_2$. Finally, we have $\dim \mathcal{C}(\mathbf{A}) = 2 = r(\mathbf{A})$. On the other hand, the left nullity of $\mathbf{A}$ is 1 with $\begin{pmatrix} \frac{-1}{2} \\ \frac{-3}{4} \\ 1 \end{pmatrix}$ being a basis for $\mathbf{L}(\mathbf{A})$. Note that just as easily we could have taken $\begin{pmatrix} 2 \\ 3 \\ -4 \end{pmatrix}$ as the basis. Note $2+1=3$, the number of rows of $\mathbf{A}$, and as observed before everything in $\mathbf{L}(\mathbf{A})$ is orthogonal to everything in $\mathcal{C}(\mathbf{A})$

We arrive at a very interesting and unexpected fact already exemplified above

Corollary (Rank of Transpose). Let $\mathbf{A}$ be $m \times n$. Then $r(\mathbf{A}) = r(\mathbf{A}^{\mathrm{T}})$.

Proof. It is easy since $r(\mathbf{A}) = \dim \mathcal{C}(\mathbf{A}) = \dim \mathbf{R}(\mathbf{A}^{\mathrm{T}}) = r(\mathbf{A}^{\mathrm{T}})$. ⌘

Corollary. (Rank of a Product). Let $\mathbf{A}$ be $m \times n$ and $\mathbf{B}$ be $n \times p$. Then

$$r(\mathbf{AB}) \le r(\mathbf{A}) \text{ and } r(\mathbf{AB}) \le r(\mathbf{B}).$$

Proof. Since $(\mathbf{AB})\mathbf{u} = \mathbf{A}(\mathbf{Bu})$, we have that $\mathcal{C}(\mathbf{AB})$ is contained in $\mathcal{C}(\mathbf{A})$, and therefore it has smaller dimension. Thus, $r(\mathbf{AB}) \le r(\mathbf{A})$. To prove the other inequality, we have that $r(\mathbf{AB}) = r\left((\mathbf{AB})^{\mathrm{T}}\right) = r(\mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}) \le r(\mathbf{B}^{\mathrm{T}}) = r(\mathbf{B})$. ⌘

Example 13. Consider $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ and $\mathbf{B} = \mathbf{A}^{\mathrm{T}}$. Then $\mathbf{AB} = \mathbf{AA}^{\mathrm{T}} = \begin{pmatrix} 5 & 11 & 17 \\ 11 & 25 & 39 \\ 17 & 39 & 61 \end{pmatrix}$, which can have rank at most 2, and indeed in this case it is 2.

Corollary. (Rank & Submatrices). Let $\mathbf{A}$ be $m \times n$. Then $r(\mathbf{A}) \ge k$ if and only if there is a $k \times k$ invertible submatrix of $\mathbf{A}$.

Proof. Suppose $r(\mathbf{A}) \geq k$, then **A** has *k* linearly independent rows. Let **B** consists of those rows, so **B** is $k \times n$ of full row rank. Then **B** has to have *k* linearly independent columns. Let **C** be the submatrix of **B** consisting of those columns. Then **C** is $k \times k$ of rank *k*, and hence invertible. The converse is trivial since the submatrix already has rank *k*. ⌘

Example 14. Let $\mathbf{A} = \begin{pmatrix} 5 & 11 & 17 \\ 11 & 25 & 39 \\ 17 & 39 & 61 \end{pmatrix}$. Then $5 \cdot 25 - 11^2 \neq 0$, so the rank is at least 2.

Corollary. (Spaces and Matrices). Let V be a vector space. Then there exist matrices **A**, **B**, **C** and **D** such that $V = \mathcal{C}(\mathbf{A}) = \mathcal{R}(\mathbf{B}) = \mathrm{N}(\mathbf{C}) = \mathrm{L}(\mathbf{D})$.

Proof. Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be a basis for *V*. Let $\mathbf{A} = \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \end{pmatrix}$. Let $\mathbf{B} = \mathbf{A}^{\mathrm{T}}$. Let $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m$ be a basis for $\mathrm{N}(\mathbf{B})$. Let $\mathbf{C} = \begin{pmatrix} \mathbf{w}_1^{\mathrm{T}} \\ \mathbf{w}_2^{\mathrm{T}} \\ \vdots \\ \mathbf{w}_n^{\mathrm{T}} \end{pmatrix}$. Finally, let $\mathbf{D} = \mathbf{C}^{\mathrm{T}}$. ⌘

Example 15. Let *V* be the span of the vectors $\begin{pmatrix} 5 \\ 11 \\ 17 \\ 23 \\ 29 \end{pmatrix}$, $\begin{pmatrix} 11 \\ 25 \\ 39 \\ 53 \\ 67 \end{pmatrix}$ and $\begin{pmatrix} 17 \\ 39 \\ 61 \\ 83 \\ 105 \end{pmatrix}$, so we could take **A** to be the matrix with these three columns, but as it turns out they are not independent, so a more efficient **A** is $\mathbf{A} = \begin{pmatrix} 5 & 11 \\ 11 & 25 \\ 17 & 39 \\ 23 & 53 \\ 29 & 67 \end{pmatrix}$. Now $\mathbf{B} = \mathbf{A}^{\mathrm{T}}$, which reduces to $\begin{pmatrix} 1 & 0 & -1 & -2 & -3 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$ so a basis for $\mathrm{N}(\mathbf{B})$ is $\begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 2 \\ -3 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 3 \\ -4 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. So $\mathbf{C} = \begin{pmatrix} 1 & -2 & 1 & 0 & 0 \\ 2 & -3 & 0 & 1 & 0 \\ 3 & -4 & 0 & 0 & 1 \end{pmatrix}$.

❶❷ Matrices as Transformations

In this section we look at how the nature of a matrix is reflected when we view it as a transformation—actually what is known as a linear transformation.

For example, consider $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$, then define a function $f_{\mathbf{A}} : \mathbb{R}^2 \to \mathbb{R}^3$ simply by $\mathbf{u} \mapsto \mathbf{Au}$, explicitly $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x+2y \\ 3x+4y \\ 5x+6y \end{pmatrix}$. In general, if $\mathbf{A}$ is an $m \times n$ matrix, then we think of it as a transformation from $\mathbb{R}^n$ into $\mathbb{R}^m$ by simple multiplication—namely, if $\mathbf{u} \in \mathbb{R}^n$, then $\mathbf{u} \mapsto \mathbf{Au} \in \mathbb{R}^m$. In functional notation, $f_{\mathbf{A}} : \mathbb{R}^n \to \mathbb{R}^m$, $f_{\mathbf{A}}(\mathbf{u}) = \mathbf{Au}$. It is clear that the following two properties are satisfied by this transformation:

$f_{\mathbf{A}}(\mathbf{u}+\mathbf{v}) = \mathbf{A}(\mathbf{u}+\mathbf{v}) = \mathbf{Au}+\mathbf{Av}$ the **image of a sum is the sum of the images**

and

$f_{\mathbf{A}}(a\mathbf{u}) = \mathbf{A}(a\mathbf{u}) = a\mathbf{Au}$ **image of a multiple is the multiple of the image**.

A function that satisfies these properties is called a **linear transformation**, since they take lines to lines among other things. The connection between linear transformations and matrices is intimate indeed. In fact, composition of functions corresponds to matrix multiplication:

> **Theorem (Composition).** Let $\mathbf{A}$ be $m \times n$, $\mathbf{B}$ be $n \times p$, so $f_{\mathbf{A}} : \mathbb{R}^n \to \mathbb{R}^m$ and $f_{\mathbf{B}} : \mathbb{R}^p \to \mathbb{R}^n$. Then their composition $f_{\mathbf{A}} \circ f_{\mathbf{B}} : \mathbb{R}^p \to \mathbb{R}^m$ is nothing but matrix multiplication, $f_{\mathbf{A}} \circ f_{\mathbf{B}} = f_{\mathbf{AB}}$.

Proof. It is trivial: $f_{\mathbf{A}} \circ f_{\mathbf{B}}(\mathbf{u}) = f_{\mathbf{A}}(\mathbf{Bu}) = \mathbf{ABu} = f_{\mathbf{AB}}(\mathbf{u})$. ⌘

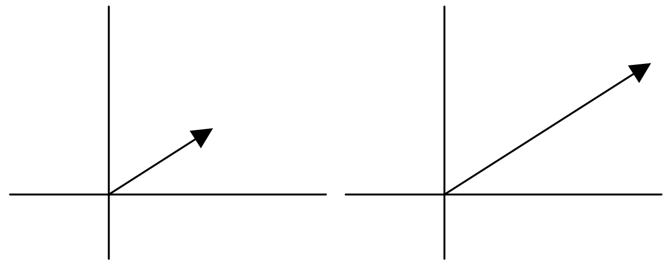
Example 1. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ and let $\mathbf{B} = \begin{pmatrix} 2 & 5 & 8 \end{pmatrix}$. So $\mathbf{BA} = \begin{pmatrix} 57 & 72 \end{pmatrix}$. Now $\begin{pmatrix} x \\ y \end{pmatrix} \overset{f_{\mathbf{A}}}{\longmapsto} \begin{pmatrix} x+2y \\ 3x+4y \\ 5x+6y \end{pmatrix}$ while $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \overset{f_{\mathbf{B}}}{\longmapsto} (2x+5y+8z)$, and $\begin{pmatrix} x \\ y \end{pmatrix} \overset{f_{\mathbf{B}} \circ f_{\mathbf{A}}}{\longmapsto} (57x+72y)$.

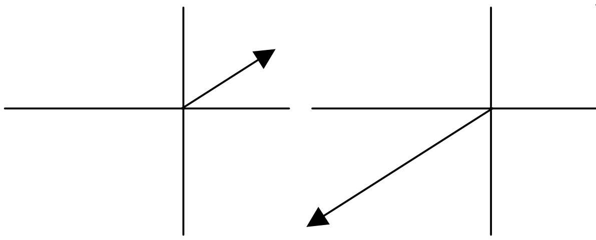
In general, when discussing multidimensional transformations, it is hard to visualize what they are actually doing. So, as usual we will look in the lower dimensional situations first. But first two general examples.

Example 2. The simplest example one can think of is to use $\mathbf{A}=\mathbf{0}$. In that case every vector gets mapped to the zero vector, $\mathbf{u}\mapsto\mathbf{0}$ or $f_{\mathbf{0}}(\mathbf{u})=\mathbf{0}$. This is the **zero function**, and, of course, by choosing the size of the zero matrix appropriately, one can map vectors of any given size, to the zero vector of a chosen size.

Example 3. Another simple example is to choose $\mathbf{A}=\mathbf{I}$. Then every vector gets mapped to itself, $\mathbf{u}\mapsto\mathbf{u}$, it is the **identity function**.

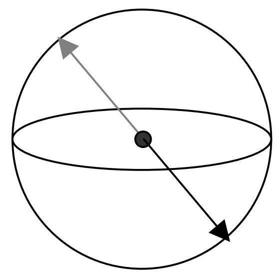
Now, let $\mathbf{A}=2\mathbf{I}$. This is an example of a **dilatation**. The geometric action is simple, every vector is doubled, is multiplied by 2.





In contrast, the case $\mathbf{A}=-2\mathbf{I}$ is more interesting since it also rotates vectors by 180°.

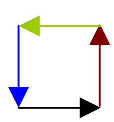
More concretely, if $\mathbf{A}=-\mathbf{I}$ in 3-space, then we have an **antipodal** map that maps every point of a sphere centered at the origin to its antipodal point:



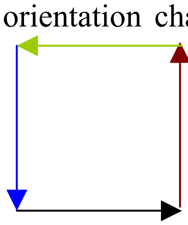
These two examples are easily observed in any dimension, but the next few examples are restricted to the plane—and then we will have a few in 3-space.

One of the crucial facts about linear transformations is that they are easily understood once one understands what is happening to the axes.

For example, in $\mathbb{R}^2$, since $\mathbf{A}\begin{pmatrix}a\\b\end{pmatrix}=a\mathbf{A}\begin{pmatrix}1\\0\end{pmatrix}+b\mathbf{A}\begin{pmatrix}0\\1\end{pmatrix}$, once we understand what geometrically is happening to $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$, we know what is happening to all vectors. One way to visualize this is to see what is happening to the unit box, that is in the case of the plane, the square with corners at the origin, $\begin{pmatrix}1\\0\end{pmatrix}$, $\begin{pmatrix}1\\1\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$ in that order to be able

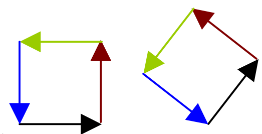


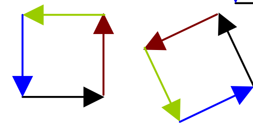
to detect orientation changes. For example, for the transformation $\mathbf{A}=2\mathbf{I}$, becomes

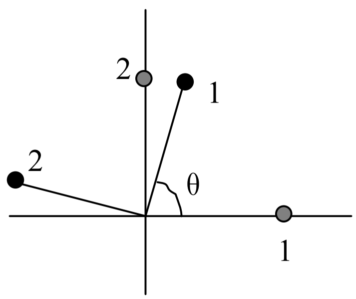


, and the area has quadrupled.

Example 4. Let $\mathbf{A} = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$. This is a **rotation** by 60° about the origin (counterclockwise, of course). Similarly, $\mathbf{A}^2 = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix}$ represents a 120° rotation.

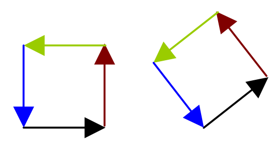




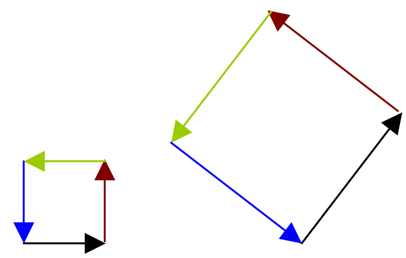


In general, if $\mathbf{A} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, then $f_{\mathbf{A}}$ is the rotation by angle θ, $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$.

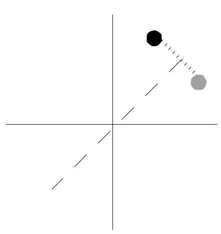
Thus, $\mathbf{A} = \frac{1}{2}\begin{pmatrix} \sqrt{2} & -\sqrt{2} \\ \sqrt{2} & \sqrt{2} \end{pmatrix}$ represents a 45°-rotation.



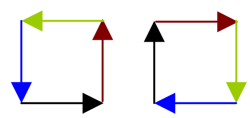
Example 5. Let $\mathbf{A} = \begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$. This is the composition of the previous two examples, thus it rotates as it doubles.



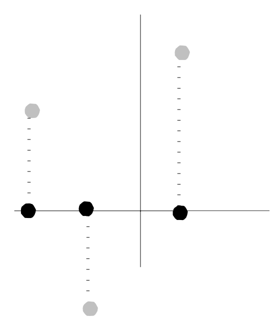
The following does reverse the orientation.

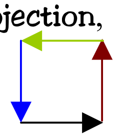


Example 6. Let $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Geometrically what is occurring is the **reflection** on the $y = x$ line. Note that its determinant is -1. The action is given by $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} b \\ a \end{pmatrix}$.

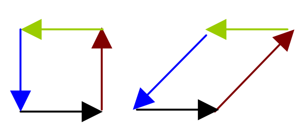


Example 7. Let $\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Everything is mapped to the x-axis: $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ 0 \end{pmatrix}$. It is called a **projection**, this particular example being the projection onto the x-axis.

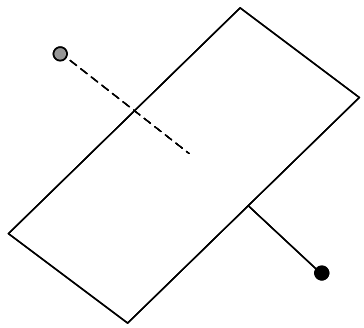




Example 8. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. This is an example of a **shear**—it maps the square to a parallelogram of the same area.



Now we will discuss some transformation of 3-space. As it turns out, these transformations are far richer than those in the plane.



Example 9. Reflection on a Plane. Let $\mathbf{u}$ be a unit vector. Consider the matrix $\mathbf{A} = \mathbf{I} - 2\mathbf{u}\mathbf{u}^{\mathrm{T}}$. Then $\mathbf{A} = \mathbf{A}^{\mathrm{T}}$, $\mathbf{A}$ is symmetric, and

$$\mathbf{A}^2 = \mathbf{I} - 4\mathbf{u}\mathbf{u}^{\mathrm{T}} + 4\mathbf{u}\mathbf{u}^{\mathrm{T}}\mathbf{u}\mathbf{u}^{\mathrm{T}} = \mathbf{I},$$

since $\mathbf{u}^{\mathrm{T}}\mathbf{u} = 1$. What does the transformation $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ do? Easily, $\mathbf{A}\mathbf{u} = -\mathbf{u}$. Consider any vector $\mathbf{v}$ perpendicular to $\mathbf{u}$, then since $\mathbf{u}^{\mathrm{T}}\mathbf{v} = 0$, we have $\mathbf{A}\mathbf{v} = \mathbf{v}$. Thus the plane of vector perpendicular to $\mathbf{u}$ is a plane of fixed points.

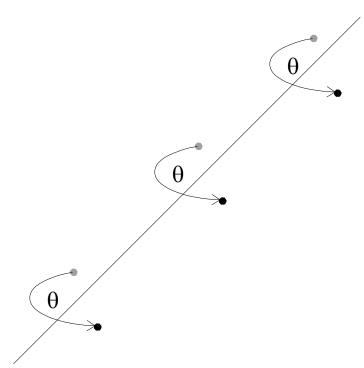
If $\mathbf{p}$ is any other point, then $\mathbf{p}^{\mathrm{T}}\mathbf{v} = \mathbf{p}^{\mathrm{T}}\mathbf{A}\mathbf{v} = (\mathbf{A}\mathbf{p})^{\mathrm{T}}\mathbf{v}$, and so $(\mathbf{A}\mathbf{p} - \mathbf{p})$ is orthogonal to the plane. We recognize here **the reflection on the plane with normal $\mathbf{u}$**. Reflections in space, as was the case in the plane, have determinant -1. Below we will see a different way of computing reflections in any space.

For example, if we let $\mathbf{u} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, so it is orthogonal to the *x*-*y* plane. Then $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ is the reflection on that plane.

Note that the size of the vector is immaterial, and indeed the expression $\mathbf{A} = \mathbf{I} - 2\mathbf{u}\mathbf{u}^{\mathrm{T}}$ will always represent the reflection on the hyperplane orthogonal to $\mathbf{u}$.

Example 10. If we wanted to find the reflection on the plane $2x + 3y + 6z = 0$, we need a unit normal to that plane. One such vector is $\mathbf{u} = \frac{1}{7}\begin{pmatrix} 2 \\ 3 \\ 6 \end{pmatrix}$, and so $\frac{1}{49}\begin{pmatrix} 41 & -12 & -24 \\ -12 & 31 & -36 \\ -24 & -36 & -23 \end{pmatrix}$ is the reflection matrix.

Example 11. Suppose that $\mathbf{u}$ and $\mathbf{v}$ are unit vectors, not parallel, *i.e.*, not equivalent directions. When we multiply (or compose) their respective reflections, we get $\mathbf{I} - 2\mathbf{u}\mathbf{u}^{\mathrm{T}} - 2\mathbf{v}\mathbf{v}^{\mathrm{T}} + 4(\mathbf{u}\cdot\mathbf{v})\mathbf{u}\mathbf{v}^{\mathrm{T}}$. This matrix will have determinant 1, so it will not be a reflection. Since the cross product $\mathbf{u}\times\mathbf{v}$ is orthogonal to both vectors, it will be a fixed point of both transformations and hence of their composition.



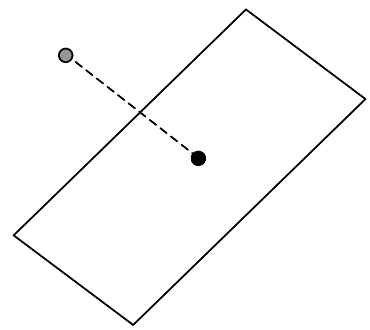
Hence we have a line of fixed points: $[\mathbf{u}\times\mathbf{v}]$. What happens to the plane perpendicular to that fixed line? **This plane**

orthogonal to the fixed line has to be transformed into itself. As it turns it is a rotation of that plane where the angle of the rotation is twice the angle between the vector **u** and **v**.

This is an example of a **rotation in 3-space**. They have an **axis of rotation** (of fixed points) and every other point moves in planes perpendicular to that axis of rotation by a rotation in that plane by a fixed angle. Thus a rotation has two parameters, the axis and the angle.

Closely related to reflections (and very relevant to our course) is the notion of projection.

Example 12. Projection on a Plane. Suppose we are given a plane in $\mathbb{R}^3$. Then the projection of a point to that plane is the point in the plane in which the original point lands when it is dropped perpendicularly to the plane. In other words, it is the intersection of the plane and the line between a point and its reflection. It is also **the point on the closest to our original point.** Below we will see how to compute projections.



The next example is more abstract:

Example 13. (Polynomials & Derivatives) A polynomial is an expression of the form

$$p(x) = a_0 + a_1x^1 + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

where $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{R}$. If $a_n \neq 0$, then $p(x)$ is said to be of degree *n*. Easily if one adds two polynomials, one gets another polynomial, and the same is true if one multiplies by a scalar. Every polynomial of degree at most *n* can be thought of as a vector of size $n+1$ by simply thinking of $p(x)$ as above to correspond to $\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}$, and so we can think of all of these polynomials as being $\mathbb{R}^{n+1}$.

Consider now all polynomials of degree at most 3, so we are considering elements of $\mathbb{R}^4$. Now we know that **the derivative of a sum is the sum of the derivatives** from calculus, we also know that the derivative of a constant times a function is the constant times the derivative of the function—in other words taking derivatives is a linear transformations. Since the derivative lowers the degree, we are considering a transformation from $\mathbb{R}^4$ to $\mathbb{R}^3$, so the matrix **D** that accomplishes this transformation should be a 3×4. What does it do to the vector $\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$? This will be the first column of D.

But the vector represents the polynomial 1 which has derivative 0, so the first column is $\begin{pmatrix}0\\0\\0\end{pmatrix}$. Similarly, x is represented by $\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$, so the second column of **D** is $\begin{pmatrix}1\\0\\0\end{pmatrix}$. Continuing in this fashion we see that $\mathbf{D}=\begin{pmatrix}0&1&0&0\\0&0&2&0\\0&0&0&3\end{pmatrix}$.

Example 14. (Polynomials again) Consider multiplication by the polynomial $1+x^2$. This is a linear transformation that will send our domain of polynomials of degree at most 3 to polynomials of degree at most 5, so our transformation goes from $\mathbb{R}^4$ to $\mathbb{R}^6$, and the matrix should be 6×4. Since $1\mapsto 1+x^2$, $\begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}\mapsto\begin{pmatrix}1\\0\\1\\0\\0\\0\end{pmatrix}$, and the matrix $\mathbf{M}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{pmatrix}$ is arrived at by considering what happens to x, x^2 and x^3.

We can connect some of the notions about matrices with some common words about functions.

A function is said to be **one-to-one** if it does not map two objects in the domain to the same object in the codomain. The last example was one-to-one because no two polynomials give the same product when multiplied by $1+x^2$.

A function is said to be **onto** if every possible output in the codomain is an actual output from the domain. The derivative example is onto because every polynomial of degree at most two is the derivative of a polynomial of degree at most 3.

If a function is both one-to-one and onto, then it is called a **bijection** (or **one-to-one correspondence**).

The following theorem is a direct consequence of the **Existence and Uniqueness of Solutions Facts** proven before

Theorem (One-to-one and onto). Let $\mathbf{A}$ be an $m\times n$ matrix so $f_{\mathbf{A}}:\mathbb{R}^n\to\mathbb{R}^m$. Then the following are true:

① $f_{\mathbf{A}}$ is one-to-one if and only if the columns of $\mathbf{A}$ are linearly independent, or equivalently, if $\mathbf{A}$ is of full column rank.

② $f_{\mathbf{A}}$ is onto if and only if $\mathcal{C}(\mathbf{A})=\mathbb{R}^m$, or equivalently, if $\mathbf{A}$ is of full row rank.

If $n=m$, then the following four statements are equivalent:

$f_{\mathbf{A}}$ is a bijection	$f_{\mathbf{A}}$ is one-to-one
$f_{\mathbf{A}}$ is onto	$\mathbf{A}$ is invertible.

Example 15. We saw $\mathbf{M}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\1&0&1&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{pmatrix}$ was one-to-one while $\mathbf{D}=\begin{pmatrix}0&1&0&0\\0&0&2&0\\0&0&0&3\end{pmatrix}$ was onto.

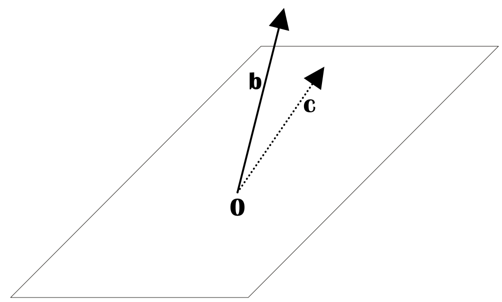
On the other hand, $\mathbf{M}^{\mathrm{T}}\mathbf{M}=\begin{pmatrix}2&0&1&0\\0&2&0&1\\1&0&2&0\\0&1&0&2\end{pmatrix}$ and $\mathbf{DD}^{\mathrm{T}}=\begin{pmatrix}1&0&0\\0&4&0\\0&0&9\end{pmatrix}$ are both bijections.

For the remainder of the section we concentrate on projections. We all know the geometric fact that two points in the plane determine a unique line. From the linear algebraic point of view, this is a clear claim: if $\begin{pmatrix}x_1\\y_1\end{pmatrix}$ and $\begin{pmatrix}x_2\\y_2\end{pmatrix}$ are the two points, and without loss we assume that $x_1\neq x_2$, then we want an m and a b so that $y_1=mx_1+b$ and $y_2=mx_2+b$—in other words, we are looking for a solution to the system $\mathbf{Ax}=\mathbf{b}$ where $\mathbf{A}=\begin{pmatrix}x_1&1\\x_2&1\end{pmatrix}$, $\mathbf{x}=\begin{pmatrix}m\\b\end{pmatrix}$ and $\mathbf{b}=\begin{pmatrix}y_1\\y_2\end{pmatrix}$. Since $\det\mathbf{A}=x_1-x_2\neq 0$, we know the system has a unique solution.

But what happens if we have three or more points in the plane—in that case there may be a line or there may not be a line that goes through those points. If we are given the points $\begin{pmatrix}x_1\\y_1\end{pmatrix}$, $\begin{pmatrix}x_2\\y_2\end{pmatrix}$, …, $\begin{pmatrix}x_t\\y_t\end{pmatrix}$, then we need, as before, to find an m and a b so that $y_1=mx_1+b$, $y_2=mx_2+b$, …, $y_t=mx_t+b$. In other words, we need a solution to the system $\mathbf{Ax}=\mathbf{b}$

where $\mathbf{A} = \begin{pmatrix} x_1 & 1 \\ x_2 & 1 \\ \vdots & \vdots \\ x_t & 1 \end{pmatrix}$, $\mathbf{x} = \begin{pmatrix} m \\ b \end{pmatrix}$ and $\mathbf{b} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}$. Of course, we now run into the problem of whether there is a solution or not by equivalently asking whether **b** is in the column space of **A** or not. We know that the column space of **A** is a plane in $\mathbb{R}^t$, and the vector **b** may lie in that plane or it may not.

There is a problem in the latter case, and in that case, it has been a consistent assumption for over two centuries (and clearly justified for many applications) to put all the error in the vector **b**. In that case, the key idea is to take the vector **c** in the plane that is closest to the vector **b**, and solve the system $\mathbf{Ax} = \mathbf{c}$.



How do we find **c** then? Our geometric intuition indicates then the vector $\mathbf{b} - \mathbf{c}$ should be perpendicular to the plane, and so it should be the case then that $\mathbf{b} - \mathbf{c}$ is perpendicular to $\mathbf{Ax}$ (expressed by $\mathbf{b} - \mathbf{c} \perp \mathbf{Ax}$) for any vector $\mathbf{x} \in \mathbb{R}^2$. But we want **c** to be in the column space of **A**, and so there must exist a **z** such that $\mathbf{Az} = \mathbf{c}$. And so we arrive to the fact that for any $\mathbf{x} \in \mathbb{R}^2$, and for some $\mathbf{z} \in \mathbb{R}^2$,

$$(\mathbf{Ax})^{\mathrm{T}}(\mathbf{b} - \mathbf{Az}) = \mathbf{x}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}(\mathbf{b} - \mathbf{Az}) = 0,$$

and since this is true for all $\mathbf{x} \in \mathbb{R}^2$, we must have

$$\mathbf{A}^{\mathrm{T}}(\mathbf{b} - \mathbf{Az}) = \mathbf{0}.$$

and thus we know we should let **z** be a solution to

$$\mathbf{A}^{\mathrm{T}}\mathbf{Az} = \mathbf{A}^{\mathrm{T}}\mathbf{b},$$

and since the columns of **A** are linearly independent, the rank of $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is 2 (see **Lemma** below), and $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is invertible, and thus

$$\mathbf{z} = \left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}}\mathbf{b}$$

and since even more interesting than the vector **c** is the vector **z**, we are done. By the way, we can always find **c** by $\mathbf{c} = \mathbf{Az}$.

> **Lemma.** For any $m \times n$ matrix **A**, the rank of $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is the same as the rank of **A**.

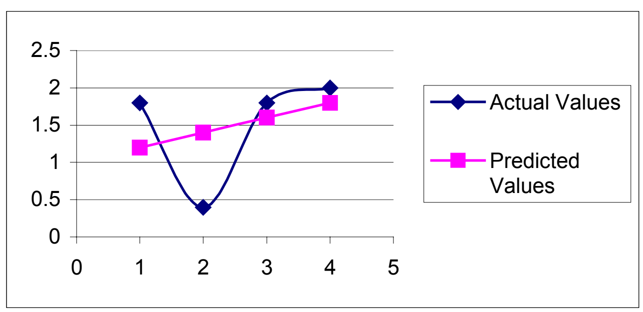
Proof. It suffices to show that they have the same null space because the rank of either matrix **A** or $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is $n -$ dimension of the null space, and so we would be done. Clearly, if $\mathbf{Ax} = \mathbf{0}$, then $\mathbf{A}^{\mathrm{T}}\mathbf{Ax} = \mathbf{0}$. But conversely, if $\mathbf{A}^{\mathrm{T}}\mathbf{Ax} = \mathbf{0}$, then $(\mathbf{Ax})^{\mathrm{T}}\mathbf{Ax} = \mathbf{x}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}\mathbf{Ax} = 0$, and so $\mathbf{Ax} \perp \mathbf{Ax}$, and so $\mathbf{Ax} = \mathbf{0}$. ⌘

Example 16. You are a young executive in a relatively young firm, and you are in charge of forecasting sales. At the end of the first but very prosperous year, the company sold \$1.8 million, but during the second year when a lot of competition showed up, it sold only \$400,000. However, good management and aggressive salesmanship helped the firm bounce back by matching the first year's performance during the third year. Things got even better during the fourth year (the end of which is the present) when it sold a cool \$2 million. Your boss would like to know how likely is it that sales will increase next year and by how much. She wants to use a linear model. You adequately obey her and find the best fit line and use it to forecast sales for the fifth year. But you also discuss with her the limitations of using a linear model.

Here what we want is to find a line that goes through the points $\begin{pmatrix}1\\1.8\end{pmatrix}$, $\begin{pmatrix}2\\0.4\end{pmatrix}$, $\begin{pmatrix}3\\1.8\end{pmatrix}$ and $\begin{pmatrix}4\\2.0\end{pmatrix}$. So we want an m and a b so that $y = mx + b$ is the line. In particular we want $1.8 = m + b$, $0.4 = 2m + b$, $1.8 = 3m + b$ and $2.0 = 4m + b$. In other words, we are looking for a solution to the system $\mathbf{Ax} = \mathbf{b}$ where $\mathbf{A} = \begin{pmatrix}1 & 1\\2 & 1\\3 & 1\\4 & 1\end{pmatrix}$, $\mathbf{b} = \begin{pmatrix}1.8\\0.4\\1.8\\2.0\end{pmatrix}$ and $\mathbf{x} = \begin{pmatrix}m\\b\end{pmatrix}$.

Using the reasoning from above we start with the equation $\mathbf{Ax} = \mathbf{b}$, and then multiply by $\mathbf{A}^{\mathrm{T}}$, and so we consider the equation $\mathbf{A}^{\mathrm{T}}\mathbf{Ax} = \mathbf{A}^{\mathrm{T}}\mathbf{b}$. But $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \begin{pmatrix}30 & 10\\10 & 4\end{pmatrix}$ is invertible, and $\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1} = \frac{1}{20}\begin{pmatrix}4 & -10\\-10 & 30\end{pmatrix}$, and since $\mathbf{A}^{\mathrm{T}}\mathbf{b} = \begin{pmatrix}16\\6\end{pmatrix}$, so we get $\mathbf{x} = \left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}}\mathbf{b} = \begin{pmatrix}0.2\\1\end{pmatrix}$, and we use the line $y = .2x + 1$ as the best fit line to the data we have, and so when we let $x = 5$, we will get \$2 million for a prediction.

Year	Actual Values	Prediction
1	1.8	1.2
2	0.4	1.4
3	1.8	1.6
4	2	1.8

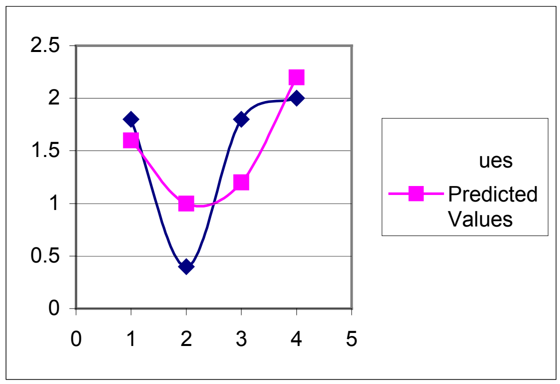


How comfortable are we with our prediction?

What we are saying is that the vector $\mathbf{c} = \begin{pmatrix}1.2\\1.4\\1.6\\1.8\end{pmatrix}$ is the vector in the column space of $\mathbf{A}$ that is closest (nearest) to the vector $\mathbf{b} = \begin{pmatrix}1.8\\0.4\\1.8\\2.0\end{pmatrix}$, and so we are changing the vector $\mathbf{b}$

as little as we can and yet obtain a solution. The distance from $\mathbf{b}$ to $\mathbf{c}$ is $\sqrt{.36+1+.04+.04}=\sqrt{1.44}=1.2$.

Of course, by looking at the shape of the original data, we could have speculated that a quadratic approximation was perhaps better suited for the prediction, so we should rather perhaps be considering an equation of the form $y=ax^2+bx+c$. Then we need to solve the system $\mathbf{Ax}=\mathbf{b}$ where $\mathbf{A}=\begin{pmatrix}1&1&1\\4&2&1\\9&3&1\\16&4&1\end{pmatrix}$, $\mathbf{x}=\begin{pmatrix}a\\b\\c\end{pmatrix}$ and $\mathbf{b}=\begin{pmatrix}1.8\\0.4\\1.8\\2.0\end{pmatrix}$. When we compute $\mathbf{A}^{\mathrm{T}}\mathbf{A}=\begin{pmatrix}354&100&30\\100&30&10\\30&10&4\end{pmatrix}$, and so $\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}=\frac{1}{20}\begin{pmatrix}5&-25&25\\-25&129&-135\\25&-135&155\end{pmatrix}$, and since $\mathbf{A}^{\mathrm{T}}\mathbf{b}=\begin{pmatrix}51.6\\16\\6\end{pmatrix}$, we get $\mathbf{x}=\begin{pmatrix}a\\b\\c\end{pmatrix}=\begin{pmatrix}0.4\\-1.8\\3\end{pmatrix}$, and thus we would use the parabola $y=.4x^2-1.8x+3$ for our predictions, and then we would get a very striking \$4 million for next year.



Year	Actual Values	Prediction
1	1.8	1.6
2	0.4	1.0
3	1.8	1.2
4	2	2.2

Thus our reconsideration led to very different results. Again, one way to measure our uncertainty is to see how much change we have had in the vector $\mathbf{b}$, which went from $\mathbf{b}=\begin{pmatrix}1.8\\0.4\\1.8\\2.0\end{pmatrix}$ to $\mathbf{c}=\begin{pmatrix}1.6\\1.0\\1.2\\2.2\end{pmatrix}$, and their distance apart is $\sqrt{0.8}\approx .89$, a smaller change.

Of course, we can only push this idea so far. If we got to the cubic (the next case up), we would have that now the matrix is invertible, so $\mathbf{b}$ would not need to change at all, and we would be claiming that we have an exact procedure of prediction, which is highly unlikely. Just for thoroughness sake, the cubic would be $-\frac{2}{3}x^3+5.4x^2-\frac{194}{15}x+10$, and the model is so silly that it would predict **negative** sales of \$3 million in year 5.
Now that we have finished this very long example, the time has come to put a theoretical framework around it.

The key theorem is the following:

Theorem (Projections). Let V be a subspace of $\mathbb{R}^m$. Then there exists a unique matrix $\mathbf{Q}$ that satisfies the following:

① $\mathbf{Q}^2 = \mathbf{Q}$ ② $\mathbf{Q}^{\mathrm{T}} = \mathbf{Q}$

③ for any $\mathbf{u}$, $\mathbf{Qu} \in V$, thus $\mathcal{C}(\mathbf{Q}) = V$.

Moreover, for every $\mathbf{u} \in \mathbb{R}^m$, $\mathbf{u} - \mathbf{Qu} \in \mathrm{N}(\mathbf{Q})$, and for every $\mathbf{v} \in V$, $\mathbf{Qv} = \mathbf{v}$.

Proof. Let $\mathbf{v}_1$, $\mathbf{v}_2$, …, $\mathbf{v}_t$ be a basis of V, and let $\mathbf{A}$ be the matrix whose columns are the $\mathbf{v}$'s. Then since its columns are linearly independent, $\mathbf{A}$ has rank t, and so $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ (by the lemma above) is invertible since it has rank t and is of size $t \times t$. Also since the columns of $\mathbf{A}$ span V, we have that $\mathcal{C}(\mathbf{A}) = V$, so for any $\mathbf{u} \in \mathbb{R}^m$, $\mathbf{Au} \in V$, and, vice versa, if $\mathbf{v} \in V$, then $\mathbf{v} = \mathbf{Au}$ for some $\mathbf{u}$. Consider the $m \times m$ matrix $\mathbf{Q} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}}$. We have $\mathbf{Q}^2 = \mathbf{QQ} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}}\mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}} = \mathbf{Q}$, and we have the first condition. Also $\mathbf{Q}^{\mathrm{T}} = \left(\mathbf{A}^{\mathrm{T}}\right)^{\mathrm{T}}\left(\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\right)^{\mathrm{T}}\mathbf{A}^{\mathrm{T}} = \mathbf{A}\left(\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{\mathrm{T}}\right)^{-1}\mathbf{A}^{\mathrm{T}}$, but since $\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}}\mathbf{A}$, we have ②. Let $\mathbf{u} \in \mathbb{R}^m$, then $\mathbf{Qu} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}}\mathbf{u} = \mathbf{Ax} \in V$, so $\mathcal{C}(\mathbf{Q})$ is contained in V. Conversely, let $\mathbf{v} \in V$, then we know $\mathbf{v} = \mathbf{Au}$ for some $\mathbf{u}$, and then $\mathbf{Qv} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}}\mathbf{Au} = \mathbf{Au} = \mathbf{v}$, so we have ③. Now $\mathbf{Q}(\mathbf{u} - \mathbf{Qu}) = \mathbf{Qu} - \mathbf{Q}^2\mathbf{u} = \mathbf{0}$ so we have the added comment. All that is left to prove is that $\mathbf{Q}$ is unique. But suppose $\mathbf{P}$ also works. Then we know that for any $\mathbf{u}$, $\mathbf{QPu} = \mathbf{Pu}$ since $\mathbf{Pu} \in V$. Thus $\mathbf{QP} = \mathbf{P}$, and this implies that $\mathbf{QP}$ is symmetric, which implies $\mathbf{PQ} = \mathbf{QP}$ (see exercises). For any $\mathbf{v} \in V$, we have that $\mathbf{v} = \mathbf{Pu}$, and so $\mathbf{Pv} = \mathbf{PPu} = \mathbf{v}$, and so we get $\mathbf{PQu} = \mathbf{Qu}$, so $\mathbf{PQ} = \mathbf{Q}$, and we have equality. ⌘

$\mathbf{Q}$ is known as the **projection** along V. A matrix that satisfies the first property is called an **idempotent** matrix, while of course, a matrix that satisfies the second property is **symmetric**. Thus, projection matrices are **symmetric idempotents**. By the uniqueness in the theorem, it is clear that every symmetric idempotent is the projection along its column space.

Example 17. Suppose $V = \mathcal{C}(\mathbf{M})$ where $\mathbf{M} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$. Then as we saw before the first two columns form a basis for V, and so we can let $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 4 & 5 \\ 7 & 8 \end{pmatrix}$ in the construction above, and so the projection matrix $\mathbf{Q} = \frac{1}{6}\begin{pmatrix} 5 & 2 & -1 \\ 2 & 2 & 2 \\ -1 & 2 & 5 \end{pmatrix}$. But also the first and the third column form a basis, so we could have used $\mathbf{B} = \begin{pmatrix} 1 & 3 \\ 4 & 6 \\ 7 & 9 \end{pmatrix}$. Due to the uniqueness of the projection (and an easy computation for the nonbelievers), $\mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}} = \mathbf{Q} = \mathbf{B}\left(\mathbf{B}^{\mathrm{T}}\mathbf{B}\right)^{-1}\mathbf{B}^{\mathrm{T}}$.

The fundamental geometric property of projections is given in the following theorem:

> **Theorem (Nearest Point).** Let V be a subspace of $\mathbb{R}^m$, and let $\mathbf{Q}$ be its projection. Then for any $\mathbf{u} \in \mathbb{R}^m$, $\mathbf{Qu}$ is the unique vector in V nearest to $\mathbf{u}$.

Proof. We need to show that for any $\mathbf{x}$, the distance between $\mathbf{Qx}$ and $\mathbf{u}$ is at least as big as the distance between $\mathbf{Qu}$ and $\mathbf{u}$ with equality if and only if $\mathbf{Qx} = \mathbf{Qu}$. We know that it suffices to prove the inequality for the square of the distances. But then the square of the former is given by

$$(\mathbf{Qx} - \mathbf{u}) \cdot (\mathbf{Qx} - \mathbf{u}) = (\mathbf{Qx} - \mathbf{u})^{\mathrm{T}} (\mathbf{Qx} - \mathbf{u}) = \left(\mathbf{x}^{\mathrm{T}}\mathbf{Q} - \mathbf{u}^{\mathrm{T}}\right)(\mathbf{Qx} - \mathbf{u}) = \mathbf{x}^{\mathrm{T}}\mathbf{Qx} - 2\mathbf{x}^{\mathrm{T}}\mathbf{Qu} + \mathbf{u}^{\mathrm{T}}\mathbf{u}$$

while the square of the distance between $\mathbf{Qu}$ and $\mathbf{u}$ is given by

$$(\mathbf{Qu} - \mathbf{u}) \cdot (\mathbf{Qu} - \mathbf{u}) = (\mathbf{Qu} - \mathbf{u})^{\mathrm{T}} (\mathbf{Qu} - \mathbf{u}) = \left(\mathbf{u}^{\mathrm{T}}\mathbf{Q} - \mathbf{u}^{\mathrm{T}}\right)(\mathbf{Qu} - \mathbf{u}) = \mathbf{u}^{\mathrm{T}}\mathbf{Qu} - 2\mathbf{u}^{\mathrm{T}}\mathbf{Qu} + \mathbf{u}^{\mathrm{T}}\mathbf{u},$$

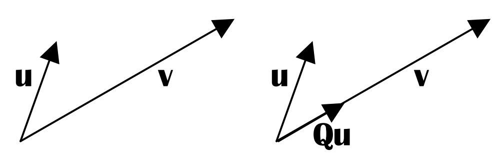
and subtracting the second from the first, we get

$$\mathbf{x}^{\mathrm{T}}\mathbf{Qx} - 2\mathbf{x}^{\mathrm{T}}\mathbf{Qu} + \mathbf{u}^{\mathrm{T}}\mathbf{Qu} = (\mathbf{Qx} - \mathbf{Qu})^{\mathrm{T}} (\mathbf{Qx} - \mathbf{Qu}) = (\mathbf{Qx} - \mathbf{Qu}) \cdot (\mathbf{Qx} - \mathbf{Qu}) \geq 0$$

with equality if and only if $\mathbf{Qx} = \mathbf{Qu}$. ⌘

It is this theorem that gives the method applied to examples at the beginning of the section its name—**the method of least squares**.

Example 18. Suppose we let $V = [\mathbf{v}]$. Then $\mathbf{A} = (\mathbf{v})$, so $\mathbf{Q} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}} = \dfrac{1}{\mathbf{v} \cdot \mathbf{v}}\mathbf{v}\mathbf{v}^{\mathrm{T}}$, and so the nearest multiple of $\mathbf{v}$ to a given $\mathbf{u}$ is given by $\mathbf{Qu} = \dfrac{\mathbf{v} \cdot \mathbf{u}}{\mathbf{v} \cdot \mathbf{v}}\mathbf{v}$, which goes well with this picture on the right:



Of particular interest is when $\mathbf{v} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$. This is the case, for example, when we have made a number of observations, say t, on an unknown quantity, and the system of equations is of the form $x = a_1$, $x = a_2$, …, $x = a_t$. But then we shall take the projection of $\mathbf{u} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_t \end{pmatrix}$

along **v**, which is $\frac{a_1 + a_2 + \cdots + a_t}{t}\mathbf{v}$, the average of the observations. This is the nearest vector to **u**, not surprising, yet satisfying.

Example 19. The Nearest Symmetric Matrix. As we saw in a previous section $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, form a basis for the 2×2 symmetric matrices. If we would like to project along this space, we need to compute the projection matrix, and switching our point of view, we need to think of matrices as vectors, so there elements of the basis become $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, respectively. And then if we let **A** be the matrix with these as its columns, we have that $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and so $\mathbf{Q} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, and thus the nearest symmetric matrix to $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} a & \frac{b+c}{2} \\ \frac{b+c}{2} & d \end{pmatrix}$, common sense indeed.

Example 20. Projections and Reflections. Given a subspace V we can think of the reflection on that subspace—namely the reflection would leave every point of the subspace alone while it would take every vector perpendicular to that subspace to its negative. This is the natural extension of the reflections in $\mathbb{R}^3$ previously discussed. Let then **Q** be the projection along V, and let **R** be the reflection on V. We can see that geometrically there is an intimate connection between the two transformations.

Observe first that if **w** is perpendicular to V, then **w** is perpendicular to every column of **Q**, but since **Q** is symmetric, we have that **w** is orthogonal to every row of **Q**, or equivalently, $\mathbf{Qw} = \mathbf{0}$. Of course, we already know that $\mathbf{Qv} = \mathbf{v}$ for every **v** in V. But then if we consider the matrix $2\mathbf{Q} - \mathbf{I}$, we can see that this transformation accomplishes the same effect as the reflection, and so $\mathbf{R} = 2\mathbf{Q} - \mathbf{I}$.

Specifically, suppose we consider the plane $2x + 3y + 6z = 0$. Then the vectors $\begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}$ form a basis for the plane, so if we let $\mathbf{A} = \begin{pmatrix} -3 & 0 \\ 0 & -2 \\ 1 & 1 \end{pmatrix}$, then

$$\mathbf{Q} = \mathbf{A}\left(\mathbf{A}^{\mathrm{T}}\mathbf{A}\right)^{-1}\mathbf{A}^{\mathrm{T}} = \frac{1}{49}\begin{pmatrix} 45 & -6 & -12 \\ -6 & 40 & -18 \\ -12 & -18 & 13 \end{pmatrix}.$$

And if we compute $2\mathbf{Q}-\mathbf{I}$, we in fact obtain the previously computed

$$\mathbf{R} = \frac{1}{49}\begin{pmatrix} 41 & -12 & -24 \\ -12 & 31 & -36 \\ -24 & -36 & -23 \end{pmatrix}.$$

But at the same time we can use the reflection matrix to give us projections. For example if we wanted the projection onto the hyperplane given by the equation:

$$x+2y+3z+4w+5u=0.$$

Then since $\mathbf{u} = \frac{1}{\sqrt{55}}\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix}$ is a unit vector orthogonal to the hyperplane, we get the reflection on that hyperplane to be $\mathbf{R} = \mathbf{I} - 2\mathbf{u}\mathbf{u}^{\mathrm{T}} = \frac{1}{55}\begin{pmatrix} 53 & -4 & -6 & -8 & -10 \\ -4 & 47 & -12 & -16 & -20 \\ -6 & -12 & 37 & -24 & -30 \\ -8 & -16 & -24 & 23 & -40 \\ -10 & -20 & -30 & -40 & 5 \end{pmatrix}$, and so the projection is $\mathbf{Q} = \frac{1}{2}\left(\mathbf{R}+\mathbf{I}\right)$.

❶❸ Determinants & Adjoints

We now return to the topic of determinants. Of course, we have seen before:

$$\det \mathbf{A} = a \text{ for the } 1\times 1 \text{ matrix } \mathbf{A} = (a),$$

$$\det \mathbf{A} = ad - bc \text{ for the } 2\times 2 \text{ matrix } \mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

$$\det \mathbf{A} = aei + bfg + cdh - ceg - afh - bdi \text{ for the } 3\times 3 \text{ matrix } \mathbf{A} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}.$$

And the time has come to consider the determinant of an $n\times n$ matrix. But before we can do that we need to recall the connection between determinants and inverses. In fact what happened was that in each of these instances we found a matrix $\mathbf{B}$ such that

$$\mathbf{AB} = \mathbf{BA} = (\det \mathbf{A})\mathbf{I}.$$

Recalling the construction in the 3×3 case, we went through three stages:

1. Compute the matrix of subdeterminants where at each entry one places the determinant obtained from $\mathbf{A}$ by scratching out the given row and column;
2. Change the sign of the odd positions, where the $i, j-$position is odd if $i + j$ is odd;
3. Transpose the matrix.

Then starting with $\mathbf{A} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$, one gets $\mathbf{B} = \begin{pmatrix} ei - fh & ch - bi & bf - ce \\ fg - di & ai - cg & cd - af \\ dh - eg & bg - ah & ae - bd \end{pmatrix}$.

What we need to observe now is that if we had applied the construction to the 2×2 matrix $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we would have obtained respectively, $\begin{pmatrix} d & c \\ b & a \end{pmatrix}$, $\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ and $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. But this last matrix is exactly the matrix seen before that satisfies the critical equation $\mathbf{AB} = \mathbf{BA} = (\det \mathbf{A})\mathbf{I}$. Even further, if one were to take the determinant of the empty matrix (0×0) to be 1, the constructions would also work in the 1×1 case.

Thus the matrix built by the three steps 1, 2 and 3 plays in role in both the definition of determinants and the construction of the inverse. Thus, it necessitates a name:

Let **A** be an $n\times n$ matrix and suppose we already know how to compute the determinant of $(n-1)\times(n-1)$ matrices. Then the matrix obtained from **A** by pursuing steps **1**, **2** and **3** above is called the **classical adjoint** of **A**, and we will use $\tilde{\mathbf{A}}$ to denote the adjoint[1].

Thus, $\widetilde{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ for example.

The fabulous theorem says it all:

> **Theorem (Adjoints).** Let **A** be an $n\times n$ matrix. Then there is a scalar a such that
> $$\mathbf{A}\tilde{\mathbf{A}} = \tilde{\mathbf{A}}\mathbf{A} = a\mathbf{I}.$$

One defines this scalar a to be the determinant of **A**, $\det \mathbf{A}$. Thus as a trivial consequence,

$$\mathbf{A}\tilde{\mathbf{A}} = \tilde{\mathbf{A}}\mathbf{A} = (\det \mathbf{A})\mathbf{I}.$$

Thus the determinant is defined recursively—one has to know how to compute 3×3's to be able to compute 4×4's, etcetera. Below we will see how to circumvent this necessity via another theorem. The proof of the Adjoint Theorem can be found in the Appendix of Proofs.

Example 1. Consider $\mathbf{A} = \begin{pmatrix} 1 & 3 & 5 & 6 \\ 5 & 7 & 8 & 9 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix}$. Then the matrix obtained by taking the subdeterminants is $\begin{pmatrix} 0 & 4 & 8 & 4 \\ 4 & 8 & 4 & 0 \\ 7 & 4 & -29 & -25 \\ 3 & 0 & -21 & -17 \end{pmatrix}$, then changing the signs in the appropriate positions, we get $\begin{pmatrix} 0 & -4 & 8 & -4 \\ -4 & 8 & -4 & 0 \\ 7 & -4 & -29 & 25 \\ -3 & 0 & 21 & -17 \end{pmatrix}$, and finally by transposing, we get $\tilde{\mathbf{A}} = \begin{pmatrix} 0 & -4 & 7 & -3 \\ -4 & 8 & -4 & 0 \\ 8 & -4 & -29 & 21 \\ -4 & 0 & 25 & -17 \end{pmatrix}$, and one can then readily verify that

$$\mathbf{A}\tilde{\mathbf{A}} = \tilde{\mathbf{A}}\mathbf{A} = 4\mathbf{I},$$

and so $\det \mathbf{A} = 4$.

---

[1] This is not standard notation, some books use $\operatorname{adj}\mathbf{A}$ instead.

By the way, the 4×4 case of odd positions is given by $\begin{pmatrix} e & o & e & o \\ o & e & o & e \\ e & o & e & o \\ o & e & o & e \end{pmatrix}$.

Note that as an obvious consequence of the equation

$$\mathbf{A}\tilde{\mathbf{A}} = \tilde{\mathbf{A}}\mathbf{A} = (\det \mathbf{A})\mathbf{I},$$

we have the following:

① If $\mathbf{A}$ has a row of zeroes, then $\det \mathbf{A} = 0$ since that row of zeroes will produce a row of zeroes in $\mathbf{A}\tilde{\mathbf{A}}$.

Similarly, a column of zeroes in $\mathbf{A}$ will produce a column of zeroes in $\tilde{\mathbf{A}}\mathbf{A}$.

② If $\mathbf{A}$ has two identical rows, then $\det \mathbf{A} = 0$, because those two identical rows will produce two identical rows in $\mathbf{A}\tilde{\mathbf{A}}$.

Similarly if $\mathbf{A}$ has two identical columns, it will have zero determinant.

Clarifying notation, if we let $\mathbf{A}_{ij}$ denote the matrix obtained from $\mathbf{A}$ by deleting the i^{th} row and j^{th} column, then the $i, j-$position of $\tilde{\mathbf{A}}$, $\tilde{a}_{ij}$, is given by

$$\tilde{a}_{ij} = (-1)^{i+j} \det \mathbf{A}_{ji}.$$

Of course, if all one wanted was the determinant of a matrix, all we would need would be to compute one row or one column of $\tilde{\mathbf{A}}$. This follows directly from the fact that

$$\det \mathbf{A} = a_{i1}\tilde{a}_{1i} + a_{i2}\tilde{a}_{2i} + \cdots + a_{in}\tilde{a}_{ni} = \tilde{a}_{i1}a_{1i} + \tilde{a}_{i2}a_{2i} + \cdots + \tilde{a}_{in}a_{ni}$$

for any i. But to compute $\tilde{a}_{ki}$, one needs to scratch the i^{th} row and k^{th} column. For example, to compute the first column of $\tilde{\mathbf{A}}$, we would be using the first row of $\mathbf{A}$, and we would compute the determinant of the matrix obtained when the first row and each of the columns is cancelled, and then we would do the sign change, and obtain the numbers $\begin{pmatrix} 0 & -4 & 8 & -4 \end{pmatrix}$, and when we look at the dot product of this vector with the first row of $\mathbf{A}$, which is $\begin{pmatrix} 1 & 3 & 5 & 6 \end{pmatrix}$, we get $-12+40-24=4$, and thus, that is the determinant.

Note that again we could have chosen any row or column of the matrix to perform this computation since $\mathbf{A}\tilde{\mathbf{A}} = \tilde{\mathbf{A}}\mathbf{A} = (\det \mathbf{A})\mathbf{I}$. This way of computing the determinant is referred to as **row** (or **column**) **expansion of the determinant of A.** To streamline this important remark further, we highlight it further. As before, if we let $\mathbf{A}_{ij}$ denote the matrix obtained from $\mathbf{A}$ by deleting the i^{th} row and j^{th} column,

> To compute the determinant of any (square) matrix $\mathbf{A}$, we can select an arbitrary road or column to expand by it. To do the computation, and for example's sake, assume we have chosen the second row to expand by, then if let $\hat{\mathbf{a}}_{ij}$ be the determinant of the submatrix obtained by crossing out the i^{th} row and j^{th} column, then we have

$$\det \mathbf{A} = (-1)^{2+1} a_{21}\widehat{\mathbf{a}}_{21} + (-1)^{2+2} a_{22}\widehat{\mathbf{a}}_{22} + (-1)^{2+3} a_{23}\widehat{\mathbf{a}}_{23} + \cdots + (-1)^{2+n} a_{2n}\widehat{\mathbf{a}}_{2n}.$$

Observe the transpose operation is being accomplished by the switch in the indices. One situation where row or column expansion is particularly useful is when most of the entries in that row or column are 0 since then the number of subdeterminants to be computed is minimized

Example 2. Consider $\mathbf{A} = \begin{pmatrix} 2 & 5 & 7 & 11 & 8 & 9 \\ 6 & 8 & 4 & 3 & 2 & 0 \\ 0 & 3 & 4 & 5 & 6 & 0 \\ 0 & 5 & 6 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 4 & 5 & 0 \end{pmatrix}$. Then we can expand by the last column, and we get that $\det \mathbf{A} = (-1)^7 9 \det \mathbf{B}$ where $\mathbf{B} = \begin{pmatrix} 6 & 8 & 4 & 3 & 2 \\ 0 & 3 & 4 & 5 & 6 \\ 0 & 5 & 6 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 2 & 4 & 5 \end{pmatrix}$, and now expanding by the first column, we get $\det \mathbf{B} = (-1)^2 6 \det \mathbf{C}$ where $\mathbf{C} = \begin{pmatrix} 3 & 4 & 5 & 6 \\ 5 & 6 & 0 & 0 \\ 8 & 0 & 0 & 0 \\ 0 & 2 & 4 & 5 \end{pmatrix}$. Note the 6 received the sign it had in the matrix **B**, not in the matrix **A**. Computing the determinant of **C** by expanding by the third row, we have then $\det \mathbf{C} = (-1)^4 8 \det \mathbf{D}$ where $\mathbf{D} = \begin{pmatrix} 4 & 5 & 6 \\ 6 & 0 & 0 \\ 2 & 4 & 5 \end{pmatrix}$, and $\det \mathbf{D} = -6 \det \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix} = -6$, so we get

$$\det \mathbf{A} = -9 \times 6 \times 8 \times -6 = 2592.$$

Corollary (Upper Triangular Matrices). If **A** is upper triangular, then

$$\det \mathbf{A} = a_{11} a_{22} \cdots a_{nn} = \prod_{i=1}^{n} a_{ii},$$

the product of its diagonal entries.

Proof. By induction on *n*. It is true for $n = 2$ easily. The rest follows readily by expanding by the last row, which is of the form $\begin{pmatrix} 0 & \cdots & 0 & a_{nn} \end{pmatrix}$. Then we obviously do not care what any of the subdeterminants are (since we intend to take the dot product of this last row with the vector of subdeterminants) except for the one obtained when we cancel the last row and the last column. But then the left over matrix is also upper triangular, and so by inducting we get that the vector of subdeterminants is of the form

$\begin{pmatrix} * & \cdots & * & \prod_{i=1}^{n-1} a_{ii} \end{pmatrix}$ (note that since we are at a diagonal entry the sign is positive), and so we obtain the corollary. ⌘

In particular, $\det \mathbf{I} = 1$.

Example 3. Permutation Matrices. Let $\mathbf{P}$ be a permutation matrix where each row and each column has exactly one 1 in it, and zeroes everywhere else.

In the 2×2 case, we have two such matrices, the identity of determinant 1 and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of determinant -1. when the identity had positive determinant and $\det\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$.

For the 3×3 case there are 6 permutation matrices: $\mathbf{I}$, $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ of determinant 1, and $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ of determinant -1.

In general, the expansion of the determinant of a permutation matrix is relatively painless, and clearly since each $\mathbf{P}_{ij}$ is either a permutation matrix or has a row of zeroes, all we need to keep track are the signs, and eventually we will arrive at a 2×2 permutation matrix, so the determinant of a permutation matrix of any size is either $+1$ or -1. As in the small cases, half of them have determinant $+1$ and half of them have determinant -1.

One key observation needs to be made in general. Suppose a permutation matrix is obtained from the identity matrix by just simply swapping two rows, then this matrix would have $n-2$ ones on the main diagonal, so if we were to expand by each of these first we would end up with the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, of negative determinant. For example, $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ where the 2^{nd} and 4^{th} rows have exchanged places, if we expand by the 1^{st}, 3^{rd} and 5^{th} rows first, we will easily get determinant -1.

As a consequence of the construction (and the theorem) we get:

Theorem (Transposes). Let $\mathbf{A}$ be a square matrix. Then
$$\widetilde{\mathbf{A}^{\mathrm{T}}} = \widetilde{\mathbf{A}}^{\mathrm{T}} \text{ and } \det\left(\mathbf{A}^{\mathrm{T}}\right) = \det \mathbf{A}.$$

Proof. By induction on n. It is true for $n = 2$ easily. Just as readily, $\left(\mathbf{A}^{\mathrm{T}}\right)_{ij} = \left(\mathbf{A}_{ji}\right)^{\mathrm{T}}$. By definition, the $i, j-$entry of $\widetilde{\mathbf{A}^{\mathrm{T}}}$ is $(-1)^{i+j} \det\left(\mathbf{A}^{\mathrm{T}}\right)_{ji}$, which equals $(-1)^{i+j} \det \mathbf{A}_{ij}$, by induction, but this is the $j, i-$entry of $\widetilde{\mathbf{A}}$. And the first claim has been established. For the second, since $\mathbf{A}\widetilde{\mathbf{A}} = \widetilde{\mathbf{A}}\mathbf{A} = (\det \mathbf{A})\mathbf{I}$, by transposing this equation we get $\widetilde{\mathbf{A}}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}}\widetilde{\mathbf{A}}^{\mathrm{T}} = (\det \mathbf{A})\mathbf{I}$, and by we have just proven, this is tantamount to
$$\widetilde{\mathbf{A}^{\mathrm{T}}}\mathbf{A}^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}}\widetilde{\mathbf{A}^{\mathrm{T}}} = (\det \mathbf{A})\mathbf{I}$$
which implies $\det\left(\mathbf{A}^{\mathrm{T}}\right) = \det \mathbf{A}$. ⌘

Note actually we proved more—namely that if the Adjoint Theorem held for $\mathbf{A}$, then it also held for $\mathbf{A}^{\mathrm{T}}$.

Example 4. Thus, as in the previous example, the adjoint of $\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} 1 & 5 & 9 & 13 \\ 3 & 7 & 10 & 14 \\ 5 & 8 & 11 & 15 \\ 6 & 9 & 12 & 16 \end{pmatrix}$ is given by $\begin{pmatrix} 0 & -4 & 8 & -4 \\ -4 & 8 & -4 & 0 \\ 7 & -4 & -29 & 25 \\ -3 & 0 & 21 & -17 \end{pmatrix}$.

The proof of the Adjoint Theorem is intimately connected with reduction, and as part of the consequence those developments we will obtain another major theorem about determinants and adjoints. But first we need a Corollary to the theorem.

Corollary (Rank & Adjoints). Let $\mathbf{A}$ be $n \times n$. Then exactly one of ❶, ❷ or ❸ occurs:

	Matrix	Adjoint	Det
❶	$r(\mathbf{A}) = n$	$r(\widetilde{\mathbf{A}}) = n$	$\neq 0$
❷	$r(\mathbf{A}) = n-1$	$r(\widetilde{\mathbf{A}}) = 1$	0
❸	$r(\mathbf{A}) \leq n-2$	$r(\widetilde{\mathbf{A}}) = 0$	0

Proof. Recall that we already know that $\mathbf{A}$ is invertible if and only if $r(\mathbf{A}) = n$, and by the theorem, if $\det \mathbf{A} \neq 0$, $\mathbf{A}$ is invertible. Once again the proof is by induction. If $n = 2$, then the rank of $\mathbf{A}$ is either 0, 1 or 2. If $r(\mathbf{A})=0$, then clearly $\tilde{\mathbf{A}}=\mathbf{0}$ and $\det\mathbf{A}=0$. If $r(\mathbf{A})=2$, then we already know that $\det\mathbf{A}\neq 0$ and $r(\tilde{\mathbf{A}})=2$. Finally, if $r(\mathbf{A})=1$, then clearly $\det\mathbf{A}=0$ (because otherwise $\mathbf{A}$ would be invertible), and so $\mathbf{A}\tilde{\mathbf{A}}=\tilde{\mathbf{A}}\mathbf{A}=\mathbf{0}$, and since neither $\mathbf{A}$ nor $\tilde{\mathbf{A}}$ is $\mathbf{0}$, we must have ❷. By induction if $r(\mathbf{A})\leq n-2$, then $\det\mathbf{A}_{ij}=0$ for all *i, j* since $r(\mathbf{A}_{ij})<n-1$, and so $\tilde{\mathbf{A}}=\mathbf{0}$, and ❸ is done. On the other hand if $r(\mathbf{A})\geq n-1$, then we know $\mathbf{A}$ has an has $n-1\times n-1$ invertible submatrix and so $\tilde{\mathbf{A}}\neq\mathbf{0}$. If $r(\mathbf{A})=n-1$, then $\mathbf{A}$ is not invertible, and so $\det\mathbf{A}=0$. But since $\mathbf{A}\tilde{\mathbf{A}}=\mathbf{0}$, every column of $\tilde{\mathbf{A}}$ is in $\mathbf{N}(\mathbf{A})$, and since $\dim\mathbf{N}(\mathbf{A})=1$, $r(\tilde{\mathbf{A}})=1$, and we have ❷. Finally, if $r(\mathbf{A})=n$, then since $\tilde{\mathbf{A}}\neq\mathbf{0}$, $\det\tilde{\mathbf{A}}\neq 0$, and $\tilde{\mathbf{A}}=\det(\mathbf{A})\mathbf{A}^{-1}$, so $r(\tilde{\mathbf{A}})=n$. ⌘

A fact from the last corollary is worth isolating:

> **Corollary (Determinants and Inverses).** $\mathbf{A}$ is invertible if and only if $\det\mathbf{A}\neq 0$. If that is the case, $\tilde{\mathbf{A}}=\det(\mathbf{A})\mathbf{A}^{-1}$.

Example 5. Let $\mathbf{A}=\begin{pmatrix}1&2&3\\3&6&9\\12&24&36\end{pmatrix}$, then $\tilde{\mathbf{A}}=\mathbf{0}$ since $r(\mathbf{A})=1$. Let $\mathbf{A}=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}$, then $\tilde{\mathbf{A}}=\begin{pmatrix}-3&6&-3\\6&-12&6\\-3&6&-3\end{pmatrix}$, while if $\mathbf{A}=\begin{pmatrix}1&2&3\\4&5&9\\7&8&15\end{pmatrix}$, then $\tilde{\mathbf{A}}=\begin{pmatrix}3&-6&3\\3&-6&3\\-3&6&-3\end{pmatrix}$.

The adjoint together with row (and column) expansion allow us to discuss an alternate way to solve square linear systems with unique solutions. Ironically, it is a method that in the West precedes Gaussian elimination.

Example 6. *Cramer's Rule.* Consider the system $\mathbf{Ax}=\mathbf{b}$ where $\mathbf{A}=\begin{pmatrix}1&3&5&6\\5&7&8&9\\9&10&11&12\\13&14&15&16\end{pmatrix}$, the matrix from a previous example, and $\mathbf{b}=\begin{pmatrix}1\\2\\3\\4\end{pmatrix}$. Then since $\mathbf{A}$ is invertible, we know that $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$. If we let $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$, since then $\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}\tilde{\mathbf{A}}$, we have that

$$x_i = \frac{\mathbf{v}_i \mathbf{b}}{\det \mathbf{A}}$$

where $\mathbf{v}_i$ is the i^{th} row of $\tilde{\mathbf{A}}$. Consider the matrix $\mathbf{A}_i$ obtained from $\mathbf{A}$ when its i^{th} column is replaced by $\mathbf{b}$. Since $\mathbf{A}$ and $\mathbf{A}_i$ agree in all columns but the i^{th} column, the i^{th} row of $\tilde{\mathbf{A}}$ is the same as the i^{th} row of $\widetilde{\mathbf{A}_i}$. But then $\mathbf{v}_i\mathbf{b}$ is nothing but i^{th} row of $\widetilde{\mathbf{A}_i}$ times the i^{th} column of $\mathbf{A}_i$, which is the $i,i-$entry of $\tilde{\mathbf{A}}_i\mathbf{A}_i = (\det \mathbf{A}_i) I$. Thus we have

$$x_i = \frac{\det \mathbf{A}_i}{\det \mathbf{A}}.$$

For example

$$x_1 = \frac{\det\begin{pmatrix} 1 & 3 & 5 & 6 \\ 2 & 7 & 8 & 9 \\ 3 & 10 & 11 & 12 \\ 4 & 14 & 15 & 16 \end{pmatrix}}{\mathbf{A}} = \frac{1}{4} \text{ and } x_2 = \frac{\det\begin{pmatrix} 1 & 1 & 5 & 6 \\ 5 & 2 & 8 & 9 \\ 9 & 3 & 11 & 12 \\ 13 & 4 & 15 & 16 \end{pmatrix}}{\mathbf{A}} = \frac{0}{4}.$$

Now we are ready for the second major theorem on determinants:

> **Theorem (Multiplicativity).** Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$. Then $\widetilde{\mathbf{AB}} = \tilde{\mathbf{B}}\tilde{\mathbf{A}}$ and $\det \mathbf{AB} = \det \mathbf{A} \det \mathbf{B}$.

The proof of this theorem can be found in the Appendix of Proofs. The mantra to go with this theorem is, of course,

the determinant of a product is the product of the determinants.

From the geometric point of view this is clear, since the scale of magnification of volume under the transformation $f_{\mathbf{A}}$ is $\det \mathbf{A}$, in other words, we have that the area of any figure when transformed by $f_{\mathbf{A}}$ will be multiplied by $\det \mathbf{A}$. And since $f_{\mathbf{A}} \circ f_{\mathbf{B}} = f_{\mathbf{AB}}$, we should have that the eventual change of a volume under $f_{\mathbf{AB}}$ is $\det \mathbf{AB} = \det \mathbf{A} \det \mathbf{B}$.

Note that since $\mathbf{AA}^{-1} = \mathbf{I}$, we have

> **Corollary (Determinant of Inverse).** Let $\mathbf{A}$ be invertible, then
> $$\det \mathbf{A}^{-1} = (\det \mathbf{A})^{-1} = \frac{1}{\det \mathbf{A}}.$$

The **Multiplicativity Theorem** allows us to predict the effect that elimination has on the determinant—recall the three key steps to row reduction:

① **Permuting rows;**

② **Multiplying a row by a nonzero number,**

and

③ **Adding a multiple of a row to another row.**

Since each of these is multiplication on the left by the appropriate matrix, we can use the theorem to gauge the effect of reduction on the determinant.

Of course, if we swap two rows of a matrix $\mathbf{A}$, **its determinant will change signs** because the determinant of such a permutation matrix (as we saw before) is -1. If we multiply a row by a nonzero number, **the determinant is being multiplied by the same number** since we are multiplying by a diagonal matrix with all entries 1 except for the nonzero number, and finally if we add a multiple of a row to another row, **we do not change the determinant** since we are multiplying by a triangular matrix with 1's on the main diagonal.

Example 7. Let $\mathbf{A}=\begin{pmatrix} -1 & 2 & 7 & 8 & 4 \\ 2 & 3 & 13 & 6 & 2 \\ 3 & 5 & 4 & 5 & 5 \\ 2 & 5 & 7 & 8 & 7 \\ 2 & 8 & 12 & 14 & 0 \end{pmatrix}$. Then we can start by pulling the 2 from the last row to obtain the matrix $\mathbf{B}=\begin{pmatrix} -1 & 2 & 7 & 8 & 4 \\ 2 & 3 & 13 & 6 & 2 \\ 3 & 5 & 4 & 5 & 5 \\ 2 & 5 & 7 & 8 & 7 \\ 1 & 4 & 6 & 7 & 0 \end{pmatrix}$. What is the relation between the determinants of the two matrices? Since $\mathbf{B}=\mathbf{DA}$ where $\mathbf{D}$ is the diagonal matrix with $\mathbf{1}$'s on the diagonal except for the $5,5-$position where there is a $\frac{1}{2}$, we have that $\det\mathbf{D}=\frac{1}{2}$, and so $\det\mathbf{A}=2\det\mathbf{B}$ (note the 2 has been pulled). So it suffices to compute $\det\mathbf{B}$. But in this matrix, we can subtract multiples of the last row from the other rows (pivot on the $5,5-$position) to obtain the matrix with the same determinant, $\begin{pmatrix} 0 & 6 & 13 & 15 & 4 \\ 0 & -5 & 1 & -8 & 2 \\ 0 & -7 & -14 & -16 & 5 \\ 0 & -3 & -5 & -6 & 7 \\ 1 & 4 & 6 & 7 & 0 \end{pmatrix}$. Then expanding by the first column, since the $5,5-$position has a positive sign, we have that this matrix has the same determinant as the matrix $\begin{pmatrix} 6 & 13 & 15 & 4 \\ -5 & 1 & -8 & 2 \\ -7 & -14 & -16 & 5 \\ -3 & -5 & -6 & 7 \end{pmatrix}$, and then by **column reducing** (which can not be done for systems, but can be done for determinants since a matrix and its transpose have the same determinant), when we use the

$2,2-$position, we get $\begin{pmatrix} 71 & 13 & 119 & -22 \\ 0 & 1 & 0 & 0 \\ -77 & -14 & -128 & 33 \\ -28 & -5 & -46 & 17 \end{pmatrix}$, of the same determinant. Expanding this determinant by the second row, we get $\begin{pmatrix} 71 & 119 & -22 \\ -77 & -128 & 33 \\ -28 & -46 & 17 \end{pmatrix}$ of equal determinant. Finally, we could choose to compute this 3×3 directly, or to do some more reduction. We could subtract twice the third row from the second one, obtaining $\begin{pmatrix} 71 & 119 & -22 \\ -21 & -36 & -1 \\ -28 & -46 & 17 \end{pmatrix}$, and then use the $2,3-$position to do cleaning in that column, getting the matrix $\begin{pmatrix} 533 & 911 & 0 \\ -21 & -36 & -1 \\ -385 & -658 & 0 \end{pmatrix}$. Expanding the determinant of this matrix by the third column we get since the $2,3-$position has a negative sign, that we do not change determinants if we consider the matrix $\begin{pmatrix} 533 & 911 \\ -385 & -658 \end{pmatrix}$, which has determinant 21, and so $\det \mathbf{B} = 21$, and so $\det \mathbf{A} = 42$. There are many alternate ways to compute this determinant, but they will all lead to the same answer, 42.

Example 8. What is the determinant of the matrix $\mathbf{M} = \begin{pmatrix} 1-x & 1 & 1 & 1 \\ 1 & 1-x & 1 & 1 \\ 1 & 1 & 1-x & 1 \\ 1 & 1 & 1 & 1-x \end{pmatrix}$? If we add each other row to the first row, the determinant has not changed, and we get the matrix $\mathbf{N} = \begin{pmatrix} 4-x & 4-x & 4-x & 4-x \\ 1 & 1-x & 1 & 1 \\ 1 & 1 & 1-x & 1 \\ 1 & 1 & 1 & 1-x \end{pmatrix}$. Now we know then that

$$\det \mathbf{M} = \det \mathbf{N} = (4-x)\det \mathbf{K}$$

where $\mathbf{K} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1-x & 1 & 1 \\ 1 & 1 & 1-x & 1 \\ 1 & 1 & 1 & 1-x \end{pmatrix}$. Subtracting now the first row from the other rows, again the determinant does not change, but now the matrix is $\mathbf{L} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -x & 0 & 0 \\ 0 & 0 & -x & 0 \\ 0 & 0 & 0 & 0-x \end{pmatrix}$

which by triangularity has determinant $-x^3$, and so

$$\det \mathbf{M} = \det \mathbf{N} = (4-x)\det \mathbf{K} = -(4-x)x^3.$$

We finish the section with another useful consequence of the **Multiplicativity Theorem** allows

Corollary (Determinants & Block Upper Triangular). Let $\mathbf{M} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{C} \end{pmatrix}$ be in balanced block upper triangular form. Then

$$\det \mathbf{M} = \det \mathbf{A} \det \mathbf{C}.$$

Proof. Note that it is not required that $\mathbf{A}$ and $\mathbf{C}$ be of the same size, just each of them be a square matrix. If $\mathbf{C}$ is not invertible, then $\det \mathbf{M} = 0 = \det \mathbf{A} \det \mathbf{C}$. Otherwise, consider the matrix $\mathbf{X} = \begin{pmatrix} \mathbf{I} & -\mathbf{B}\mathbf{C}^{-1} \\ \mathbf{0} & \mathbf{C}^{-1} \end{pmatrix}$. Then by expanding by the first column, and then by the new first column, etcetera, we see that $\det \mathbf{X} = \det \mathbf{C}^{-1} = \dfrac{1}{\det \mathbf{C}}$. Now

$$\mathbf{N} = \mathbf{X}\mathbf{M} = \begin{pmatrix} \mathbf{I} & -\mathbf{B}\mathbf{C}^{-1} \\ \mathbf{0} & \mathbf{C}^{-1} \end{pmatrix}\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{C} \end{pmatrix} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}.$$

Then expanding by the last column, and then by the new last column, etcetera, we see that $\det \mathbf{N} = \det \mathbf{A}$. But then

$$\det \mathbf{A} = \det \mathbf{N} = \det \mathbf{X} \det \mathbf{M} = \frac{\det \mathbf{M}}{\det \mathbf{C}},$$

and we are done. ⌘

The theorem can easily be extended by induction to block triangular matrices with more than 2 blocks.

Example 9. Let $\mathbf{A} = \begin{pmatrix} 2 & 1 & 3 & 4 & 5 & 6 \\ 1 & 2 & 7 & 8 & 9 & 2 \\ 0 & 0 & 3 & 1 & 5 & 6 \\ 0 & 0 & 1 & 3 & 7 & 8 \\ 0 & 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 0 & 1 & 4 \end{pmatrix}$. Then we can see this as a 3×3 block upper triangular, and so the determinant is the product of the determinant $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, which is 3, the determinant of $\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$, 8, and the determinant of $\begin{pmatrix} 4 & 1 \\ 1 & 4 \end{pmatrix}$, 15. Thus $\det \mathbf{A} = 3\times 8\times 15 = 360$.

❶❹ The Need for Eigenvalues

We start the study of eigenvalues with a well-known example:

Example 1. The Fibonacci Sequence. The sequence 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144,… is known as the Fibonacci sequence. In symbols,

$$F_0 = 0\,,\ F_1 = 1\,,\ F_2 = 1, \ldots,\ F_{n-1}\,,\ F_n\,,\ F_{n+1} = F_n + F_{n-1}, \ldots$$

Note that our level of understanding of the sequence is limited. For example, if we wanted to know F_{25}, we would have to compute all the F_i's prior to it. So we look for an alternate way of gaining insight into the sequence.

Let $\mathbf{u}_n = \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}$, so $\mathbf{u}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\mathbf{u}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $\mathbf{u}_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, $\mathbf{u}_3 = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$, et cetera. Let $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then

$$\mathbf{Au}_n = \begin{pmatrix} F_{n+1} + F_n \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \mathbf{u}_{n+1},$$

so $\mathbf{Au}_0 = \mathbf{u}_1$, $\mathbf{Au}_1 = \mathbf{u}_2$, $\mathbf{Au}_2 = \mathbf{u}_3$, etcetera. But then $\mathbf{u}_2 = \mathbf{Au}_1 = \mathbf{AAu}_0 = \mathbf{A}^2\mathbf{u}_0$, similarly, $\mathbf{u}_3 = \mathbf{Au}_2 = \mathbf{AA}^2\mathbf{u}_0 = \mathbf{A}^3\mathbf{u}_0$, and in general

$$\mathbf{A}^n\mathbf{u}_0 = \mathbf{u}_n\,.$$

Unfortunately, just because we have this expression does not mean we are ready to compute $\mathbf{u}_{25}$ since that would require us knowing $\mathbf{A}^{25}$, and it does seem that we are going around in circles. Of course, machines are quite useful, but there is another more interesting way.

Nobody would disagree that if $\mathbf{A}$ had been a diagonal matrix, its powers would be easily computed since they are nothing but the powers of the entries in the diagonal of the matrix. But $\mathbf{A}$ is not diagonal. However, can we find a matrix $\mathbf{P}$ such that

$$\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$$

is a diagonal matrix? If so, how? And would that be useful? Let us tackle the last issue first.

Suppose we had $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$. Solving for $\mathbf{A}$, we would get $\mathbf{A} = \mathbf{PDP}^{-1}$, and then multiplying this by itself, we have

$$\mathbf{A}^2 = \mathbf{AA} = \mathbf{PDP}^{-1}\mathbf{PDP}^{-1} = \mathbf{PDDP}^{-1} = \mathbf{PD}^2\mathbf{P}^{-1},$$

and similarly

$$\mathbf{A}^3 = \mathbf{A}^2\mathbf{A} = \mathbf{PD}^2\mathbf{P}^{-1}\mathbf{PDP}^{-1} = \mathbf{PD}^2\mathbf{DP}^{-1} = \mathbf{PD}^3\mathbf{P}^{-1},$$

and continuing by induction one has that for any positive integer *n*,

$$\mathbf{A}^n = \mathbf{PD}^n\mathbf{P}^{-1}.$$

Thus, the powers of $\mathbf{A}$ would be readily available (by just two matrix multiplications) from the powers of $\mathbf{D}$.

Now we proceed to decide whether we can find such a diagonal matrix $\mathbf{D}$ and such a matrix $\mathbf{P}$. If we are to have $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, then we must equivalently have that $\mathbf{AP} = \mathbf{PD}$, with $\mathbf{P}$ invertible. Let then $\mathbf{D} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ and $\mathbf{P} = \begin{pmatrix} \mathbf{u} & \mathbf{v} \end{pmatrix}$, where the latter is given in terms of its columns. From $\mathbf{AP} = \mathbf{PD}$, by simple matrix multiplication, we have that

$$\begin{pmatrix} \mathbf{Au} & \mathbf{Av} \end{pmatrix} = \mathbf{AP} = \mathbf{PD} = \begin{pmatrix} \lambda\mathbf{u} & \mu\mathbf{v} \end{pmatrix},$$

and so we arrive at the necessary condition that

$$\mathbf{Au} = \lambda\mathbf{u} \text{ and } \mathbf{Av} = \lambda\mathbf{v}$$

and since we want $\mathbf{u}$ and $\mathbf{v}$ to be independent, in particular we must have that $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{v} \neq \mathbf{0}$.

Thus, this simply we have arrived at the definition of eigenvalue and eigenvector.

Let $\mathbf{M}$ be a square matrix, and let $\mathbf{w}$ be a nonzero vector. Then $\mathbf{w}$ is said to be an **eigenvector** of $\mathbf{M}$ with corresponding **eigenvalue** α (just a scalar) if

$$\mathbf{Mw} = \alpha\mathbf{w}.$$

Next, how do we find these eigenvector and eigenvalues? If $\mathbf{Mw} = \alpha\mathbf{w}$, then $\mathbf{Mw} = \alpha\mathbf{Iw}$, so $(\mathbf{M} - \alpha\mathbf{I})\mathbf{w} = \mathbf{0}$, and since we want $\mathbf{w} \neq \mathbf{0}$, we must have that the matrix $\mathbf{M} - \alpha\mathbf{I}$ is not invertible, and then $\mathbf{w} \in \mathrm{N}(\mathbf{M} - \alpha\mathbf{I})$.

So to find eigenvalues for a matrix $\mathbf{M}$, we needed to find scalars λ so that the matrix $\mathbf{M} - \lambda\mathbf{I}$ is not invertible, or equivalently, $\det(\mathbf{M} - \lambda\mathbf{I}) = 0$. This leads to the notion of the **characteristic polynomial** of a matrix, which is simply defined as $\det(\mathbf{M} - x\mathbf{I}) = 0$ where we now consider x to be the typical polynomial unknown. We will use $c_{\mathbf{M}}(x)$ to denote the characteristic polynomial of $\mathbf{M}$.

After one has found eigenvalues, then one easily finds eigenvectors by computing null spaces of the appropriate matrices. In fact, if λ is an eigenvalue for the matrix $\mathbf{M}$, then the null space of $\mathbf{M} - \lambda\mathbf{I}$, $\mathrm{N}(\mathbf{M} - \lambda\mathbf{I})$, is called the **eigenspace** corresponding to that eigenvalue. Every vector in it except the zero vector is an eigenvector.

Returning to the Fibonacci example, we need a λ such that $\mathbf{A} - \lambda\mathbf{I} = \begin{pmatrix} 1-\lambda & 1 \\ 1 & -\lambda \end{pmatrix}$ is not invertible. But that is equivalent to λ being a root of the characteristic polynomial

$$c_{\mathbf{A}}(x) = \det(\mathbf{A} - x\mathbf{I}) = \det\begin{pmatrix} 1-x & 1 \\ 1 & -x \end{pmatrix} = -1 - x + x^2.$$

The roots of this polynomial are $\lambda=\frac{1+\sqrt{5}}{2}$ and $\mu=\frac{1-\sqrt{5}}{2}$, so these two numbers are the eigenvalues of the matrix $\mathbf{A}=\begin{pmatrix}1&1\\1&0\end{pmatrix}$. Those historically minded will recognize these two numbers as being connected with the **Golden Ratio**, $\lambda\approx 1.6180$ and $\mu\approx -0.6180$.

To find eigenvectors, we need to find vectors in $\mathbf{N}(\mathbf{A}-\lambda\mathbf{I})$ and $\mathbf{N}(\mathbf{A}-\mu\mathbf{I})$. Of course, once we find one eigenvector, any multiple of it would also work since we know the null space of any matrix is a subspace. But as it turns out each eigenvalue can only provide one column of the matrix $\mathbf{P}$ since although there are infinitely many vectors in each null space, each is populated with multiples of only one vector, they are 1-dimensional.

So we need the null space of $\mathbf{A}-\lambda\mathbf{I}=\begin{pmatrix}1-\lambda&1\\1&-\lambda\end{pmatrix}$, and since we know the rank of this matrix has to be 1 (it is not invertible), we can immediately write its reduced form without any work: $\begin{pmatrix}1&-\lambda\\0&0\end{pmatrix}$, and so the vector $\begin{pmatrix}\lambda\\1\end{pmatrix}$ is an eigenvector for $\mathbf{A}$ with corresponding eigenvalue λ. Equivalently, we could have verified that

$$\mathbf{A}\begin{pmatrix}\lambda\\1\end{pmatrix}=\begin{pmatrix}\lambda+1\\\lambda\end{pmatrix}=\lambda\begin{pmatrix}\lambda\\1\end{pmatrix}.$$

Just as easily, we could have found $\begin{pmatrix}\mu\\1\end{pmatrix}$ to be an eigenvector for $\mathbf{A}$ for the eigenvalue μ.

Let $\mathbf{P}=\begin{pmatrix}\lambda&\mu\\1&1\end{pmatrix}$. Then $\mathbf{P}^{-1}=\frac{1}{\sqrt{5}}\begin{pmatrix}1&-\mu\\-1&\lambda\end{pmatrix}$, and by construction,

$$\mathbf{P}^{-1}\mathbf{A}\mathbf{P}=\mathbf{D}=\begin{pmatrix}\lambda&0\\0&\mu\end{pmatrix}.$$

So

$$\mathbf{A}^n=\mathbf{P}\mathbf{D}^n\mathbf{P}^{-1}=\frac{1}{\sqrt{5}}\begin{pmatrix}\lambda^{n+1}-\mu^{n+1}&\lambda\mu^{n+1}-\lambda^{n+1}\mu\\\lambda^n-\mu^n&\lambda\mu^n-\lambda^n\mu\end{pmatrix}.$$

Since $\mathbf{u}_n=\mathbf{A}^n\begin{pmatrix}1\\0\end{pmatrix}=\frac{1}{\sqrt{5}}\begin{pmatrix}\lambda^{n+1}-\mu^{n+1}\\\lambda^n-\mu^n\end{pmatrix}$, we get

$$F_n=\frac{\lambda^n-\mu^n}{\sqrt{5}}.$$

Moreover since $|\mu|<1$, we know that $\mu^n\to 0$ for larger n, so we can simply say that F_n is the nearest integer to $F_n\approx\frac{\lambda^n}{\sqrt{5}}$. So for example,

$$F_{25} \approx \frac{\lambda^{25}}{\sqrt{5}} = \frac{167761.000006}{\sqrt{5}} = 75024.99999$$

and we can readily claim that $F_{25} = 75025$, as is indeed the case.

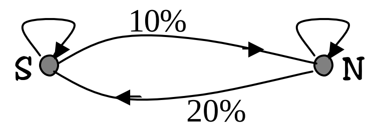
Also we can see that, $\dfrac{F_n}{F_{n+1}} = \dfrac{\lambda^n - \mu^n}{\lambda^{n+1} - \mu^{n+1}}$, but since $\lim\limits_{n\to\infty} \mu^n = 0$,

$$\lim_{n\to\infty} \frac{F_n}{F_{n+1}} = \frac{1}{\lambda} = \frac{\sqrt{5}-1}{2},$$

another of the forms of the **Golden Ratio**—a fact that Fibonacci himself discovered and was proud of.

Now we examine another example—**Example 5** from Section ❶. This example was closely associated to the graphs and digraphs that have been previously discussed—except that now after a discrete (and well defined) moment in time, one will move from one vertex to (possibly) another one with certain probabilities. The key assumption is that these probabilities do not change as we travel in time through the network. Such a process is called a (finite) **Markov chain**.

Example 5 Revisited. Every year, 10% of the people in Southern California move to Northern California while 20% of the people from Northern California move to Southern California. Assuming the total population is a constant, what is the long-range behavior of the population? In this case, our digraph is very simple:



The associated matrix with this example was $\mathbf{A} = \begin{pmatrix} 0.9 & 0.1 \\ 0.2 & 0.8 \end{pmatrix}$ where at each entry one places the probability of going from the row to the column in one transition—hence the name **transition matrix**.

Then what does $\mathbf{A}^2 = \begin{pmatrix} .83 & .17 \\ .34 & .66 \end{pmatrix}$ represent? Just as in the graph case, it represents the probabilities of going from one stage to the other but in a period of two years, not 1. Thus, 17% from Southern California will move to Northern California in two-years while 34% will move from Northern California to Southern, or viewed in another way, the probability that a random Southern Californian will be in Northern California in two years is 17%. Similarly, $\mathbf{A}^3 = \begin{pmatrix} .781 & .219 \\ .438 & .562 \end{pmatrix}$ would represent the probabilities in 3 years—thus a resident in Southern California at present has probability .781 of being there in 3 years.

The long-range behavior of the process would then be determined by the matrix

$$\mathbf{A}^\infty = \lim_{n\to\infty} \mathbf{A}^n .$$

How could we compute this? By suing eigenvalues and eigenvectors, for if $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{D}$, then as before

$$\mathbf{A}^n = \mathbf{P}\mathbf{D}^n\mathbf{P}^{-1}$$

so, by taking limits,

$$\mathbf{A}^\infty = \mathbf{P}\mathbf{D}^\infty\mathbf{P}^{-1}.$$

So we pursue the eigenvalues and eigenvectors of $\mathbf{A} = \begin{pmatrix} 0.9 & 0.1 \\ 0.2 & 0.8 \end{pmatrix}$. Now, easily $\mathbf{A}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, so we know that 1 is an eigenvalue, and an eigenvector for that eigenvalue is $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. This occurred because the row sums of $\mathbf{A}$ where all the same, 1 in this case. But this eigenvalue can only provide one column of the matrix $\mathbf{P}$.

So we need to search for another value. The characteristic polynomial of $\mathbf{A}$, *i.e.*, the determinant of $\mathbf{A} - x\mathbf{I} = \begin{pmatrix} .9 - x & .1 \\ .2 & .8 - x \end{pmatrix}$ equals

$$c_{\mathbf{A}}(x) = (.9 - x)(.8 - x) - .02 = .7 - 1.7x + x^2 ,$$

and the roots of this quadratic are 1 (which we already knew) and 0.7. Now we need an eigenvector for the latter, so we need to find the null space of $\mathbf{A} - .7\mathbf{I} = \begin{pmatrix} .2 & .1 \\ .2 & .1 \end{pmatrix}$, which again is 1-dimensional, with basis $\begin{pmatrix} 1 \\ -2 \end{pmatrix}$. Thus, we are now ready to write $\mathbf{P} = \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}$, which is clearly invertible ($\det \mathbf{P} = -3$), and satisfies

$$\mathbf{A}\mathbf{P} = \begin{pmatrix} .9 & .1 \\ .2 & .8 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & .7 \\ 1 & -1.4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & .7 \end{pmatrix} = \mathbf{P}\mathbf{D} ,$$

and so we have that

$$\mathbf{A}^n = \mathbf{P}\mathbf{D}^n\mathbf{P}^{-1} .$$

Taking limits as $n \to \infty$, since $(.7)^n \to 0$, we get that $\mathbf{D}^n \to \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, so

$$\mathbf{A}^\infty = \lim_{n\to\infty} \mathbf{A}^n = \mathbf{P}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\mathbf{P}^{-1} = \frac{1}{3}\begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}.$$

So in the long run, this model would predict that $\frac{2}{3}$ of the population would live in Southern California.

Note that if we had started with the population being distributed that way, namely $\frac{2}{3}$ in Southern California and $\frac{1}{3}$ in Northern California, then the following year, since 10% of $\frac{2}{3}$ is the same as 20% of $\frac{1}{3}$, we would have that although the actual people living on each side of the state would change, the numbers would not. Namely we would arrive at a stable situation. And actually, since the powers of $\mathbf{A}$ do have a limit, no matter what population we start with, we will tend to that stable $\frac{2}{3}$ vs. $\frac{1}{3}$ population split. The following various starting positions and their evolutions through 12 years confirm our expectations:

	SC	NC	SC	NC	SC	NC	SC	NC
0	0.000%	100.000%	100.000%	0.000%	50.000%	50.000%	20.000%	80.000%
1	20.000%	80.000%	90.000%	10.000%	55.000%	45.000%	34.000%	66.000%
2	34.000%	66.000%	83.000%	17.000%	58.500%	41.500%	43.800%	56.200%
3	43.800%	56.200%	78.100%	21.900%	60.950%	39.050%	50.660%	49.340%
4	50.660%	49.340%	74.670%	25.330%	62.665%	37.335%	55.462%	44.538%
5	55.462%	44.538%	72.269%	27.731%	63.866%	36.135%	58.823%	41.177%
6	58.823%	41.177%	70.588%	29.412%	64.706%	35.294%	61.176%	38.824%
7	61.176%	38.824%	69.412%	30.588%	65.294%	34.706%	62.823%	37.177%
8	62.823%	37.177%	68.588%	31.412%	65.706%	34.294%	63.976%	36.024%
9	63.976%	36.024%	68.012%	31.988%	65.994%	34.006%	64.783%	35.217%
10	64.783%	35.217%	67.608%	32.392%	66.196%	33.804%	65.348%	34.652%
11	65.348%	34.652%	67.326%	32.674%	66.337%	33.663%	65.744%	34.256%
12	65.744%	34.256%	67.128%	32.872%	66.436%	33.564%	66.021%	33.979%

In a similar situation previously, we looked at the following problem

Example 2. In Orangerock Park, the female deer population can be classified into three groups: **young**, **mature** and **old**. Every year, 30% of the young population matures, and 5% dies, while the rest remains classified as young. Of the mature population, 25% changes to old, another 25% gives birth to young, and 15% dies. Of the group of old, 50% dies every year. Suppose the vector $\mathbf{u}=\begin{pmatrix}120\\200\\80\end{pmatrix}$ represents the number of deer in each of the three respective categories, young, mature and old. If we then let $\mathbf{A}=\begin{pmatrix}.65 & .25 & 0\\ .3 & .60 & 0\\ 0 & .25 & .5\end{pmatrix}$, then $\mathbf{Au}=\begin{pmatrix}128\\156\\90\end{pmatrix}$, would represent the population next year, and then $\mathbf{A}^2\mathbf{u}$, $\mathbf{A}^3\mathbf{u}$, $\mathbf{A}^4\mathbf{u}$, … would represent the populations in the consequent years, so again the powers of $\mathbf{A}$ become relevant, and so do the eigenvalues.

Again, to find eigenvalues we need to look for roots of the characteristic polynomial:

$$c_{\mathbf{A}}(x)=\det(\mathbf{A}-x\mathbf{I})=\det\begin{pmatrix}.65-x & .25 & 0\\ .3 & .6-x & 0\\ 0 & .25 & .5-x\end{pmatrix},$$

and expanding this determinant by the third column, we get $(.5-x)\det\begin{pmatrix}.65-x & .25\\ .3 & .6-x\end{pmatrix}$, which equals $(.5-x)(.315-1.25x+x^2)=(.5-x)(x-.9)(x-.35)$, and so we have 3 eigenvalues for **A**, they are .35, .50 and .90. As it turns out, in this case we will be able to find a matrix **P** such that $\mathbf{P}^{-1}\mathbf{AP}$ is diagonal by finding an eigenvector for each of the eigenvalues. As before this is tantamount to finding some null spaces.

For the eigenvalue $\lambda = .35$, $\mathbf{A} - .35\mathbf{I} = \begin{pmatrix} .3 & .25 & 0 \\ .3 & .25 & 0 \\ 0 & .25 & .15 \end{pmatrix}$, and a basis for its null space is $\begin{pmatrix} 5 \\ -6 \\ 10 \end{pmatrix}$, while for $\lambda = .5$, $\mathbf{A} - .5\mathbf{I} = \begin{pmatrix} .15 & .25 & 0 \\ .3 & .1 & 0 \\ 0 & .25 & 0 \end{pmatrix}$ and its null space is spanned by $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Finally for $\lambda = .9$, $\mathbf{A} - .9\mathbf{I} = \begin{pmatrix} -.25 & .25 & 0 \\ .3 & -.3 & 0 \\ 0 & .25 & -.4 \end{pmatrix}$, and an eigenvector is $\begin{pmatrix} 8 \\ 8 \\ 5 \end{pmatrix}$.

Thus if we let $\mathbf{P} = \begin{pmatrix} 5 & 0 & 8 \\ -6 & 0 & 8 \\ 10 & 1 & 5 \end{pmatrix}$, then we have that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D} = \begin{pmatrix} .35 & 0 & 0 \\ 0 & .5 & 0 \\ 0 & 0 & .9 \end{pmatrix}$. Of course, if we had permuted the columns of **P**, or multiplied them by scalars, since a multiple of an eigenvector is an eigenvector, this would result in the corresponding permutation of the entries in **D**. *E.g.*, if we take $\mathbf{Q} = \begin{pmatrix} 0 & -8 & 10 \\ 0 & -8 & -12 \\ 1 & -5 & 20 \end{pmatrix}$, then $\mathbf{Q}^{-1}\mathbf{AQ} = \mathbf{D} = \begin{pmatrix} .5 & 0 & 0 \\ 0 & .9 & 0 \\ 0 & 0 & .35 \end{pmatrix}$.

Note that since $\mathbf{D}^{\infty} = \mathbf{0}$, we will also have that $\mathbf{A}^{\infty} = \mathbf{0}$, so the population of deer will disappear in the long run, regardless of the present population.

The previous three examples illustrated some of the uses of eigenvalues and eigenvectors. Let us review what we have learned.

Suppose **A** is a square matrix. If we are to find a **P** such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{D}$, a diagonal matrix, then we know the columns of **P** are eigenvectors of **A** while the diagonal entries of **D** are the corresponding eigenvalues. That fact itself motivated the definition of eigenvalues and eigenvectors, characteristic polynomial and eigenspace. Alas, it will not be true that we will be able to find such a **P** for an arbitrary matrix **A**—but one can come close.

First we develop further understanding of the key notions of eigenvalue and eigenvector, and their connections with the powers of a matrix.

Theorem (Easy Eigenvalues). Let **A** be $n \times n$. Let **u** be an eigenvector for **A** with corresponding eigenvector λ. Then the following are true:

① **u** is an eigenvector for $\mathbf{A}^2$ with corresponding eigenvalue λ^2.

② If a is any scalar, then $\mathbf{u}$ is an eigenvector for $a\mathbf{A}$ with corresponding eigenvalue $a\lambda$.

③ If $p(x)$ is an arbitrary polynomial, then $\mathbf{u}$ is an eigenvector for $p(\mathbf{A})$ with corresponding eigenvalue $p(\lambda)$.

④ If $\mathbf{A}$ is invertible, then $\lambda \neq 0$, and $\mathbf{u}$ is an eigenvector for $\mathbf{A}^{-1}$ with corresponding eigenvalue $\frac{1}{\lambda}$.

Proof. It is given that $\mathbf{Au} = \lambda\mathbf{u}$, so $\mathbf{A}(\mathbf{Au}) = \mathbf{A}(\lambda\mathbf{u}) = \lambda\mathbf{Au} = \lambda(\lambda\mathbf{u}) = \lambda^2\mathbf{u}$, and we have ①. In fact, ② and ③ are very similar. Assume now that $\mathbf{A}$ is invertible. Since $\mathbf{Au} = \lambda\mathbf{u}$, $\mathbf{A}^{-1}(\mathbf{Au}) = \mathbf{A}^{-1}(\lambda\mathbf{u})$, so $\mathbf{u} = \lambda\mathbf{A}^{-1}\mathbf{u}$, and since $\mathbf{u} \neq \mathbf{0}$, $\lambda \neq 0$, and then $\mathbf{A}^{-1}\mathbf{u} = \frac{1}{\lambda}\mathbf{u}$, and we have ④. ⌘

Example 3. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 4 & -3 \\ 2 & -1 & 5 \end{pmatrix}$. Then $\mathbf{u} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ is an eigenvector for the eigenvalue 6 since $\mathbf{Au} = 6\mathbf{u}$. Now $\mathbf{A}^2 = \begin{pmatrix} 17 & 7 & 12 \\ 19 & 29 & -12 \\ 7 & -5 & 34 \end{pmatrix}$ has the same eigenvector with the eigenvalue 36, and $-2\mathbf{A} = \begin{pmatrix} -2 & -4 & -6 \\ -10 & -8 & 6 \\ -4 & 2 & -10 \end{pmatrix}$'s eigenvalue for the vector is -12. Similarly,

$$\mathbf{A}^3 + 2\mathbf{A}^2 - 50\mathbf{A} + 12\mathbf{I} = \begin{pmatrix} 72 & -36 & -36 \\ -72 & 36 & 36 \\ -36 & 0 & 36 \end{pmatrix}$$

has 0 as the eigenvalue corresponding to $\mathbf{u}$ since $6^3 + 2\times 6^2 - 50\times 6 + 12 = 0$. Finally, $\mathbf{A}^{-1} = \frac{1}{84}\begin{pmatrix} -17 & 13 & 18 \\ 31 & 1 & -18 \\ 13 & -5 & 6 \end{pmatrix}$ satisfies $\mathbf{A}^{-1}\mathbf{u} = \frac{1}{6}\mathbf{u}$.

Note that in the previous example we did not pursue the computation of the whole set of eigenvalues, nor of the characteristic polynomial, these sometimes are not necessary. In general, the computation of the characteristic polynomial is rather nontrivial, although great strides have been accomplished in the last decades through the use of computers and calculators. And in actuality, it is not the characteristic polynomial of a matrix that is as interesting as the roots of that polynomial, the eigenvalues of the matrix, and its corresponding eigenvectors. Induction easily does the first part of the following:

Theorem. Let $\mathbf{A}$ be an $n \times n$ matrix, and let $c_{\mathbf{A}}(x) = \det(\mathbf{A} - x\mathbf{I})$ be its characteristic polynomial. Then

① $c_{\mathbf{A}}(x)$ is a polynomial of degree *n*, and the coefficient of the highest order term is $(-1)^n$.

② Its roots $\lambda_1, \lambda_2, \ldots, \lambda_n$ are exactly the eigenvalues of $\mathbf{A}$, and

$$\det \mathbf{A} = \prod_{i=1}^{n} \lambda_i .$$

Proof. Only the last remark deserves to be proven. We have

$$c_{\mathbf{A}}(x) = \det(\mathbf{A} - x\mathbf{I}) = (\lambda_1 - x)(\lambda_2 - x)\cdots(\lambda_n - x),$$

so if we let $x = 0$, we get $\det \mathbf{A} = \prod_{i=1}^{n} \lambda_i$. ⌘

In words then,

the determinant of a matrix is the product of its eigenvalues.

One uses the word **spectrum** to denote the complete list of eigenvalues of a matrix. Naturally, an $n \times n$ matrix will have *n* elements in its spectrum—but as we will see below some of them may have to be complex numbers.

Another function that is of intense interest is the **trace** of a matrix, which is defined as the sum of the entries of the main diagonal of a matrix. We will let $\operatorname{tr}\mathbf{A}$ denote the trace, and a wonderful fact easily obtained from polynomials (and proven below) is that the

the trace of a matrix is the sum of its eigenvalues.

Also true is that the trace is the coefficient of x^{n-1} in the characteristic polynomial, multiplied by $(-1)^{n-1}$.

Example 4. Let $\mathbf{A} = \mathbf{I}_n$, the identity matrix. Then clearly, $c_{\mathbf{A}}(x) = (1-x)^n$, so all of its eigenvalues are 1, and we say of multiplicity *n*, since 1 is a root of the polynomial that many times. The spectrum of $\mathbf{I}$ is 1, *n* times.

Example 5. Let us now consider $\mathbf{A} = \mathbf{J}_n$, the matrix of all 1's. Clearly, if $n = 2$, then $c_{\mathbf{J}_2}(x) = (1-x)^2 - 1 = x(x-2)$. So its spectrum is 2 and 0.

Let us consider $\det\begin{pmatrix} 1-x & 1 & 1 \\ 1 & 1-x & 1 \\ 1 & 1 & 1-x \end{pmatrix}$. If we add the bottom two rows to the first row (which does not alter the determinant), we get the matrix $\begin{pmatrix} 3-x & 3-x & 3-x \\ 1 & 1-x & 1 \\ 1 & 1 & 1-x \end{pmatrix}$, and so $c_{\mathbf{J}_3}(x) = (3-x)\det\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1-x & 1 \\ 1 & 1 & 1-x \end{pmatrix}$, but by subtracting the first column from the other two columns, we have then $c_{\mathbf{J}_3}(x) = (3-x)\det\begin{pmatrix} 1 & 0 & 0 \\ 1 & -x & 0 \\ 1 & 0 & -x \end{pmatrix}$, which by expanding on the first row then gives $c_{\mathbf{J}_3}(x) = (3-x)x^2$, so the eigenvalues of $\mathbf{J}_3$ are 3 (with multiplicity 1) and 0 with multiplicity 2, or equivalently, its spectrum is 3, 0 and 0. This argument should look familiar.

The similar technique of adding all the rows to the first row, and pulling out the $n-x$ term from the first row, and then subtracting the first column from every other column, we get that the characteristic polynomial of $\mathbf{J}_n$ is given by $(n-x)x^{n-1}(-1)^{n-1}$, and so its spectrum is n (of multiplicity 1) and 0 (of multiplicity $n-1$).

Note that the determinant and trace facts are easily verified in the two examples just given. But they are particularly transparent in the following important generic example:

Example 6. Eigenvalues and Upper Triangulars. In fact the eigenvalues in this case are easily observable, **the eigenvalues of any triangular matrix are its diagonal entries**:

$$\text{if } \mathbf{A} = \begin{pmatrix} a_{11} & * & \cdots & * \\ 0 & a_{22} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}, \text{ then } \mathbf{A} - x\mathbf{I} = \begin{pmatrix} a_{11}-x & * & \cdots & * \\ 0 & a_{22}-x & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn}-x \end{pmatrix}, \text{ so}$$

$$c_{\mathbf{A}}(x) = \det(\mathbf{A} - x\mathbf{I}) = (a_{11}-x)(a_{22}-x)\cdots(a_{nn}-x).$$

Also notice that as further clarification of the **Easy Eigenvalues Theorem** above, the diagonal entries of $\mathbf{A}^2$ are the squares of the diagonal entries of A, and since $\mathbf{A}^2$ is also upper triangular, we see that these squares are then the eigenvalues of $\mathbf{A}^2$. Similarly for the inverse

> **Theorem (Spectrum of Inverse).** Let $\mathbf{A}$ be $n \times n$. Then $\mathbf{A}$ is invertible if and only if none of its eigenvalues is 0. If this is the case, and $\lambda_1, \lambda_2, \ldots, \lambda_n$ is the spectrum of $\mathbf{A}$, then $\frac{1}{\lambda_1}, \frac{1}{\lambda_2}, \ldots, \frac{1}{\lambda_n}$ is the spectrum of $\mathbf{A}^{-1}$.

Proof. The first claim follows immediately from the connection between eigenvalues and the determinant. But it can also be seen directly, since a matrix is not invertible if and only if it has a nontrivial null space, and that is equivalent to having an eigenvector for the eigenvalue 0. Now, $c_{\mathbf{A}}(x) = (\lambda_1 - x)(\lambda_2 - x)\cdots(\lambda_n - x) = \det(\mathbf{A} - x\mathbf{I})$. But then $\det\left(\mathbf{A} - \frac{1}{x}\mathbf{I}\right) = \left(\lambda_1 - \frac{1}{x}\right)\left(\lambda_2 - \frac{1}{x}\right)\cdots\left(\lambda_n - \frac{1}{x}\right)$. Also $\det\left(x\mathbf{A}^{-1}\right) = \frac{x^n}{\lambda_1\lambda_2\cdots\lambda_n}$, and thus

$$\det\left(\mathbf{A}^{-1} - x\mathbf{I}\right) = \det\left(\left(x\mathbf{A}^{-1}\right)\left(\frac{1}{x}\mathbf{I} - \mathbf{A}\right)\right) =$$

$$\det\left(x\mathbf{A}^{-1}\right)\det\left(\frac{1}{x}\mathbf{I} - \mathbf{A}\right) = \frac{x^n}{\lambda_1\lambda_2\cdots\lambda_n}(-1)^n\left(\lambda_1 - \frac{1}{x}\right)\left(\lambda_2 - \frac{1}{x}\right)\cdots\left(\lambda_n - \frac{1}{x}\right) =$$

$$(-1)^n\left(x - \frac{1}{\lambda_1}\right)\left(x - \frac{1}{\lambda_2}\right)\cdots\left(x - \frac{1}{\lambda_n}\right) = \left(\frac{1}{\lambda_1} - x\right)\left(\frac{1}{\lambda_2} - x\right)\cdots\left(\frac{1}{\lambda_n} - x\right)$$

and the claim is proven. ⌘

Example 7. Let $\mathbf{A} = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$. Then since $\mathbf{A}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 4 \end{pmatrix}$, 4 is an eigenvalue. By the trace, the other eigenvalue has to be -2. Now, $\mathbf{A}^{-1} = \begin{pmatrix} \frac{-1}{8} & \frac{3}{8} \\ \frac{3}{8} & \frac{-1}{8} \end{pmatrix}$, and the eigenvectors of this matrix are $\frac{1}{4}$ and $\frac{-1}{2}$.

Example 3 Revisited. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 4 & -3 \\ 2 & -1 & 5 \end{pmatrix}$. Then we already know that 6 is an eigenvalue. We have $\det\mathbf{A} = -84$ and $\operatorname{tr}\mathbf{A} = 10$. So if we let λ and μ be the other two eigenvalues, we must have that $6\lambda\mu = -84$ and $6 + \lambda + \mu = 10$, or equivalently $\lambda\mu = -14$ and $\lambda + \mu = 4$. By simple algebra, we get that the spectrum of $\mathbf{A}$ is 6, $2 + 3\sqrt{2}$ and $2 - 3\sqrt{2}$. Thus the spectrum of $\mathbf{A}^{-1} = \frac{1}{84}\begin{pmatrix} -17 & 13 & 18 \\ 31 & 1 & -18 \\ 13 & -5 & 6 \end{pmatrix}$ consists of $\frac{1}{6}$, $\frac{1}{2 + 3\sqrt{2}} = \frac{3\sqrt{2} - 2}{14}$ and $\frac{1}{2 - 3\sqrt{2}} = \frac{-3\sqrt{2} - 2}{14}$. Note for example that the trace condition is easily verified: $\frac{1}{6} - \frac{4}{14} = \frac{-5}{42}$.

As a trivial consequence of a fact about determinants, we get an interesting consequence about eigenvalues.

Theorem (Eigenvalues and Upper Triangular Form). Let $\mathbf{M}=\begin{pmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{0} & \mathbf{C}\end{pmatrix}$ be in balanced block upper triangular form. Then $c_{\mathbf{M}}(x)=c_{\mathbf{A}}(x)c_{\mathbf{C}}(x)$. Thus, the spectrum of $\mathbf{M}$ is the union of the two spectra of $\mathbf{A}$ and $\mathbf{C}$.

Proof. By the determinant fact, $\det(\mathbf{M}-x\mathbf{I})=\det(\mathbf{A}-x\mathbf{I})\det(\mathbf{C}-x\mathbf{I})$, and the claim follows. ⌘

Example 8. Let $\mathbf{A}=\begin{pmatrix}2&1&3&4&5&6\\1&2&7&8&9&2\\0&0&3&1&5&6\\0&0&1&3&7&8\\0&0&0&0&4&1\\0&0&0&0&1&4\end{pmatrix}$. Then we can see this as a 3×3 block upper triangular, and so the eigenvalues are the eigenvalues of $\begin{pmatrix}2&1\\1&2\end{pmatrix}$ which are 3 and 1 (look at the row sum, and hence the eigenvector $\begin{pmatrix}1\\1\end{pmatrix}$), and $\begin{pmatrix}3&1\\1&3\end{pmatrix}$ of spectrum 4 and 2, and finally, 5 and 3 which are the eigenvalues of $\begin{pmatrix}4&1\\1&4\end{pmatrix}$. Observe that although the blocks here were of the same size, that was not at all required, rather what was needed was that the diagonal blocks be square.

Example 9. *Geometry and Eigenvectors.* In this example, we explore some of the geometric meaning of eigenvector (and eigenvalue). We concentrate in the plane to start with since this is easiest to visualize. Consider first $\mathbf{A}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, which we saw before was the reflection on the $y=x$ line. But then clearly, we already have an eigenvector, $\begin{pmatrix}1\\1\end{pmatrix}$ which is on the line of the reflection, so it is a fixed point, and hence an eigenvector of eigenvalue 1. The other obvious eigenvector is $\begin{pmatrix}1\\-1\end{pmatrix}$ and for this one $\begin{pmatrix}1\\-1\end{pmatrix}\mapsto\begin{pmatrix}-1\\1\end{pmatrix}$, so the eigenvalue is -1. This example illustrates very clearly the import of eigenvectors from the geometrical point of view. The **search for eigenvectors is the search for lines that get mapped to themselves** as the matrix transforms the vector space. In the reflection case, the two lines are very obvious, the line of reflection and the line perpendicular to it (both through the origin of course, since we are discussing subspaces).

To confirm our suspicions, consider the reflection on the line $3x+4y=0$. As we saw before, this reflection is accomplished by the matrix $\mathbf{A}=\mathbf{I}-2\mathbf{u}\mathbf{u}^{\mathrm{T}}$ where $\mathbf{u}$ is a unit normal to the line, which in this case we can take $\mathbf{u} = \frac{1}{5}\begin{pmatrix} 3 \\ 4 \end{pmatrix}$, and so $\mathbf{A} = \frac{1}{25}\begin{pmatrix} 7 & -24 \\ -24 & -7 \end{pmatrix}$. Readily, $\begin{pmatrix} -4 \\ 3 \end{pmatrix}$ is an eigenvector with eigenvalue 1, and $\begin{pmatrix} 3 \\ 4 \end{pmatrix}$ is also with eigenvalue -1. Just as expected.

Example 10. Nasty Issues. With better understanding under our belt, we can see that some matrices will not have eigenvalues (real eigenvalues, that is). In particular if we take any rotation, because of the geometric nature of the transformation, there should not be any lines that are fixed, and thus there should not be any eigenvalues. For example, let $\mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, which is 90°-rotation. Its characteristic polynomial is $x^2 + 1$, the most notorious of polynomials without a real root. Of course, if we consider complex numbers, this matrix has two eigenvalues $\mathbf{i}$ and $-\mathbf{i}$, and corresponding eigenvectors: $\begin{pmatrix} 1 \\ -\mathbf{i} \end{pmatrix}$ and $\begin{pmatrix} 1 \\ \mathbf{i} \end{pmatrix}$. Observe that the trace and determinant condition still hold in this case, namely the sum of the eigenvalues is 0, which is the trace, and the product is 1, which is the determinant.

Thus if we will claim that the spectrum of an $n \times n$ matrix has n numbers in it, we would have to extend our view of number to include the whole set of complex numbers. We will not do that in this course, since we will concentrate on matrices that have real eigenvalues.

❶❺ Triangularization & Diagonalization

In the last section we saw that for a given matrix $\mathbf{A}$ it would be desirable if we could find matrices invertible $\mathbf{P}$ and diagonal $\mathbf{D}$ so that $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{D}$. It was within this pursuit that the fundamental concepts of eigenvalue and eigenvector were developed. So we now formalize this relation.

Let $\mathbf{A}$ and $\mathbf{B}$ be square matrices. They are said to be **similar** if there is an invertible matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{B}$. This definition does not seem balanced in the sense we could almost say that instead of $\mathbf{A}$ and $\mathbf{B}$ being similar, we should refer to $\mathbf{A}$ being similar to $\mathbf{B}$. But this superficial asymmetry is remedied easily, since if $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{B}$, then $\mathbf{Q}^{-1}\mathbf{BQ}=\mathbf{A}$, where $\mathbf{Q}=\mathbf{P}^{-1}$.

A matrix is called **diagonable** if it is similar to a diagonal matrix. Thus, in the 3 examples at the beginning of the previous section, our matrices were all diagonable. That will not always be the case, as some examples will show below. A matrix is called **triangularizable** if it is similar to a triangular matrix. We will see below that although every matrix is not diagonable, every matrix is triangularizable.

First we make a simple observation about the trace of a product:

Let $\mathbf{M}$ be $m\times n$ and let $\mathbf{N}$ be $n\times m$. Then $\operatorname{tr}(\mathbf{MN})=\operatorname{tr}(\mathbf{NM})$.

The reason is simple bookkeeping:

$$\operatorname{tr}(\mathbf{MN})=\sum_{i=1}^{m}(\mathbf{MN})_i=\sum_{i=1}^{m}\sum_{k=1}^{n}m_{ik}n_{ki}=\sum_{i=1}^{m}\sum_{k=1}^{n}n_{ki}m_{ik}=\sum_{k=1}^{n}\sum_{i=1}^{m}n_{ki}m_{ik}=\sum_{k=1}^{n}(\mathbf{NM})_k=\operatorname{tr}(\mathbf{NM}).$$

Example 1. Let $\mathbf{M}=\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}$, and let $\mathbf{N}=\begin{pmatrix}a&b\\c&d\\e&f\end{pmatrix}$. Now $\mathbf{MN}=\begin{pmatrix}a+2c+3e & b+2d+3f\\4a+5c+6e & 4b+5d+6f\end{pmatrix}$ is 2×2 of trace $a+2c+3e+4b+5d+6f$ while $\mathbf{NM}=\begin{pmatrix}a+4b&2a+5b&3a+6b\\c+4d&2c+5d&3c+6d\\e+4f&2e+5f&3e+6f\end{pmatrix}$ is 3×3 of the same trace.

Theorem (Similarity). Let $\mathbf{A}$ and $\mathbf{B}$ be similar. Then the following are true.

① $c_{\mathbf{A}}(x)=c_{\mathbf{B}}(x)$, *i.e.*, $\mathbf{A}$ and $\mathbf{B}$ have the same characteristic polynomial.

In particular,

② $\det\mathbf{A}=\det\mathbf{B}$

and

③ $\operatorname{tr}\mathbf{A}=\operatorname{tr}\mathbf{B}$.

Proof. Suppose $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{B}$, so $\mathbf{P}^{-1}\mathbf{AP}-x\mathbf{I}=\mathbf{B}-x\mathbf{I}$, and so $\mathbf{P}^{-1}\mathbf{AP}-x\mathbf{P}^{-1}\mathbf{IP}=\mathbf{B}-x\mathbf{I}$, hence $\mathbf{P}^{-1}(\mathbf{A}-x\mathbf{I})\mathbf{P}=\mathbf{B}-x\mathbf{I}$, and so $\det\left(\mathbf{P}^{-1}(\mathbf{A}-x\mathbf{I})\mathbf{P}\right)=\det(\mathbf{B}-x\mathbf{I})$, and since

$$\det\left(\mathbf{P}^{-1}(\mathbf{A}-x\mathbf{I})\mathbf{P}\right)=\det\mathbf{P}^{-1}\det(\mathbf{A}-x\mathbf{I})\det\mathbf{P},$$

we are done with ①. On the other hand by letting $x=0$, we get ②. To prove ③, we use the observation above: $\operatorname{tr}\mathbf{B}=\operatorname{tr}\left(\mathbf{P}^{-1}\mathbf{AP}\right)=\operatorname{tr}\left(\mathbf{APP}^{-1}\right)=\operatorname{tr}\mathbf{A}$. ⌘

The converse of the **Similarity Theorem** is not true. We have that if two matrices are similar, then their characteristic polynomials were the same—however, two matrices can have the same characteristic polynomial without being similar. To give the simplest example, observe that nothing but itself is similar to the zero matrix since for any $\mathbf{P}$, $\mathbf{P}^{-1}\mathbf{0P}=\mathbf{0}$. But the matrix $\mathbf{A}=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$ has the same characteristic polynomial as the zero matrix without being similar to it. Moreover, note that $\mathbf{A}$ cannot be diagonalized because if it could be diagonalized it would be to the zero matrix. However, note that $\mathbf{A}$ is upper triangular matrix already because every matrix is similar to a diagonable. But of course **the required necessity of having real eigenvalues has to be met.**

> **Theorem (Triangularity).** Let $\mathbf{A}$ have real eigenvalues. Then there exists an invertible (real) matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{T}$ is triangular. By necessity, the diagonal entries of $\mathbf{T}$ are the eigenvalues of $\mathbf{A}$.

A proof of this theorem can be found in the **Appendix of Proofs**—and a more powerful fact will be proven in a following section. However, we can argue the last part of the theorem readily: since $\mathbf{A}$ and $\mathbf{T}$ are similar, by the **Similarity Theorem**, they have the same eigenvalues, and since $\mathbf{T}$ is upper triangular, its eigenvalues are its diagonal entries.

Recall that given any polynomial, for example, $p(x)=2x^3+3x^2-5x+4$, and any square matrix $\mathbf{A}$, then $p(\mathbf{A})$ is simply $2\mathbf{A}^3+3\mathbf{A}^2-5\mathbf{A}+4\mathbf{I}$. And we have an interesting and important consequence of the theorem:

> **Corollary (Polynomials & Eigenvalues).** Let $p(x)$ be a polynomial. Let $\mathbf{A}$ be $n\times n$ with spectrum λ_1, $\lambda_2,\ldots,\lambda_n$ (not necessarily distinct). Let $\mathbf{P}$ be such that $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{T}$ where $\mathbf{T}$ is triangular. Then the following are true:
>
> ① $\mathbf{P}^{-1}p(\mathbf{A})\mathbf{P}=p(\mathbf{T})$.
>
> ② The spectrum of $p(\mathbf{A})$ consists $p(\lambda_1)$, $p(\lambda_2),\ldots,p(\lambda_n)$.

Proof. Easily $\mathbf{P}^{-1}\mathbf{A}^k\mathbf{P} = \underbrace{\left(\mathbf{P}^{-1}\mathbf{AP}\right)\left(\mathbf{P}^{-1}\mathbf{AP}\right)\cdots\left(\mathbf{P}^{-1}\mathbf{AP}\right)}_{k} = \mathbf{T}^k$. But also since for any matrices $\mathbf{X}$ and $\mathbf{Y}$ and any scalar a, $\mathbf{P}^{-1}\left(a\mathbf{X}+\mathbf{Y}\right)\mathbf{P} = a\mathbf{P}^{-1}\mathbf{XP}+\mathbf{P}^{-1}\mathbf{YP}$, ① follows. Since $p\left(\mathbf{T}\right)$ is upper triangular with $p\left(\lambda_1\right)$, $p\left(\lambda_2\right),\ldots,p\left(\lambda_n\right)$ along the main diagonal, we also have ②.⌘

The mantra: **the eigenvalues of a polynomial are the polynomial of the eigenvalues**.

Example 2. We saw before that the eigenvalues of $\mathbf{A} = \begin{pmatrix} .65 & .25 & 0 \\ .3 & .60 & 0 \\ 0 & .25 & .5 \end{pmatrix}$ are .35, .50 and .90. Thus if we take the polynomial $p\left(x\right) = 3-4x-2x^2+x^3$, then when we substitute $\mathbf{A}$, we get $p\left(\mathbf{A}\right) = \begin{pmatrix} -.178 & -1.313 & 0 \\ -1.576 & .0848 & 0 \\ -.019 & -1.304 & .625 \end{pmatrix}$ that has eigenvalues $p\left(.35\right) = 1.397875$, $p\left(.5\right) = .625$ and $p\left(.9\right) = -1.491$.

But there is another way to take advantage of this theorem and its corollary.

Example 3. Consider the following symmetric permutation matrix of size $n\times n$: $\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & ⋰ & ⋰ & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}$. Since its square is the identity, we have that all of its eigenvalues are either 1 or -1. But the trace is 0 if *n* is even, so in that case half of the eigenvalues are 1 and half of them are -1. If *n* is odd, the trace is 1 so then $\frac{n+1}{2}$ of the eigenvalues are 1 while $\frac{n-1}{2}$ of them are -1. For example, $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ has spectrum 1, 1, -1 and -1 while $\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$ has spectrum 1, 1, 1, -1 and -1.

Example 4. Consider the matrix of the Petersen graph,

$$\mathbf{A}=\begin{pmatrix}0&1&0&0&1&1&0&0&0&0\\1&0&1&0&0&0&1&0&0&0\\0&1&0&1&0&0&0&1&0&0\\0&0&1&0&1&0&0&0&1&0\\1&0&0&1&0&0&0&0&0&1\\1&0&0&0&0&0&0&1&1&0\\0&1&0&0&0&0&0&0&1&1\\0&0&1&0&0&1&0&0&0&1\\0&0&0&1&0&1&1&0&0&0\\0&0&0&0&1&0&1&1&0&0\end{pmatrix}.$$

Then by either multiplication, or from the graph theoretic point of view, we can see that this matrix satisfies $\mathbf{AJ}=\mathbf{JA}=3\mathbf{J}$ (all this means is 3 ones in each row and in each column), and more importantly $\mathbf{A}^2+\mathbf{A}=2\mathbf{I}+\mathbf{J}$. Equivalently, $\mathbf{A}^2+\mathbf{A}-2\mathbf{I}=\mathbf{J}$. But multiplying by $\mathbf{A}-3\mathbf{I}$, we get then $(\mathbf{A}-3\mathbf{I})(\mathbf{A}^2+\mathbf{A}-2\mathbf{I})=\mathbf{0}$, so if we take the polynomial $p(x)=(x-3)(x^2+x-2)$, then we know that the eigenvalues of $p(\mathbf{A})$ are all of the form $p(\lambda)$ where λ is an eigenvalue of $\mathbf{A}$. But since $p(\mathbf{A})=\mathbf{0}$, all of the eigenvalues of $p(\mathbf{A})$ are 0, so this means that $p(\lambda)=0$ for any eigenvalue λ of $\mathbf{A}$. In other words, the eigenvalues of $\mathbf{A}$ have to be roots of $p(x)=(x-3)(x^2+x-2)$. Since this polynomial has 3 roots, 3, 1 and -2, these must be the eigenvalues of $\mathbf{A}$. In fact, one can show that 3 occurs only once as an eigenvalue, and then we can figure out the multiplicity of the other two by the trace condition. Let m be the multiplicity of 1 and let n be the multiplicity of -2. Then we must have that $m+n=9$ (since $\mathbf{A}$ is 10×10 and one eigenvalue has been accounted for), but we must also have that (because of the trace) $3+m\cdot1+n(-2)=0$, and these two equations provide the unique possibility, $m=5$ and $n=4$, and so the complete spectrum of the Petersen graph is 3, once, 1, a total of 5 times, and -2, four times. Thus its determinant must be 48.

Observe we could have used a similar technique to find the spectrum of the matrix $\mathbf{J}_n$. Since $\mathbf{J}_n^2=n\mathbf{J}_n$, the eigenvalues of $\mathbf{J}_n$ have to satisfy the polynomial $x^2=nx$, and so they have to be n and 0. Now using the trace condition, we see as before that the spectrum is given by n, once, and 0, a total of $n-1$ times.

Triangularity also allows us to prove a famous theorem by two of the early masters of the subject, **William Hamilton** and **Arthur Cayley**. We need a technical lemma first

> **Lemma.** Let $\mathbf{T}_1$, $\mathbf{T}_2$, …, $\mathbf{T}_n$ be upper triangular matrices of size n. Suppose the $i,i-$ entry of $\mathbf{T}_i$ is 0. Then $\mathbf{T}_1\mathbf{T}_2\cdots\mathbf{T}_n=\mathbf{0}$.

Proof. By induction on n. If $n=1$, there is nothing to prove. Assume the theorem holds true for $n-1$. Then $\mathbf{T}_1\mathbf{T}_2\cdots\mathbf{T}_{n-1}$ is of the form $\begin{pmatrix}\mathbf{0} & x\\ \mathbf{0} & a\end{pmatrix}$, but $\mathbf{T}_n=\begin{pmatrix}\mathbf{B} & y\\ \mathbf{0} & 0\end{pmatrix}$, so $\mathbf{T}_1\mathbf{T}_2\cdots\mathbf{T}_n=\mathbf{0}$. ⌘

Although the proof that we give requires that the matrix have real eigenvalues, the theorem is true in any situation.

> **Corollary (Cayley-Hamilton).** A matrix satisfies its characteristic polynomial.

Proof. By triangularity, without loss, we can assume that the matrix **A** is upper triangular. Let λ_1, $\lambda_2,\ldots,$ λ_n be the list of eigenvalues of **A** in the order they occur in the main diagonal. Let $\mathbf{T}_i=\mathbf{A}-\lambda_i\mathbf{I}$. Then by the lemma, $c_{\mathbf{A}}(\mathbf{A})=\prod_{i=1}^{n}(\mathbf{A}-\lambda_i\mathbf{I})=\mathbf{T}_1\cdots\mathbf{T}_n=\mathbf{0}$. ⌘

Example 5. Let $\mathbf{A}=\begin{pmatrix}1 & 2 & 3\\ 5 & 4 & -3\\ 2 & -1 & 5\end{pmatrix}$. Then $c_{\mathbf{A}}(x)=84+10x-10x^2+x^3$ is its characteristic polynomial. Indeed if one computes $c_{\mathbf{A}}(\mathbf{A})=84\mathbf{I}+10\mathbf{A}-10\mathbf{A}^2+\mathbf{A}^3$ one obtains **0**, the zero matrix.

Now we proceed to the important topic of diagonalization—namely, when is the **T** obtained from the theorem actually diagonal. We already have a fair understanding of what is required in order for us to be able to diagonalize a matrix. Namely at the very onset of the previous section, we saw that if $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}=\mathbf{D}$, then the columns of **P** are eigenvectors of **A** and the entries of **D** are eigenvalues of **A**. Since the columns of **P** are linearly independent, they must constitute a basis, and hence we already can state that

> **Theorem (Diagonability).** Let **A** be $n\times n$. Then **A** is a diagonable if and only if **A** has n linearly independent eigenvectors, in other words, a basis of eigenvectors. If this is the case, and $p(x)$ is any polynomial, then $p(\mathbf{A})$ is also diagonable. Moreover, if **A** is invertible and diagonable, then so is $\mathbf{A}^{-1}$.

Proof. If $\mathbf{P}^{-1}\mathbf{A}\mathbf{P}=\mathbf{D}$, then as we saw before, since $\mathbf{A}\mathbf{P}=\mathbf{P}\mathbf{D}$, we have that every column of **A** is an eigenvector of **A**, and the converse is just as easy. The second remark follows easily since $\mathbf{P}^{-1}p(\mathbf{A})\mathbf{P}=p(\mathbf{D})$ by the theorem. If **A** is invertible, then none of its eigenvalues are 0, and by inverting the equation, we get $\mathbf{P}^{-1}\mathbf{A}^{-1}\mathbf{P}=\mathbf{D}^{-1}$, and this matrix is naturally diagonal. ⌘

Note that **A** and $\mathbf{A}^{-1}$, as we saw before, have the same eigenvectors since the same matrix diagonalizes both.

Example 6. Consider the matrix $\mathbf{A}=\begin{pmatrix}1&2&3&-1&-2\\1&2&3&-1&-2\\1&2&3&-1&-2\\1&2&3&-1&-2\\1&2&3&-1&-2\end{pmatrix}$. By visual inspection we see that it has rank 1, so its nullity is 4, and so here are four linearly independent eigenvectors for the eigenvalue 0. By the row sum condition, another eigenvalue is 3, and we know that the vector of all ones is an eigenvector for the eigenvalue 3. The next theorem claims that eigenvectors corresponding to different eigenvalues are automatically linearly independent, and so we will have 5 linearly independent eigenvectors, hence **A** will be diagonable. Indeed, $\mathbf{P}=\begin{pmatrix}-2&-3&1&2&1\\1&0&0&0&1\\0&1&0&0&1\\0&0&1&0&1\\0&0&0&1&1\end{pmatrix}$ is an invertible matrix whose columns are eigenvectors of **A**, so **P** diagonalizes **A**.

Theorem (Eigenvectors and Independence). Suppose $\mathbf{u}_1$, $\mathbf{u}_2,\ldots,\mathbf{u}_t$ are eigenvectors of **A** corresponding to different eigenvalues. Then the vectors $\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_t$ are linearly independent.

Proof. By induction on *t*. It is trivially true if $t=1$. Assume it is true for $t-1$. Assume by way of contradiction that $\mathbf{u}_1$, $\mathbf{u}_2,\ldots,\mathbf{u}_t$ are not independent. Then one of them, say $\mathbf{u}_t$, is a linear combination of the others:

$$\mathbf{u}_t=a_1\mathbf{u}_1+a_2\mathbf{u}_2+\cdots+a_{t-1}\mathbf{u}_{t-1},$$

where not all a_i's are 0 since $\mathbf{u}_t$ is not zero. Without loss assume $a_{t-1}\neq 0$. Let λ_i be the eigenvalue corresponding to $\mathbf{u}_i$. Then when we multiply the equation by λ_t we get:

$$\lambda_t\mathbf{u}_t=a_1\lambda_t\mathbf{u}_1+a_2\lambda_t\mathbf{u}_2+\cdots+a_{t-1}\lambda_t\mathbf{u}_{t-1}$$

while if we multiply it by **A**

$$\lambda_t\mathbf{u}_t=\mathbf{A}\mathbf{u}_t=a_1\mathbf{A}\mathbf{u}_1+a_2\mathbf{A}\mathbf{u}_2+\cdots+a_{t-1}\mathbf{A}\mathbf{u}_{t-1}=a_1\lambda_1\mathbf{u}_1+a_2\lambda_2\mathbf{u}_2+\cdots+a_{t-1}\lambda_{t-1}\mathbf{u}_{t-1}$$

and subtracting these two equations we obtain:

$$\mathbf{0}=a_1\left(\lambda_1-\lambda_t\right)\mathbf{u}_1+a_2\left(\lambda_2-\lambda_t\right)\mathbf{u}_2+\cdots+a_{t-1}\left(\lambda_{t-1}-\lambda_t\right)\mathbf{u}_{t-1}.$$

But since $a_{t-1}\left(\lambda_{t-1}-\lambda_t\right)\neq 0$, we can solve for $\mathbf{u}_{t-1}$, in terms of $\mathbf{u}_1$, $\mathbf{u}_2,\ldots,\mathbf{u}_{t-2}$, giving us a contradiction to the induction hypothesis. ⌘

We get a very useful corollary to the theorem:

Corollary (Different Eigenvalues). If **A** has different eigenvalues, then **A** is diagonable.

Proof. If we have *n* different eigenvalues, since we always have at least one eigenvector for each eigenvalue, we have *n* linearly independent eigenvectors. ⌘

Example 7. Let $\mathbf{A}=\begin{pmatrix}1&2&3\\5&4&-3\\2&-1&5\end{pmatrix}$. Then $\mathbf{A}$ is diagonable since its spectrum is 6, $2+3\sqrt{2}$ and $2-3\sqrt{2}$. In fact, if we find an eigenvector for each of the eigenvalues, they will be independent. Respectively the eigenvectors are $\begin{pmatrix}1\\1\\1\end{pmatrix}$, $\begin{pmatrix}-1+\sqrt{2}\\1-\sqrt{2}\\1\end{pmatrix}$ and $\begin{pmatrix}-1-\sqrt{2}\\1+\sqrt{2}\\1\end{pmatrix}$.

Of course, given λ, an eigenvalue of $\mathbf{A}$, the nullity of $\mathbf{A}-\lambda\mathbf{I}$ is the dimension of $\mathrm{N}(\mathbf{A}-\lambda\mathbf{I})$, and this is the dimension of the eigenspace corresponding to λ. The dimension of this eigenspace is of relevance for the issue of diagonability. But there is an unexpected requirement on this dimension.

> **Theorem (Multiplicity vs. Dimension of Eigenspace).** Let λ be an eigenvalue of $\mathbf{A}$. Then the dimension of the eigenspace corresponding to λ is at most its multiplicity in $c_{\mathbf{A}}(x)$.

Proof. Suppose $\mathbf{u}_1,\ \mathbf{u}_2,\ldots,\mathbf{u}_t$ is a basis for the eigenspace. We need to show then that λ has multiplicity at least *t*. But since this set is linearly independent, we can find an invertible matrix $\mathbf{P}$ whose first t columns are $\mathbf{u}_1,\ \mathbf{u}_2,\ldots,\mathbf{u}_t$. Let us then consider the matrix $\mathbf{P}^{-1}\mathbf{AP}=\mathbf{M}$, and let $\mathbf{v}_1,\ \mathbf{v}_2,\ldots,\mathbf{v}_t$ be the first *t* columns of $\mathbf{M}$. Then since $\mathbf{AP}=\mathbf{PM}$ and $\mathbf{Au}_i=\lambda\mathbf{u}_i$, we must have that $\mathbf{v}_i=\lambda\mathbf{e}_i$ where $\mathbf{e}_i$ is the i^{th} column of the identity matrix. Thus $\mathbf{M}$ is of the form $\mathbf{M}=\begin{pmatrix}\lambda\mathbf{I}&\mathbf{X}\\\mathbf{0}&\mathbf{Y}\end{pmatrix}$, and so the characteristic polynomial of $\mathbf{A}$ satisfies $c_{\mathbf{A}}(x)=c_{\mathbf{M}}(x)=(\lambda-x)^t c_{\mathbf{Y}}(x)$, and our claim is established. ⌘

Example 8. Suppose a matrix $\mathbf{A}$ has characteristic polynomial given by

$$c_A(x)=(4-x)^5(3-x)^3(2-x).$$

Then we know that $\mathbf{A}$ is 9×9, we know its trace 31 and its determinant $55296=4^5 3^3 2$. In particular its rank is 9. But what is the rank of $\mathbf{A}-\lambda\mathbf{I}$ for a given number λ? Of course, if $\lambda\neq4,3,2$, then we know the rank is 9. And on the other hand, if $\lambda=4,3,2$, then the rank is at most 8. But more is known, by the theorem we know that $\mathbf{A}-2\mathbf{I}$ is of rank exactly 8 since 2 occurs only once as an eigenvalue, so there can only be one free variable in the reduced form of $\mathbf{A}-2\mathbf{I}$. Similarly, $\mathbf{A}-3\mathbf{I}$ has rank at least 6 (at most 3 free variables), and $\mathbf{A}-4\mathbf{I}$ has rank at least 4 (at most 5 free variables).

With this in hand, we have another criterion for diagonability

Theorem (Diagonability). A matrix $\mathbf{A}$ is diagonable if and only if for each eigenvalue λ, the dimension of the eigenspace equals its multiplicity.

Proof. We have seen before that to be diagonable, what is necessary and sufficient is that there be a basis of eigenvectors. But for that basis to exist we have to find enough eigenvectors for each eigenvalue. Before we have seen that we cannot have the dimension of any of the eigenspaces bigger than the multiplicity, and since the multiplicities add up to the size of the matrix, in order to have a basis we must have the dimensions equal to the respective multiplicities. On the other hand if the dimensions of the eigenspaces equal the multiplicities, then we can pick enough independent eigenvectors for each of the eigenvalues, and putting them together will retain the independence, and so we will have a basis. ⌘

Example 9. Let $\mathbf{A} = \begin{pmatrix} 1 & x & 0 & 0 & 0 & 0 \\ 0 & 1 & y & 0 & 0 & 0 \\ 0 & 0 & 1 & z & 0 & 0 \\ 0 & 0 & 0 & 2 & w & 0 \\ 0 & 0 & 0 & 0 & 2 & u \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$, then we know its spectrum to be 1, 1, 1, 2, 2 and 3. Starting with the latter, we see that $\mathbf{A} - 3\mathbf{I}$ has 5 pivots regardless of what x, y, z, w and u are, so its null space has dimension 1, so we will only be able to pick up one eigenvector for the eigenvalue 3, confirming the fact that the multiplicity is an upper bound of the dimension of the eigenspace.

For the eigenvalue 2, the picture is not as clear, $\mathbf{A} - 2\mathbf{I} = \begin{pmatrix} -1 & x & 0 & 0 & 0 & 0 \\ 0 & -1 & y & 0 & 0 & 0 \\ 0 & 0 & -1 & z & 0 & 0 \\ 0 & 0 & 0 & 0 & w & 0 \\ 0 & 0 & 0 & 0 & 0 & u \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ which has a minimum of 4 pivots as expected, but it could have 5, and that is the case if and only if $w \neq 0$. So we will be able to find two independent eigenvectors for the eigenvalue 2 if and only if $w = 0$.

Finally, for the eigenvalue 1 we will need three independent eigenvectors, and since we have at least three pivots in $\mathbf{A} - \mathbf{I} = \begin{pmatrix} 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & y & 0 & 0 & 0 \\ 0 & 0 & 0 & z & 0 & 0 \\ 0 & 0 & 0 & 1 & w & 0 \\ 0 & 0 & 0 & 0 & 1 & u \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$, in order to not pick up any more of them we need $x = y = 0$, and so the only way $\mathbf{A}$ will be diagonable is for

$$\mathbf{A}=\begin{pmatrix}1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&z&0&0\\0&0&0&2&0&0\\0&0&0&0&2&u\\0&0&0&0&0&3\end{pmatrix}.$$

But the example above affords us to dig deeper into the notion of diagonability. We already have via the **Cayley-Hamilton Theorem** that every matrix satisfies its characteristic polynomial. And a corollary above showed that if the characteristic polynomial of a matrix has distinct roots, then the matrix is automatically diagonable, but that was not necessary as the identity matrix exemplifies. The polynomial that is crucial to diagonability is called the **minimum polynomial** and that is what we discuss next.

Let $\mathbf{A}$ be a square matrix. Since $\mathbf{A}$ satisfies a polynomial, there exists a polynomial of least degree that $\mathbf{A}$ satisfies. There is only one of such lowest degree polynomial that has leading coefficient 1. This polynomial is called the **minimum polynomial** of $\mathbf{A}$ and is denoted by $m_{\mathbf{A}}(x)$.

Example 10. The minimum polynomial of $\mathbf{I}$ is $x-1$. Also clear is that the minimum polynomial of a matrix cannot be of degree 1 unless it is a **scalar matrix**, *i.e.*, a multiple of $\mathbf{I}$. The minimum polynomial of $\mathbf{J}_n$ is x^2-nx. Any nontrivial projection matrix has x^2-x for its minimum polynomial while any reflection has x^2-1.

Theorem (Minimum Polynomial). Let $\mathbf{A}$ be $n\times n$ with minimum polynomial $m_{\mathbf{A}}(x)$.

① If $p(x)$ is any polynomial that $\mathbf{A}$ satisfies, i.e., $p(\mathbf{A})=\mathbf{O}$, then $p(x)$ is a multiple of $m_{\mathbf{A}}(x)$. In other words, $p(x)=m_{\mathbf{A}}(x)q(x)$, for some polynomial $q(x)$.

② In particular, $c_{\mathbf{A}}(x)$, the characteristic polynomial of $\mathbf{A}$ is a multiple of $m_{\mathbf{A}}(x)$, *i.e.*, $c_{\mathbf{A}}(x)=m_{\mathbf{A}}(x)q(x)$, for some polynomial $q(x)$. Thus, $m_{\mathbf{A}}(x)$ is of degree at most *n*.

③ The set of distinct eigenvalues of $\mathbf{A}$ is exactly the set of distinct roots of $m_{\mathbf{A}}(x)$. In other words, a number is an eigenvalue of $\mathbf{A}$ if and only if it is a root of $m_{\mathbf{A}}(x)$.

④ The dimension of $\langle\mathbf{A}\rangle=[\mathbf{I},\mathbf{A},\mathbf{A}^2,\mathbf{A}^3,\ldots]$, the span of the powers of $\mathbf{A}$, is the degree of the minimum polynomial of $\mathbf{A}$, $m_{\mathbf{A}}(x)$.

Proof. The first claim follows from long division of polynomials which states that if $p(x)$ is any polynomial then we can find the quotient $q(x)$ and the remainder $r(x)$ when $p(x)$ is divided by $m_{\mathbf{A}}(x)$. The remainder is always 0 or of degree less than $m_{\mathbf{A}}(x)$. So as with any division, $p(x)=m_{\mathbf{A}}(x)q(x)+r(x)$, so when we substitute **A**, we get $p(\mathbf{A})=m_{\mathbf{A}}(\mathbf{A})q(\mathbf{A})+r(\mathbf{A})$, and so if $p(\mathbf{A})=\mathbf{0}$, since $m_{\mathbf{A}}(\mathbf{A})=\mathbf{0}$, we get $r(\mathbf{A})=\mathbf{0}$, and by our choice of $m_{\mathbf{A}}(x)$ as being of least possible degree, we get that $r(x)=0$, and so $p(x)$ is a multiple of $m_{\mathbf{A}}(x)$. ② follows directly from ① and the **Cayley-Hamilton Theorem**. That every eigenvalue of **A** is a root of $m_{\mathbf{A}}(x)$ follows from the fact $m_{\mathbf{A}}(\mathbf{A})=\mathbf{0}$ and the eigenvalues of a polynomials theorem. The fact that every root of $m_{\mathbf{A}}(x)$ is an eigenvalue follows from ②. Finally ④ follows from the observation that to write $\mathbf{A}^k$ as a linear combination of lower powers is exactly to find a polynomial of degree k and leading coefficient 1 that **A** satisfies. ⌘

Example 11. The Petersen Graph Again. Let **A** be the adjacency matrix of the Petersen graph. Then we saw before that **A** satisfies the polynomial

$$(3-x)\left(2-x-x^2\right)=6-5x-2x^2+x^3.$$

Thus, we know $\mathbf{A}^3=2\mathbf{A}^2+5\mathbf{A}-6\mathbf{I}$, on the other hand it is clear that $\mathbf{A}^2$ is not a linear combination of **I** and **A**, so the dimension of $\langle\mathbf{A}\rangle=\left[\mathbf{I},\mathbf{A},\mathbf{A}^2,\mathbf{A}^3,\ldots\right]$ is 3, so indeed the minimum polynomial of A is $m_{\mathbf{A}}(x)=6-5x-2x^2+x^3$, and its roots 3, 1 and -2 is a complete list of its eigenvalues. Of course, as we saw,

$$c_{\mathbf{A}}(x)=(x-3)(x-1)^5(x+2)^4=m_{\mathbf{A}}(x)(x-1)^4(x+2)^3.$$

But the reason that minimum polynomials were introduced in this section is because there is an intimate connection between them and diagonability. The key theorem is

> **Theorem (Minimum Polynomials and Diagonability).** Let **A** be square. Then the following are equivalent:
>
> ① **A** is diagonable.
>
> ② $m_{\mathbf{A}}(x)$ has no repeated roots.
>
> ③ There exists a polynomial $p(x)$ with no repeated roots that **A** satisfies, *i.e.*, $p(\mathbf{A})=\mathbf{0}$.

The proof of this theorem can be found in the **Appendix of Proofs**.

Let us revisit a previous example:

Example 9 Revisited. Let $\mathbf{A} = \begin{pmatrix} 1 & x & 0 & 0 & 0 & 0 \\ 0 & 1 & y & 0 & 0 & 0 \\ 0 & 0 & 1 & z & 0 & 0 \\ 0 & 0 & 0 & 2 & w & 0 \\ 0 & 0 & 0 & 0 & 2 & u \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$. Then we know its characteristic polynomial to be $(1-x)^3(2-x)^2(3-x)$. Thus we know (and it could easily be verified) that $(\mathbf{A}-\mathbf{I})^3(\mathbf{A}-2\mathbf{I})^2(\mathbf{A}-3\mathbf{I}) = \mathbf{0}$ regardless of what x, y, x, w and u are.

Thus we have a small list of polynomials that $\mathbf{A}$ could satisfy, namely the factors of $(\mathbf{A}-\mathbf{I})^3(\mathbf{A}-2\mathbf{I})^2(\mathbf{A}-3\mathbf{I})$ that themselves have the factor $(\mathbf{A}-\mathbf{I})(\mathbf{A}-2\mathbf{I})(\mathbf{A}-3\mathbf{I})$, since we need to annihilate all the eigenvalues of $\mathbf{A}$. The following is a list of computations:

$p(x)$	$(x-1)^3(x-2)^2(x-3)$	$(x-1)^3(x-2)(x-3)$
$p(\mathbf{A})$	$\mathbf{0}$	$\begin{pmatrix} 0 & 0 & 0 & 0 & -xyzw & xyzwu \\ 0 & 0 & 0 & 0 & -yzw & yzwu \\ 0 & 0 & 0 & 0 & -zw & zwu \\ 0 & 0 & 0 & 0 & -w & wu \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
$p(\mathbf{A}) = \mathbf{0}$	Always	When $w=0$
$p(x)$	$(x-1)^2(x-2)^2(x-3)$	$(x-1)^2(x-2)(x-3)$
$p(\mathbf{A})$	$\begin{pmatrix} 0 & 0 & -2xy & 2xyz & -2xyzw & xyzwu \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 2xy & -2xyz & xyzw & 0 \\ 0 & 0 & 0 & 0 & -yzw & yzwu \\ 0 & 0 & 0 & 0 & -zw & zwu \\ 0 & 0 & 0 & 0 & -w & wu \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
$p(\mathbf{A}) = \mathbf{0}$	When either $x=0$ or $y=0$	When either $x=0$ or $y=0$ and $w=0$
$p(x)$	$(x-1)(x-2)^2(x-3)$	$(x-1)(x-2)(x-3)$
$p(\mathbf{A})$	$\begin{pmatrix} 0 & -2x & x^2y & 3xyz & xyzw & 0 \\ 0 & 0 & -2y & 2yz & -2yzw & yzwu \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 2x & -3xy & xyz & 0 & 0 \\ 0 & 0 & 2y & -2yz & yzw & 0 \\ 0 & 0 & 0 & 0 & -zw & zwu \\ 0 & 0 & 0 & 0 & -w & wu \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
$p(\mathbf{A}) = \mathbf{0}$	When $x=y=0$	When $x=y=0$ and $w=0$

And thus we see the minimum polynomial has no repeated roots exactly when $\mathbf{A}$ satisfies $(x-1)(x-2)(x-3)$, and that occurs if and only if $x=y=0$ and $w=0$, the same conditions for the diagonability of $\mathbf{A}$.

We end the section with a process to attempt to find the minimum polynomial of a matrix $\mathbf{A}$.

Let $\mathbf{A}$ be $n\times n$, and consider any nonzero vector $\mathbf{u}\neq\mathbf{0}$. Compute the sequence, $\mathbf{u}$, $\mathbf{Au}$, $\mathbf{A}^2\mathbf{u}$, $\mathbf{A}^3\mathbf{u}$, ….$\mathbf{A}^n\mathbf{u}$, and build the matrix $\mathbf{M}=\begin{pmatrix}\mathbf{u} & \mathbf{Au} & \mathbf{A}^2\mathbf{u} & \cdots & \mathbf{A}^n\mathbf{u}\end{pmatrix}$. Let $k=r(\mathbf{M})$. This matrix has an interesting property—its pivots will be the first k columns. The argument is simple, once we have the first nonpivotal column, then all following columns are also nonpivotal, for suppose

$$\mathbf{A}^i\mathbf{u}=a_0\mathbf{u}+a_1\mathbf{Au}+\cdots+a_{i-1}\mathbf{A}^{i-1}\mathbf{u},$$

then

$$\mathbf{A}^{i+1}\mathbf{u}=a_0\mathbf{Au}+a_1\mathbf{A}^2\mathbf{u}+\cdots+a_{i-1}\mathbf{A}^i\mathbf{u}=$$

$$a_0\mathbf{Au}+a_1\mathbf{A}^2\mathbf{u}+\cdots+a_{i-2}\mathbf{A}^{i-1}\mathbf{u}+\ a_{i-1}\left(a_0\mathbf{u}+a_1\mathbf{Au}+\cdots+a_{i-1}\mathbf{A}^{i-1}\mathbf{u}\right),$$

and so the next column is also a linear combination of the previous columns, and so on. Thus $i=k=r(\mathbf{M})$. But what is more interesting is that if we consider the polynomial $p(x)=x^k-a_{k-1}x^{k-1}-\cdots-a_1x-a_0$, then we know $p(\mathbf{A})\mathbf{u}=\mathbf{0}$, but since this is the lowest degree polynomial that will annihilate $\mathbf{u}$, by similar arguments to the ones above, we must have that $p(x)$ is a factor of $m_{\mathbf{A}}(x)$. If $p(\mathbf{A})=\mathbf{0}$, then we know that $p(x)=m_{\mathbf{A}}(x)$. If not we can consider another vector $\mathbf{v}\notin\mathcal{C}(\mathbf{M})$, and repeat the process, until we arrive at a polynomial that $\mathbf{A}$ will satisfy.

We need not compute all of $\mathbf{M}$, all we need is rank of it.

Example 12. Let $\mathbf{A}=\begin{pmatrix}0&1&0&1&0&1&0\\1&0&1&0&1&0&1\\0&1&0&1&0&1&0\\1&0&1&0&1&0&1\\0&1&0&1&0&1&0\\1&0&1&0&1&0&1\\0&1&0&1&0&1&0\end{pmatrix}$, and let $\mathbf{u}=\begin{pmatrix}1\\1\\1\\1\\1\\1\\1\end{pmatrix}$. Then $\mathbf{Au}=\begin{pmatrix}3\\4\\3\\4\\3\\4\\3\end{pmatrix}$ and $\mathbf{A}^2\mathbf{u}=\begin{pmatrix}12\\12\\12\\12\\12\\12\\12\end{pmatrix}$, so clearly, $\mathbf{A}^2\mathbf{u}=12\mathbf{u}$, and so x^2-12 is a factor of the minimum polynomial. In fact, we can verify that the polynomial $x^3 - 12x$ is the minimum polynomial of **A**, in the sense that it is a polynomial that **A** satisfies and no polynomial of lesser degree exists that **A** satisfies. By the way, the characteristic polynomial is $x^7 - 12x^5$.

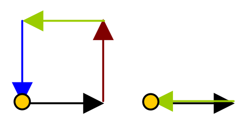
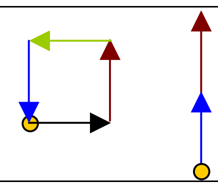
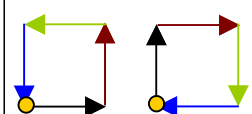
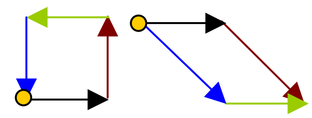
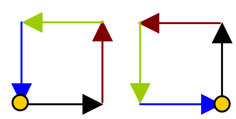
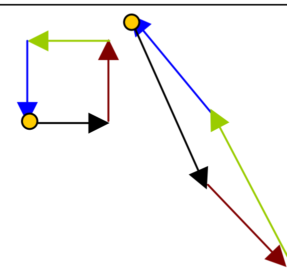
Similarly, if we let $\mathbf{B} = \mathbf{J}_7 - \mathbf{A}$, then easily $\mathbf{B}^2\mathbf{u} = -12\mathbf{u} + 7\mathbf{B}\mathbf{u}$, and so 4 and 3 which are the roots of $x^2 - 7x + 12$ are eigenvalues of **B**. Again the characteristic polynomial is $x^7 - 7x^6 + 12x^5$.

Example 13. Let $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$. Then $\mathbf{A}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 6 \\ 15 \\ 24 \end{pmatrix}$, $\mathbf{A}\begin{pmatrix} 6 \\ 15 \\ 24 \end{pmatrix} = \begin{pmatrix} 108 \\ 243 \\ 378 \end{pmatrix}$ and $\mathbf{A}\begin{pmatrix} 108 \\ 243 \\ 378 \end{pmatrix} = \begin{pmatrix} 1728 \\ 3915 \\ 6102 \end{pmatrix}$, and since the matrix $\mathbf{M} = \begin{pmatrix} 1 & 6 & 108 & 1728 \\ 1 & 15 & 243 & 3915 \\ 1 & 24 & 378 & 6102 \end{pmatrix}$ reduces to $\begin{pmatrix} 1 & 0 & 18 & 270 \\ 0 & 1 & 15 & 243 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, we must have that $x^2 = 15x + 18$ has to be a factor of the minimum polynomial. But since $\det \mathbf{A} = 0$, we must have that $m_{\mathbf{A}}(x) = c_{\mathbf{A}}(x) = 18x + 15x^2 - x^3$.

❶❻ Symmetric and Orthogonal Matrices

From the algebraic point of view, the relation of similarity leaves little to be desired. If two matrices are similar they have the same eigenvalues, characteristic polynomial, determinant, trace, and minimum polynomial. What more could one ask for?

From the geometric point of view, however, it is not that satisfying. The following examples should illustrate the remark. We consider three matrices that are easily understood as geometric transformations, and observe the impact on those matrices of the similarity by the matrix $\mathbf{P} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

	A	Geometric Description	Unit Square Effect	$\mathbf{P}^{-1}\mathbf{AP}$	Unit Square Effect
❶	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	the projection on the x-axis		$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$	
❷	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	the reflection on the $y = x$ line		$\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$	
❸	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	90° – rotation about the origin		$\begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}$	

Although we see no disturbance in area or orientation in all 3 examples (since similar matrices have the same determinant), we do observe non-uniform changes in both lengths and angles. In fact, it is length that is the most crucial of all of these geometric parameters. In ❶, $\mathbf{P}^{-1}\mathbf{AP}$ sends the vector $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ to the vector $\begin{pmatrix} 0 \\ 2 \end{pmatrix}$ (a change in length) while the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ goes to the vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ (no change). In ❷, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ goes to itself while $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is mapped to $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$, a longer vector. Finally in ❸ both $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are mapped to longer vectors of different length, the first to a vector of length $\sqrt{5}$ while the second to a vector of length $\sqrt{2}$.

Naturally from our elementary school day's experience, we expect that if a transformation preserves lengths, then area is also necessarily preserved—not so obvious is the fact that once a matrix preserves length, it preserves all geometric quantities (except perhaps orientation).

However, we first need to revisit orthogonality of vectors. Let $\mathbf{u}$ and $\mathbf{v}$ be vectors. Then, as we saw before, $\mathbf{u}$ and $\mathbf{v}$ are **perpendicular**, or **orthogonal**, denoted by $\mathbf{u}\perp\mathbf{v}$, if $\mathbf{u}\cdot\mathbf{v}=\mathbf{u}^{\mathrm{T}}\mathbf{v}=0$.

In general, a set of vectors is said to be **orthogonal** (or **mutually orthogonal**) if each one of them is perpendicular to all the others. A set of orthogonal unit vectors is called an **orthonormal** set.

> **Theorem (Orthogonal Sets).** Let $\mathbf{u}_1$, $\mathbf{u}_2,\ldots,\mathbf{u}_t\in\mathbb{R}^n$, and consider $\mathbf{A}=\begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_t\end{pmatrix}$. Then $\mathbf{u}_1$, $\mathbf{u}_2,\ldots,\mathbf{u}_t$ form an orthogonal set if and only if $\mathbf{A}^{\mathrm{T}}\mathbf{A}=\mathbf{D}$, a diagonal matrix. In particular, if the vectors are all nonzero, and orthogonal, they are necessarily independent. Moreover, they will be orthonormal if and only if $\mathbf{A}^{\mathrm{T}}\mathbf{A}=\mathbf{I}_t$.

Proof. We have seen before that for any matrix $\mathbf{A}$, the $i,j-$ entry of $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is the dot product of the i^{th} and j^{th} columns and so the main claim follows immediately. Since if the vectors are nonzero, $\mathbf{D}$ is an invertible matrix, we have an independent set, and the orthonormality claim is obvious. ⌘

Example 1. Consider the vectors $\mathbf{u}=\begin{pmatrix}-1\\-1\\2\\0\\0\end{pmatrix}$, $\mathbf{v}=\begin{pmatrix}-1\\-1\\-1\\3\\0\end{pmatrix}$ and $\mathbf{w}=\begin{pmatrix}-1\\-1\\-1\\-1\\4\end{pmatrix}$ in $\mathbb{R}^5$, and the 5×3 matrix $\mathbf{A}=\begin{pmatrix}\mathbf{u} & \mathbf{v} & \mathbf{w}\end{pmatrix}$. Then, easily, $\mathbf{A}^{\mathrm{T}}\mathbf{A}=\begin{pmatrix}6&0&0\\0&12&0\\0&0&20\end{pmatrix}$, and so the vectors form an orthogonal set. They do not form an orthonormal set since the vectors are not unit vectors. To accomplish an orthonormal set we would divide each vector by its length, $\frac{1}{\sqrt6}\mathbf{u}$, $\frac{1}{2\sqrt3}\mathbf{v}$ and $\frac{1}{2\sqrt5}\mathbf{w}$ form such an orthonormal set.

A set of vectors in a subspace V is an **orthonormal basis** if they are a basis and orthonormal (**what else?**). The vectors $\mathbf{u}=\begin{pmatrix}1\\3\\5\end{pmatrix}$, $\mathbf{v}=\begin{pmatrix}-4\\3\\-1\end{pmatrix}$ and $\mathbf{w}=\begin{pmatrix}18\\19\\-15\end{pmatrix}$ form an

orthogonal, but not orthonormal basis of $\mathbb{R}^3$. If $\mathbf{A} = \begin{pmatrix} \mathbf{u} & \mathbf{v} & \mathbf{w} \end{pmatrix}$, $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \begin{pmatrix} 35 & 0 & 0 \\ 0 & 26 & 0 \\ 0 & 0 & 910 \end{pmatrix}$.
To obtain an orthonormal basis from **u**, **v** and **w**, all that is needed is to **normalize** them, that is, to make them unit vectors. Thus, $\mathbf{u}' = \frac{1}{\sqrt{35}}\begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix}$, $\mathbf{v}' = \frac{1}{\sqrt{26}}\begin{pmatrix} -4 \\ 3 \\ -1 \end{pmatrix}$ and $\mathbf{w}' = \frac{1}{\sqrt{910}}\begin{pmatrix} 18 \\ 19 \\ -15 \end{pmatrix}$ form an orthonormal basis of $\mathbb{R}^3$.

The theorem is fundamental:

> **Theorem (Orthogonal Matrices).** Let $\mathbf{P}$ be $n \times n$ and consider the transformation $f_{\mathbf{P}} : \mathbb{R}^n \to \mathbb{R}^n$. Then the following are equivalent:
>
> ① $f_{\mathbf{P}}$ preserves lengths, *i.e.*, for any vector $\mathbf{u} \in \mathbb{R}^n$, the length of its image is the same as its length, $|\mathbf{u}| = |f_{\mathbf{P}}(\mathbf{u})|$
>
> ② $f_{\mathbf{P}}$ preserves distances, *i.e.*, for any vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, the distance between their images is the same as the distance between the two of them. Namely, if we let $d(\mathbf{u}, \mathbf{v})$ denote the distance between **u** and **v**, then $d(\mathbf{u}, \mathbf{v}) = d\left(f_{\mathbf{P}}(\mathbf{u}), f_{\mathbf{P}}(\mathbf{v})\right)$.
>
> ③ $\mathbf{P}^{\mathrm{T}}\mathbf{P} = \mathbf{I}$
>
> ④ The columns of **P** form an orthonormal basis of $\mathbb{R}^n$.
>
> Moreover, if this is case, then $f_{\mathbf{P}}$ also preserves angles and volumes.

Proof. The equivalence of ③ and ④ is clear from the theorem above. If ② is true, then since $d(\mathbf{u}, \mathbf{0}) = |\mathbf{u}|$, and $f_{\mathbf{P}}(\mathbf{0}) = \mathbf{0}$, ① follows. Conversely, since $d(\mathbf{u}, \mathbf{v}) = |\mathbf{u} - \mathbf{v}|$, if ① holds, then

$$d(\mathbf{u}, \mathbf{v}) = |\mathbf{u} - \mathbf{v}| = |f_{\mathbf{P}}(\mathbf{u} - \mathbf{v})| = |\mathbf{P}(\mathbf{u} - \mathbf{v})| = |\mathbf{Pu} - \mathbf{Pv}| = |f_{\mathbf{P}}(\mathbf{u}) - f_{\mathbf{P}}(\mathbf{v})| = d\left(f_{\mathbf{P}}(\mathbf{u}), f_{\mathbf{P}}(\mathbf{v})\right)$$

so ② holds. Assume ③ holds, then for any **u**,

$$|f_{\mathbf{P}}(\mathbf{u})|^2 = |\mathbf{Pu}|^2 = (\mathbf{Pu})^{\mathrm{T}}\mathbf{Pu} = \mathbf{u}^{\mathrm{T}}\mathbf{P}^{\mathrm{T}}\mathbf{Pu} = \mathbf{u}^{\mathrm{T}}\mathbf{u} = |\mathbf{u}|^2$$

and we have ①. Finally assume ② (and ①), and let $\mathbf{P} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$. Now since $f_{\mathbf{P}}\left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = \mathbf{u}_1$, $|\mathbf{u}_1| = 1$, and similarly for the other columns. Now we show $\mathbf{u}_1 \perp \mathbf{u}_2$, and that will suffice. We know that $d(\mathbf{u}_1, \mathbf{u}_2) = \sqrt{2}$ by ②, and so

$$2 = |\mathbf{u}_1 - \mathbf{u}_2|^2 = (\mathbf{u}_1 - \mathbf{u}_2)^{\mathrm{T}}(\mathbf{u}_1 - \mathbf{u}_2) = \mathbf{u}_1^{\mathrm{T}}\mathbf{u}_1 - \mathbf{u}_1^{\mathrm{T}}\mathbf{u}_2 - \mathbf{u}_2^{\mathrm{T}}\mathbf{u}_1 + \mathbf{u}_2^{\mathrm{T}}\mathbf{u}_2 =$$
$$1 - \mathbf{u}_1^{\mathrm{T}}\mathbf{u}_2 - \mathbf{u}_2^{\mathrm{T}}\mathbf{u}_1 + 1 = 2 - 2\mathbf{u}_1 \cdot \mathbf{u}_2$$

and so $\mathbf{u}_1 \perp \mathbf{u}_2$. Now we show that $f_\mathbf{P}$ also preserves angles and volumes. The latter is simple: since $\mathbf{P}^\mathrm{T}\mathbf{P} = \mathbf{I}$, $\det \mathbf{P} = \pm 1$, so volumes are preserved. To preserve angles it suffices to show it preserves dot products, but $\mathbf{u} \cdot \mathbf{v} = \mathbf{u}^\mathrm{T}\mathbf{v} = \mathbf{u}^\mathrm{T}\mathbf{P}^\mathrm{T}\mathbf{P}\mathbf{v} = f_P(\mathbf{u}) \cdot f_P(\mathbf{v})$, and we are finished. ⌘

A $n \times n$ matrix $\mathbf{P}$ is called **orthogonal** if it satisfies the conditions of the theorem. Equivalently $\mathbf{P}$ is orthogonal if $\mathbf{P}^{-1} = \mathbf{P}^\mathrm{T}$. Observe the unfortunate nomenclature of orthogonal matrix, yet it is not enough that its columns form an orthogonal basis, it is necessary they form an orthonormal basis.

Example 2. From both the algebraic (since $\mathbf{P}^{-1} = \mathbf{P}^\mathrm{T}$) and the geometric points of view (since $f_\mathbf{P}$ is just renaming coordinates), every permutation matrix $\mathbf{P}$ is an orthogonal matrix.

Note that for a square matrix, $\mathbf{P}^\mathrm{T}\mathbf{P} = \mathbf{I}$ if and only if $\mathbf{P}\mathbf{P}^\mathrm{T} = \mathbf{I}$, so as a trivial algebraic consequence, we get an unexpected geometric fact:

> **Corollary (Orthogonality of Rows).** A square matrix is orthogonal if and only if its rows form an orthonormal basis.

Example 3. By the example, and the theorem, $\mathbf{P} = \begin{pmatrix} \frac{1}{\sqrt{35}} & \frac{-4}{\sqrt{26}} & \frac{18}{\sqrt{910}} \\ \frac{3}{\sqrt{35}} & \frac{3}{\sqrt{26}} & \frac{19}{\sqrt{910}} \\ \frac{5}{\sqrt{35}} & \frac{-1}{\sqrt{26}} & \frac{-15}{\sqrt{910}} \end{pmatrix}$ is an orthogonal matrix but again the matrix $\mathbf{A} = \begin{pmatrix} 1 & -4 & 18 \\ 3 & 3 & 19 \\ 5 & -1 & -15 \end{pmatrix}$ is not orthogonal although its columns form an orthogonal set. Note that the rows of $\mathbf{P}$ are indeed an orthonormal basis for $\mathbb{R}^3$, in a nontrivial way. For example for the first two rows, we get: $\frac{3}{35} - \frac{12}{26} + \frac{342}{910} = 0$. On the other hand the rows of $\mathbf{A}$ are not orthogonal at all: $3 - 12 + 342 = 333$.

Trivially, the product of orthogonal matrices is orthogonal since

$$(\mathbf{PQ})^{-1} = \mathbf{Q}^{-1}\mathbf{P}^{-1} = \mathbf{Q}^\mathrm{T}\mathbf{P}^\mathrm{T} = (\mathbf{PQ})^\mathrm{T}.$$

The next stage of development is an algorithm on how to build an orthogonal set from any given set of vectors. Remember, as we saw before, it is trivial to go from an orthogonal set to an orthonormal one by simply dividing by the lengths of each vector.

One of the advantages of orthogonal sets is that if an element is written as a linear combination of them, then the components are the projections along each of the individual vectors. The geometric picture is very clear, if we have an orthogonal set, then we have a square box, so a vector is just the sum of the lengths along each of the edges.

Lemma. Let $\mathbf{u}_1,\ \mathbf{u}_2,\ldots,\mathbf{u}_t \in \mathbb{R}^n$ be nonzero orthogonal vectors. Let $\mathbf{v} = a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_t\mathbf{u}_t$. Then $a_i = \dfrac{\mathbf{v}\cdot\mathbf{u}_i}{\mathbf{u}_i\cdot\mathbf{u}_i}$.

Proof. Consider $\mathbf{v}\cdot\mathbf{u}_i$, and since all but one of the terms disappears, we are done. ⌘

Example 4. The vectors $\mathbf{u} = \begin{pmatrix}1\\3\\5\end{pmatrix}$, $\mathbf{v} = \begin{pmatrix}-4\\3\\-1\end{pmatrix}$ and $\mathbf{w} = \begin{pmatrix}18\\19\\-15\end{pmatrix}$ form an orthogonal basis of $\mathbb{R}^3$. To write $\mathbf{x} = \begin{pmatrix}x\\y\\z\end{pmatrix}$ as a linear combination of $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$, we simply take $\mathbf{x} = a\mathbf{u} + b\mathbf{v} + c\mathbf{w}$ where $a = \dfrac{x+3y+5z}{35}$, $b = \dfrac{-4x+3y-z}{26}$ and $c = \dfrac{18x+19y-15z}{910}$.

Theorem (Gram-Schmidt). Let $\mathbf{u}_1,\ \mathbf{u}_2,\ldots,\mathbf{u}_t \in \mathbb{R}^n$ be nonzero. Then there exists an orthogonal set $\mathbf{v}_1,\ \mathbf{v}_2,\ldots,\mathbf{v}_t \in \mathbb{R}^n$ such that $[\mathbf{u}_1] = [\mathbf{v}_1]$, $[\mathbf{u}_1,\mathbf{u}_2] = [\mathbf{v}_1,\mathbf{v}_2]$, $[\mathbf{u}_1,\mathbf{u}_2,\mathbf{u}_3] = [\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3]$,..., $[\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_t] = [\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_t]$.
Furthermore, the $\mathbf{v}$'s will be nonzero if and only if the $\mathbf{u}$'s are independent.

Proof. We proceed one vector at a time. We start with $\mathbf{v}_1 = \mathbf{u}_1$. Certainly $[\mathbf{u}_1] = [\mathbf{v}_1]$. Now, we subtract the projection of $\mathbf{u}_2$ along $\mathbf{v}_1$, and that will of course give us a vector perpendicular to $\mathbf{v}_1$, so $\mathbf{v}_2 = \mathbf{u}_2 - \dfrac{\mathbf{u}_2\cdot\mathbf{v}_1}{\mathbf{v}_1\cdot\mathbf{v}_1}\mathbf{v}_1$, and indeed $\mathbf{v}_2 \perp \mathbf{v}_1$. Note $\mathbf{v}_1 \neq \mathbf{0}$. Also obvious is the fact that $[\mathbf{u}_1,\mathbf{u}_2] = [\mathbf{v}_1,\mathbf{v}_2]$. Note that $\mathbf{v}_2 = \mathbf{0}$ if and only if $\mathbf{u}_1$ and $\mathbf{u}_2$ are dependent. We now subtract from $\mathbf{u}_3$ its projection along each of $\mathbf{v}_1$ and $\mathbf{v}_2$. Thus, we let

$$\mathbf{v}_3 = \mathbf{u}_3 - \frac{\mathbf{u}_3\cdot\mathbf{v}_1}{\mathbf{v}_1\cdot\mathbf{v}_1}\mathbf{v}_1 - \frac{\mathbf{u}_3\cdot\mathbf{v}_2}{\mathbf{v}_2\cdot\mathbf{v}_2}\mathbf{v}_2,$$

and quickly observe that since $\mathbf{v}_2 \perp \mathbf{v}_1$ already, we also get $\mathbf{v}_1\cdot\mathbf{v}_3 = \mathbf{v}_1\cdot\mathbf{u}_3 - \mathbf{u}_3\cdot\mathbf{v}_1 = 0$, so $\mathbf{v}_3 \perp \mathbf{v}_1$, and similarly $\mathbf{v}_3 \perp \mathbf{v}_2$. And since already $[\mathbf{u}_1,\mathbf{u}_2] = [\mathbf{v}_1,\mathbf{v}_2]$, we additionally get that $[\mathbf{u}_1,\mathbf{u}_2,\mathbf{u}_3] = [\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3]$. Finally, if $\mathbf{v}_3 = \mathbf{0}$, then clearly $\mathbf{u}_3 \in [\mathbf{u}_1,\mathbf{u}_2] = [\mathbf{v}_1,\mathbf{v}_2]$, and equally for the converse, since we are assuming inductively that $\mathbf{v}_1$ and $\mathbf{v}_2$ are orthogonal, and then the lemma above can apply. We can see that we can continue in this fashion, and formally use induction if necessary. ⌘

Observe that if the $\mathbf{u}$'s are orthogonal to start with, the $\mathbf{v}$'s will be exactly the $\mathbf{u}$'s.

Example 5. Consider the following four vectors, $\mathbf{u}_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{u}_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{u}_3 = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ and $\mathbf{u}_4 = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. Then $\mathbf{v}_1 = \mathbf{u}_1$. Now $\hat{\mathbf{v}}_2 = \mathbf{u}_2 - \frac{\mathbf{u}_2 \cdot \mathbf{v}_1}{\mathbf{v}_1 \cdot \mathbf{v}_1}\mathbf{v}_1 = \frac{1}{2}\begin{pmatrix} -1 \\ -1 \\ 2 \\ 0 \\ 0 \end{pmatrix}$, and actually since it is only direction we are interested in, we can actually let $\mathbf{v}_2 = \begin{pmatrix} -1 \\ -1 \\ 2 \\ 0 \\ 0 \end{pmatrix}$.

Now, for the third vector, we need to subtract two projections, $\mathbf{v}_3 = \mathbf{u}_3 - \frac{1}{2}\mathbf{v}_1 - \frac{1}{6}\mathbf{v}_2$, and we get $\hat{\mathbf{v}}_3 = \frac{1}{3}\begin{pmatrix} -1 \\ -1 \\ -1 \\ 3 \\ 0 \end{pmatrix}$, and again we can let $\mathbf{v}_3 = \begin{pmatrix} -1 \\ -1 \\ -1 \\ 3 \\ 0 \end{pmatrix}$. Finally,

$$\mathbf{v}_4 = \mathbf{u}_4 - \frac{\mathbf{u}_4 \cdot \mathbf{v}_1}{\mathbf{v}_1 \cdot \mathbf{v}_1}\mathbf{v}_1 - \frac{\mathbf{u}_4 \cdot \mathbf{v}_2}{\mathbf{v}_2 \cdot \mathbf{v}_2}\mathbf{v}_2 - \frac{\mathbf{u}_4 \cdot \mathbf{v}_3}{\mathbf{v}_3 \cdot \mathbf{v}_3}\mathbf{v}_3,$$

and computing, we get $\mathbf{v}_4 = \mathbf{u}_4 - \frac{1}{2}\mathbf{v}_1 - \frac{1}{6}\mathbf{v}_2 - \frac{1}{12}\mathbf{v}_3$, so $\hat{\mathbf{v}}_4 = \frac{1}{4}\begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ 4 \end{pmatrix}$, so again we can let $\mathbf{v}_4 = \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ 4 \end{pmatrix}$. We are finished finding an orthogonal set.

To develop an orthonormal set, all we need is to divide by the lengths of each of the vectors. Thus from $\mathbf{v}_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{v}_2 = \begin{pmatrix} -1 \\ -1 \\ 2 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{v}_3 = \begin{pmatrix} -1 \\ -1 \\ -1 \\ 3 \\ 0 \end{pmatrix}$ and $\mathbf{v}_4 = \begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ 4 \end{pmatrix}$, we get the following orthonormal set $\mathbf{w}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\\0\\0\\0\end{pmatrix}$, $\mathbf{v}_2 = \frac{1}{\sqrt{6}}\begin{pmatrix}-1\\-1\\2\\0\\0\end{pmatrix}$, $\mathbf{v}_3 = \frac{1}{\sqrt{12}}\begin{pmatrix}-1\\-1\\-1\\3\\0\end{pmatrix}$ and $\mathbf{v}_4 = \frac{1}{\sqrt{20}}\begin{pmatrix}-1\\-1\\-1\\-1\\4\end{pmatrix}$.

The previous algorithm will be crucial to our ultimate pursuit in this section—the question of orthogonal similarity. The next segment will not be so relevant, but for completeness sake, it will be discussed. The issue is to **complete an orthogonal set to an orthogonal basis of** $\mathbb{R}^n$. An example will illuminate thoroughly.

Example 6. Consider the vectors $\mathbf{u} = \begin{pmatrix}-1\\-1\\2\\0\\0\end{pmatrix}$, $\mathbf{v} = \begin{pmatrix}-1\\-1\\-1\\3\\0\end{pmatrix}$ and $\mathbf{w} = \begin{pmatrix}-1\\-1\\-1\\-1\\4\end{pmatrix}$. Can we complete these 3 orthogonal vectors to a set of 5 orthogonal vectors? Clearly to find vectors that are perpendicular to all three vectors, all we need to do is find the null space of the matrix that has these for its rows. Thus, if we let $\mathbf{A} = \begin{pmatrix}-1 & -1 & 2 & 0 & 0\\-1 & -1 & -1 & 3 & 0\\-1 & -1 & -1 & -1 & 4\end{pmatrix}$, we need $\mathbf{N}(\mathbf{A})$. Since $r(\mathbf{A}) = 3$, its nullity is 2. The reduced form of $\mathbf{A}$ is $\begin{pmatrix}1 & 1 & 0 & 0 & -2\\0 & 0 & 1 & 0 & -1\\0 & 0 & 0 & 1 & -1\end{pmatrix}$, so $\begin{pmatrix}-1\\1\\0\\0\\0\end{pmatrix}$ and $\begin{pmatrix}2\\0\\1\\1\\1\end{pmatrix}$ is a basis for $\mathbf{N}(\mathbf{A})$. These two vectors are orthogonal to all three of our previous vectors. However, they are not perpendicular to each other! But Gram-Schmidt comes to our rescue—we obtain $\begin{pmatrix}-1\\1\\0\\0\\0\end{pmatrix}$ and $\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix}$ when we run the two vectors through the process. And now we do have 5 orthogonal vectors in $\mathbb{R}^5$.

We have basically shown:

> **Corollary.** Every orthonormal set can be extended to an orthonormal basis. Equivalently, if $\mathbf{u}_1$, $\mathbf{u}_2, \ldots, \mathbf{u}_t \in \mathbb{R}^n$ are orthonormal, then there exists an orthogonal matrix $\mathbf{P}$ such that its first t columns are the $\mathbf{u}$'s.

Thus starting with $\frac{1}{\sqrt{6}}\mathbf{u}$, $\frac{1}{\sqrt{12}}\mathbf{v}$ and $\frac{1}{\sqrt{20}}\mathbf{w}$ from the previous example, we could obtain the matrix $\mathbf{P}=\begin{pmatrix} \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{5}} \\ \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{6}} & \frac{-1}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & 0 & \frac{1}{\sqrt{5}} \\ 0 & \frac{3}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & 0 & \frac{1}{\sqrt{5}} \\ 0 & 0 & \frac{4}{\sqrt{20}} & 0 & \frac{1}{\sqrt{5}} \end{pmatrix}$.

The previous example illustrated once again the power of null spaces and linear systems. We take the opportunity to give a different and newer application of these ideas. We will be doing arithmetic mod 2, or in $\mathbb{Z}_2$, as is known in the mathematics world. Basically we only have two scalars 0 and 1, and the only unexpected fact is that $1+1=0$ (we are in a 2-hour clock).

Example 7. In the 1950's, when computers were rather primitive and unavailable, the staff at **AT&T** used weekends to run many of their programs. A constant source of irritation to many of them was returning on Monday and finding out their program hadn't run, not because there was some mistake in it, but because the computer had misread some digit some time during the running of the program. It was at this juncture that **Hamming** (of the **Hamming** distance) decided to add some redundancy bits to their transmission. Of course there were many options: parity checks of any length. The advantage of a parity check scheme is that it is very economical—one redundancy bit for any number of meaningful bits that one chooses. The problem with a parity check is that although it is good at detecting one error, there is no way of decoding that one error, of correcting it. Hamming came up with a very ingenious code named after him.

The idea was simple, start with the null space of the matrix $\mathbf{M}=\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ (all mod 2), and the matrix may look a little mysterious, but its columns are simply the numbers 1 through 7 written in base 2. Since we can see three pivots, we have full row rank, so its null space has dimension 4, and its null space is given by (if we solve for the pivotal as they are and recall that $1=-1$):

$$x_3\begin{pmatrix}1\\1\\1\\0\\0\\0\\0\end{pmatrix}+x_5\begin{pmatrix}1\\0\\0\\1\\1\\0\\0\end{pmatrix}+x_6\begin{pmatrix}0\\1\\0\\1\\0\\1\\0\end{pmatrix}+x_7\begin{pmatrix}1\\1\\0\\1\\0\\0\\1\end{pmatrix}$$

and since each of the scalars can take 2 values, there are a total of 16 **code** words in the Hamming code. They are (given without parentheses)

0	1	1	0	1	0	1	0	1	0	1	0	1	0	0	1
0	1	0	1	1	1	0	0	1	1	0	0	0	1	0	1
0	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1
0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1.
0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1
0	0	0	1	0	0	1	0	1	0	1	1	0	1	1	1
0	0	0	0	1	0	0	1	0	1	1	0	1	1	1	1

And at first the virtues of the code are hidden. But the idea is to use only these as possible words to communicate, so there are 16 possible messages. Suppose now that a word is received (I actually flipped a coin to come up with this word): **1010011**. Then without concern of whether an error was committed in the transmission of the message, one multiplies the received word by the matrix $\mathbf{M}$, if one gets 0, then the word is a code word, and so one accepts it as the sent message. But if not, then we know that as what was sent was $\mathbf{w}$ which satisfies $\mathbf{Mw} = \mathbf{0}$, assuming only one error was committed, then what we received was the word, $\mathbf{w} + \mathbf{e}_i$ where $\mathbf{e}_i$ is one of the columns of the identity. But $\mathbf{M}(\mathbf{w} + \mathbf{e}_i) = \mathbf{Me}_i$, and since this is just the i^{th} column of $\mathbf{M}$, we can correct the error.

Thus, in our specific case, we have $\mathbf{M}\begin{pmatrix}1\\0\\1\\0\\0\\1\\1\end{pmatrix} = \begin{pmatrix}0\\1\\1\end{pmatrix}$, and since this is the number 3 in base 2,

we know the error occurred in the third position, so the corrected message is $\begin{pmatrix}1\\0\\0\\0\\0\\1\\1\end{pmatrix}$, one of our code words indeed, and one can also verify that is the only word that could have been sent where only one error occurred. Of course we could have seen this example as the set of vectors orthogonal to the three vectors, $\begin{pmatrix}0\\0\\0\\1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\\1\\0\\1\end{pmatrix}$, the rows of $\mathbf{M}$. Note that these three are words in the code, so that in fact each of them is perpendicular to itself, as well as to the other two: $\mathbf{MM}^{\mathrm{T}} = \mathbf{0}$. This could not have occurred if we had been dealing with real scalars.

We now continue to the fundamental theorem of the section. We show that **every symmetric matrix is not only diagonable, but the diagonal matrix can be achieved via an orthogonal matrix**—thus not only the algebraic properties of the symmetric matrix are preserved, but also the geometric ones. Before we prove the fundamental theorem, we will need three lemmas.

We saw before that eigenvectors of any matrix corresponding to different eigenvalues are independent. For a symmetric matrix much more is true.

> **Lemma (Orthogonality of Eigenvectors).** Let $\mathbf{A}$ be symmetric. Suppose $\mathbf{u}$ and $\mathbf{v}$ are eigenvectors of $\mathbf{A}$ corresponding to eigenvalues λ and μ, respectively. If $\lambda \neq \mu$, then $\mathbf{u} \perp \mathbf{v}$.

Proof.. Now $\mathbf{Au}_1 = \lambda_1 \mathbf{u}_1$ and $\mathbf{Au}_2 = \lambda_2 \mathbf{u}_2$, and $\lambda_1 \neq \lambda_2$. By transposing the second equation we get $\mathbf{u}_2^{\mathrm{T}} \mathbf{A}^{\mathrm{T}} = \lambda_2 \mathbf{u}_2^{\mathrm{T}}$, but since $\mathbf{A} = \mathbf{A}^{\mathrm{T}}$, we have $\mathbf{u}_2^{\mathrm{T}} \mathbf{A} = \lambda_2 \mathbf{u}_2^{\mathrm{T}}$. Now $\lambda_1 \mathbf{u}_2^{\mathrm{T}} \mathbf{u}_1 = \mathbf{u}_2^{\mathrm{T}} (\mathbf{Au}_1) = (\mathbf{u}_2^{\mathrm{T}} \mathbf{A}) \mathbf{u}_1 = \lambda_2 \mathbf{u}_2^{\mathrm{T}} \mathbf{u}_1$, and so we can conclude $\mathbf{u}_2^{\mathrm{T}} \mathbf{u}_1 = 0$. ⌘

Example 8. Let $\mathbf{A} = \begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix}$. Then one eigenvalue is 6 with eigenvector $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ while the other eigenvalue is -4 with eigenvector $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Remarkably, **any symmetric matrix has real eigenvalues**. The 2×2 case is simple: if we let $\mathbf{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$, then $c_A(x) = ac - b^2 - (a+c)x + x^2$, and the roots of this quadratic are given by $x = \dfrac{(a+c) \pm \sqrt{(a+c)^2 - 4(ac - b^2)}}{2}$, but the discriminant is $(a-c)^2 + 4b^2$ which is clearly positive, and so the equation has real roots. To prove this in full generality would require more exploration of the complex numbers, so we state the result with a proof in the **Appendix of Proofs**.

> **Lemma (Real Eigenvalues).** Let $\mathbf{A}$ be a real symmetric matrix. Then $\mathbf{A}$ has real eigenvalues.

The last of the three lemmas is the most fundamental. We saw before that any real matrix with real eigenvalues was similar to an upper triangular matrix. Now we prove something more powerful—the similarity can be accomplished via an orthogonal matrix!

Lemma (Schur's Lemma). Let $\mathbf{A}$ have real eigenvalues. Then there exists an orthogonal matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P} = \mathbf{T}$, an upper triangular matrix.

The proof can be found in the Appendix of Proofs.

Putting the lemmas together we obtain the major theorem of the section:

Theorem (Spectral Theorem). Let $\mathbf{A}$ be a symmetric matrix. Then there exists an orthogonal matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P} = \mathbf{D}$, a diagonal matrix.

Proof. The only thing needed is to show that we actually obtain a diagonal matrix out of Schur's Lemma. But then from the fact that $\mathbf{A}$ is symmetric, and $\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P} = \mathbf{T}$, we immediately get that $\mathbf{T}$ is symmetric, and since it is upper triangular, it means it is diagonal. ⌘

Example 9. Let $\mathbf{A} = \mathbf{J}_5$. Then previous examples have already done all the work. The eigenspace for 0 is 4-dimensional with basis $\mathbf{u}_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{u}_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{u}_3 = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ and $\mathbf{u}_4 = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, while $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ is an eigenvector for 5 (note the perpendicularity among the eigenspaces), so using Gram-Schmidt, we get, as before, $\mathbf{P} = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & \frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & \frac{1}{\sqrt{5}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{-1}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & \frac{1}{\sqrt{5}} \\ 0 & 0 & \frac{3}{\sqrt{12}} & \frac{-1}{\sqrt{20}} & \frac{1}{\sqrt{5}} \\ 0 & 0 & 0 & \frac{4}{\sqrt{20}} & \frac{1}{\sqrt{5}} \end{pmatrix}$.

Example 10. Let $\mathbf{A} = \begin{pmatrix} 7 & 5 & -8 & 2 \\ 5 & 31 & -40 & 10 \\ -8 & -40 & 70 & -16 \\ 2 & 10 & -16 & 10 \end{pmatrix}$. Then since all rows add to 6, this has to be an eigenvalue. Looking for its eigenvectors, we are concerned with $\mathbf{N}(\mathbf{A} - 6\mathbf{I})$ and since

$\mathbf{A}-6\mathbf{I}=\begin{pmatrix}1 & 5 & -8 & 2\\ 5 & 25 & -40 & 10\\ -8 & -40 & 64 & -16\\ 2 & 10 & -16 & 4\end{pmatrix}$ has rank 1, 6 occurs 3 times as an eigenvalue. By the trace, the other eigenvalue is 100. An eigenvector for 100 is $\begin{pmatrix}1\\5\\-8\\2\end{pmatrix}$. Looking for eigenvectors for 6, we get the null space $\mathbf{N}(\mathbf{A}-6\mathbf{I})$ to have basis $\begin{pmatrix}-5\\1\\0\\0\end{pmatrix}$, $\begin{pmatrix}8\\0\\1\\0\end{pmatrix}$ and $\begin{pmatrix}-2\\0\\0\\1\end{pmatrix}$. But suppose we wanted $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ to be part of the basis, then we could use $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$, $\begin{pmatrix}-5\\1\\0\\0\end{pmatrix}$ and $\begin{pmatrix}-2\\0\\0\\1\end{pmatrix}$ (we have many other choices, this was done arbitrarily). Applying the Gram-Schmidt process to these three vectors, we get $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$, $\begin{pmatrix}-4\\2\\1\\1\end{pmatrix}$ and $\begin{pmatrix}-5\\-25\\-7\\37\end{pmatrix}$. So our orthogonal diagonalizing matrix is

$$\mathbf{P}=\begin{pmatrix}\frac{1}{2} & \frac{-4}{\sqrt{22}} & \frac{-5}{2\sqrt{517}} & \frac{1}{\sqrt{94}}\\ \frac{1}{2} & \frac{2}{\sqrt{22}} & \frac{-25}{2\sqrt{517}} & \frac{5}{\sqrt{94}}\\ \frac{1}{2} & \frac{1}{\sqrt{22}} & \frac{-7}{2\sqrt{517}} & \frac{-8}{\sqrt{94}}\\ \frac{1}{2} & \frac{1}{\sqrt{22}} & \frac{37}{2\sqrt{517}} & \frac{2}{\sqrt{94}}\end{pmatrix}.$$

One of the original interests in eigenvalues was motivated by the study of the conic sections in the plane, and so we appropriately end the course with a thorough discussion on them.

On Conics

We all know that the general linear equation $ax+by=e$ is the algebraic representation of a straight line. What is the next level of complexity? For over two thousand years, humanity has been interested in quadratics (the next level). What is the most general quadratic equation on x and y? Simply

$$ax^2+2bxy+cy^2+dx+ey=f$$

where not all of the coefficients are 0. The reasons for the doubling of the coefficient of xy will become clearer below. And for many generations this was the way this equation was viewed. But we now have matrices at our disposal, and so we have more powerful notation at our disposal. If we let $\mathbf{M}=\begin{pmatrix} a & b \\ b & c \end{pmatrix}$, and if we let $\mathbf{c}=\begin{pmatrix} d \\ e \end{pmatrix}$ and $\mathbf{z}=\begin{pmatrix} x \\ y \end{pmatrix}$, then our quadratic equation simply becomes

$$\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{z}+\mathbf{z}^{\mathrm{T}}\mathbf{c}=f$$

(this is the reason for the 2 in the coefficient). Even more succinctly, we let $\mathfrak{C}(\mathbf{M},\mathbf{c},f)$ denote the set of solutions to the equation. This set of solutions is called a **conic**—although some do not quite fit our idea of such a curve due to very special cases. As we will see below, the matrix $\mathbf{M}$ plays the major role in identifying the curve.

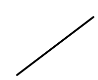
Note that $\mathbf{M}$ is a symmetric matrix, $\mathbf{M}=\mathbf{M}^{\mathrm{T}}$. Since for any nonzero scalar a,

$$\mathfrak{C}(\mathbf{M},\mathbf{c},f)=\mathfrak{C}(a\mathbf{M},a\mathbf{c},af),$$

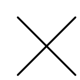
we have some freedom in choosing the $\mathbf{M}$. In particular, we can always choose the matrix $\mathbf{M}$ so that $\operatorname{tr}\mathbf{M}\geq 0$.

Examples. Mostly expected, but some unusual.

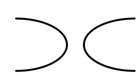
❶ If $\mathbf{M}=\mathbf{0}$, we get a linear equation, so we have a straight line. Thus linear equations are special cases of the quadratic.



❷ Consider the equation $x^2-y^2=0$. Here $\mathbf{M}=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\mathbf{c}=\mathbf{0}$ and $f=0$.

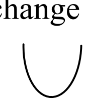


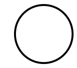
This is the union of two lines, the line $x=y$ and the line $x=-y$.
Changing to $f=1$ produces a hyperbola $x^2-y^2=1$:



❸ When $\mathbf{M}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\mathbf{c}=\mathbf{0}$ and $f=1$, we get the equation $x^2=1$ which represents two parallel vertical lines, $x=1$ and $x=-1$.

While if we change to $\mathbf{c}=\begin{pmatrix} 0 \\ -1 \end{pmatrix}$, we get the equation $x^2-y=1$, which represents a parabola:



❹ When $\mathbf{M}=\mathbf{I}$, the identity, $\mathbf{c}=\mathbf{0}$ and $f=1$, we get the unit circle: $x^2+y^2=1$  while changing to $f=0$ will produce $x^2+y^2=0$, a single point, ● and decreasing *f* further will empty the collection altogether.

On the other hand changing the original to $\mathbf{M}=\begin{pmatrix}1&0\\0&4\end{pmatrix}$, will produce the equation $x^2+4y^2=1$ which represents an ellipse. 

Points are said to be **collinear** if they lie on a line. Of course from previous work, we know that points $\begin{pmatrix}x_i\\y_i\end{pmatrix}$ for $i=1,\dots,t$ are collinear if and only if $\begin{pmatrix}x_1&y_1&-1\\x_2&y_2&-1\\\vdots&\vdots&\vdots\\x_t&y_t&-1\end{pmatrix}$ has rank at most 2.

We know that **two points determine a line**, but **five points determine a conic**.

Theorem (Five Points). Any five points lie on a conic. Moreover, the conic is unique if and only if no four of the points are collinear.

Proof. Let $\begin{pmatrix}x_i\\y_i\end{pmatrix}$ for $i=1,\dots,5$ be 5 different points in the plane. Consider the 5×6 matrix $\mathbf{A}=\begin{pmatrix}x_1^2&2x_1y_1&y_1^2&x_1&y_1&-1\\x_2^2&2x_2y_2&y_2^2&x_2&y_2&-1\\x_3^2&2x_3y_3&y_3^2&x_3&y_3&-1\\x_4^2&2x_4y_4&y_4^2&x_4&y_4&-1\\x_5^2&2x_5y_5&y_5^2&x_5&y_5&-1\end{pmatrix}$. In order to find *a*, *b*, *c*, *d*, *e*, and *f*, we need to solve $\mathbf{Ax}=\mathbf{0}$, which is a homogeneous linear system of 5 equations on 6 unknowns. Since the rank is at most 5, there is a nontrivial solution. The conic will be unique if and only if the rank is 5. The proof that the rank is 5 exactly when no four points are collinear can be found in the **Appendix of Proofs**.

Example 1. We find the conic that goes through the points, $\begin{pmatrix}0\\0\end{pmatrix}$, $\begin{pmatrix}0\\1\end{pmatrix}$, $\begin{pmatrix}1\\1\end{pmatrix}$, $\begin{pmatrix}0\\2\end{pmatrix}$ and $\begin{pmatrix}4\\0\end{pmatrix}$. We need to solve the homogeneous system $\mathbf{Ax}=\mathbf{0}$ where $\mathbf{A}$ is $\begin{pmatrix}0&0&0&0&0&-1\\0&0&1&0&1&-1\\1&2&1&1&1&-1\\0&0&4&0&2&-1\\16&0&0&4&0&-1\end{pmatrix}$, which leads to the equation $x^2+3xy-4x=0$. The parameters $\mathfrak{C}(\mathbf{M},\mathbf{c},f)$ are $\mathbf{M}=\begin{pmatrix}1&1.5\\1.5&0\end{pmatrix}$,

$\mathbf{c}=\begin{pmatrix}-4\\0\end{pmatrix}$ and $f=0$. This is the union of two lines: $x=0$ and $x+3y=4$.

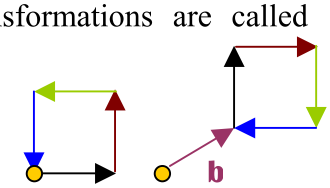
Example 2. Similarly the conic that goes through the points, $\begin{pmatrix}1\\0\end{pmatrix}$, $\begin{pmatrix}2\\5\end{pmatrix}$, $\begin{pmatrix}1\\2\end{pmatrix}$, $\begin{pmatrix}3\\3\end{pmatrix}$ and $\begin{pmatrix}4\\0\end{pmatrix}$ is given by $75x^2+24xy+2y^2-375x-28y=-300$, obtained by solving the system $\mathbf{Ax}=\mathbf{0}$ where $\mathbf{A}$ is given by $\begin{pmatrix}1&0&0&1&0&-1\\4&20&25&2&5&-1\\1&4&4&1&2&-1\\9&18&9&3&3&-1\\16&0&0&4&0&-1\end{pmatrix}$. The parameters $\mathfrak{C}(\mathbf{M},\mathbf{c},f)$ are $\mathbf{M}=\begin{pmatrix}75&12\\12&2\end{pmatrix}$, $\mathbf{c}=\begin{pmatrix}-375\\-28\end{pmatrix}$ and $f=-300$. We will see below this is an ellipse.

The acute reader will have observed that in the list of examples above, all the $\mathbf{M}$'s listed were diagonal matrices, and indeed from the geometric points of view that is all that is needed—that is what we settle next.

We have seen before the transformations $f_{\mathbf{A}}$ for a given matrix $\mathbf{A}$. We extend the idea by inserting a translational component into the function.

Let $\mathbf{A}$ be a 2×2 matrix, and $\mathbf{b}$ any vector, then the function $\mathbf{x}\mapsto\mathbf{Ax}+\mathbf{b}$ is called an **affine** function. We will refer to this function by $F_{\mathbf{A},\mathbf{b}}$, so $F_{\mathbf{A},\mathbf{b}}(\mathbf{x})=\mathbf{Ax}+\mathbf{b}$. Of course, if $\mathbf{b}=\mathbf{0}$, then $F_{\mathbf{A},\mathbf{b}}=f_{\mathbf{A}}$. We will only be interested in these when $\mathbf{A}$ is an invertible matrix, and then they are called **affine transformations**.

Example 3. A simple, yet important, family of affine transformations are called **translations**. For a fixed vector $\mathbf{b}$, the translation by $\mathbf{b}$ is the mapping that sends $\mathbf{x}\mapsto\mathbf{x}+\mathbf{b}$. So here the matrix is the identity, $\mathbf{A}=\mathbf{I}$. Note these transformations preserve distance, angles and shape.



Suppose we are given an affine transformation, $F_{\mathbf{A},\mathbf{b}}$, how does it transform a conic such as $\mathfrak{C}(\mathbf{M},\mathbf{c},f)$? The following theorem establishes the basic facts:

Theorem (Affine Transformations & Conics). Let $\mathbf{A}$ be an invertible matrix and let $\mathbf{b}$ be any vector. Then

① $F_{\mathbf{A},\mathbf{0}}\left(\mathfrak{C}(\mathbf{M},\mathbf{c},f)\right)=\mathfrak{C}(\mathbf{N},\mathbf{d},f)$ where

$$\mathbf{N}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{MA}^{-1} \text{ and } \mathbf{d}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}.$$

② $F_{\mathbf{I},\mathbf{b}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)=\mathfrak{C}\left(\mathbf{M},\mathbf{e},g\right)$ where

$$\mathbf{e}=\mathbf{c}-2\mathbf{Mb} \text{ and } g=f+\mathbf{b}\cdot\mathbf{c}-\mathbf{b}^{\mathrm{T}}\mathbf{Mb}.$$

So combining ① and ②, we get

③ $F_{\mathbf{A},\mathbf{b}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)=\mathfrak{C}\left(\mathbf{N},\mathbf{k},h\right)$ where

$$\mathbf{N}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{MA}^{-1},\ \mathbf{k}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}-2\mathbf{Nb} \text{ and}$$

$$h=f+\mathbf{b}\cdot\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}-\mathbf{b}^{\mathrm{T}}\mathbf{Nb}.$$

The proof of this technical result can be found in the usual Appendix of Proofs.

Example 4. Consider the unit circle, $\mathfrak{C}\left(\mathbf{I},\mathbf{0},1\right)$ with equation $x^2+y^2=1$. Let $\mathbf{A}=\begin{pmatrix}1&0\\0&\frac{1}{2}\end{pmatrix}$ and $\mathbf{b}=\begin{pmatrix}-1\\3\end{pmatrix}$. Then $F_{\mathbf{A},\mathbf{b}}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}x-1\\\frac{1}{2}y+3\end{pmatrix}=F_{\mathbf{I},\mathbf{b}}\circ F_{\mathbf{A},\mathbf{0}}\begin{pmatrix}x\\y\end{pmatrix}$. By the theorem the image of the unit circle, the points $\begin{pmatrix}a-1\\\frac{1}{2}b+3\end{pmatrix}$ where $a^2+b^2=1$ will all lie in and fill the conic $\mathfrak{C}\left(\mathbf{N},\mathbf{k},h\right)$ where

$$\mathbf{N}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{MA}^{-1}=\begin{pmatrix}1&0\\0&4\end{pmatrix},\ \mathbf{k}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}-2\mathbf{Nb}=\begin{pmatrix}2\\-24\end{pmatrix}$$

$$\text{and } h=f+\mathbf{b}\cdot\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}-\mathbf{b}^{\mathrm{T}}\mathbf{Nb}=-36.$$

And this conic has equation $x^2+4y^2+2x-24y=-36$. Indeed,

$$\left(a-1\right)^2+4\left(\tfrac{1}{2}b+3\right)^2+2\left(a-1\right)-24\left(\tfrac{1}{2}b+3\right)=$$
$$a^2-2a+1+b^2+12b+36+2a-2-12b-72=1+1+36-2-72=-36.$$

Since this transformation changed scales in one axis we should not be surprised the result is an ellipse.

But note the crucial observation, the change in the matrix is $\mathbf{M}\mapsto\mathbf{N}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{MA}^{-1}$, and this is a similarity only when the matrix $\mathbf{A}$ is an orthogonal matrix. It is these that we are particularly interested since these will not change distances and angles, and if we always choose the determinant to be positive, they will not change orientation either—in fact, any such matrix is a simple rotation. But by the Spectral Theorem we know that any symmetric matrix can be diagonalized by an orthogonal matrix (and we can always choose the determinant to be 1), so we know that every conic section can be rotated to one where the matrix is diagonal, and we have begun to understand all conics.

First we need a technical fact about eigenvalues and eigenvectors of matrices:

> **Theorem (Eigenvectors).** Let $\mathbf{M} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ be a 2×2 symmetric matrix. Let $d = (a-c)^2 + 4b^2$. Then the eigenvalues of $\mathbf{M}$ are $\lambda = \frac{1}{2}\left(a+c+\sqrt{d}\right)$ and $\mu = \frac{1}{2}\left(a+c-\sqrt{d}\right)$ with corresponding eigenvectors: $\mathbf{u} = \begin{pmatrix} a-c+\sqrt{d} \\ 2b \end{pmatrix}$ and $\mathbf{v} = \begin{pmatrix} -2b \\ a-c+\sqrt{d} \end{pmatrix}$. Moreover, $\mathbf{P} = \dfrac{1}{\sqrt{2\left(d+(a-c)\sqrt{d}\right)}}\begin{pmatrix} \mathbf{u} & \mathbf{v} \end{pmatrix}$ is an orthogonal matrix of determinant 1, and $\mathbf{P}^{\mathrm{T}}\mathbf{MP} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$

Proof. It is straightforward to verify that $\mathbf{Mu} = \lambda\mathbf{u}$. By trace considerations, the other eigenvalue is μ. Clearly $\mathbf{u} \perp \mathbf{v}$, so it must be the case that $\mathbf{Mv} = \mu\mathbf{v}$. Now, $\sqrt{2\left(d+(a-c)\sqrt{d}\right)}$ is the length of both $\mathbf{u}$ and $\mathbf{v}$, so the columns of $\mathbf{P}$ form an orthonormal basis, so $\mathbf{P}$ is an orthogonal matrix such that $\mathbf{P}^{\mathrm{T}}\mathbf{MP} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$. All that remains is to show that $\mathbf{P}$ has positive determinant—but that follows from the fact $\sqrt{d} \geq |a-c|$. ⌘

Note that since $\mathbf{P}$ is orthogonal of determinant 1, $\mathbf{P}$ has to be a rotation of the form $\mathbf{P}_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Can we describe θ in terms of $\mathbf{M} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$? Obviously $\tan\theta = \dfrac{2b}{a-c+\sqrt{d}}$, and although that expression is not that friendly, if one uses the fact from trigonometry, $\tan 2\theta = \dfrac{2\tan\theta}{1-\tan^2\theta}$, one arrives at the more recognizable

$$\tan 2\theta = \frac{2b}{a-c}.$$

As an immediate consequence we get

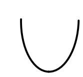
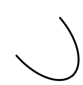
> **Theorem (Diagonability).** Consider an arbitrary conic $\mathfrak{C}(\mathbf{M},\mathbf{c},f)$ where $\mathbf{M} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Let $\mathbf{N} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ where λ and μ are the eigenvalues of $\mathbf{M}$. Let θ satisfy $\tan 2\theta = \dfrac{2b}{a-c}$. Then if $\mathbf{A}$ denotes the rotation about the origin by angle $-\theta$. Then $F_{\mathbf{A},\mathbf{0}}$ will transform $\mathfrak{C}(\mathbf{M},\mathbf{c},f)$ into $\mathfrak{C}(\mathbf{N},\mathbf{d},f)$ where $\mathbf{d} = \left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}$.

In reality, we do not need to find θ by the expression $\tan 2\theta = \dfrac{2b}{a-c}$ since it is really coming from the eigenvectors of $\mathbf{M}$. Note that $\mathbf{A} = \mathbf{P}^{-1}$ where $\mathbf{P}$ is the orthogonal diagonalizing matrix for $\mathbf{M}$ since $\mathbf{N} = \left(\mathbf{A}^{-1}\right)^{\mathrm{T}} \mathbf{M}\mathbf{A}^{-1}$ .So we could have another version of the above theorem.

> **Theorem (Diagonability II).** Consider an arbitrary conic $\mathfrak{C}(\mathbf{M}, \mathbf{c}, f)$ where $\mathbf{M} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Let $\mathbf{N} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ where λ and μ are the eigenvalues of $\mathbf{M}$. Let $\mathbf{u}$ be a unit eigenvector for λ, and $\mathbf{v}$ a unit eigenvector for μ. Let $\mathbf{P} = \begin{pmatrix} \mathbf{u} & \mathbf{v} \end{pmatrix}$. Then $F_{\mathbf{P}^{\mathrm{T}}, \mathbf{0}}$ will transform $\mathfrak{C}(\mathbf{M}, \mathbf{c}, f)$ into $\mathfrak{C}(\mathbf{N}, \mathbf{d}, f)$ where $\mathbf{d} = \mathbf{P}^{\mathrm{T}}\mathbf{c}$.

Example 5. Consider the quadratic $x^2 + 2xy + y^2 + 8x - 8y = 0$. Here $\mathbf{M} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $\mathbf{c} = \begin{pmatrix} 8 \\ -8 \end{pmatrix}$ and $f = 0$. The eigenvalues of $\mathbf{M}$ are 2 and 0 with respective eigenvectors $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$. Thus we know θ is 45° and $\mathbf{P} = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$. Hence

$$\mathbf{A} = \mathbf{P}^{-1} = \mathbf{P}^{\mathrm{T}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

We have then $\mathbf{N} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$, and $\mathbf{d} = \left(\mathbf{A}^{-1}\right)^{\mathrm{T}} \mathbf{c} = \mathbf{A}\mathbf{c} = \dfrac{-1}{\sqrt{2}}\begin{pmatrix} 0 \\ 16 \end{pmatrix}$, so the equation for $\mathfrak{C}(\mathbf{N}, \mathbf{d}, f)$ becomes $2x^2 - \dfrac{16}{\sqrt{2}}y = 0$, or equivalently $y = \dfrac{\sqrt{2}}{8}x^2$, which has the parabolic shape, 
and since this graph was obtained by rotating by -45°, the original parabola was shaped as (recall all rotations are counter-clock-wise): 

We have been rather unconcerned about dividing by 0 in the algebra above. We now address all situations. Throughout we let $\mathbf{M} = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \neq \mathbf{0}$.

Example 6. The case $\mathbf{M} = \mathbf{I}$. The only time $d = (a-c)^2 + 4b^2$ is zero occurs when $\mathbf{M}$ is a scalar matrix, and since we can always multiply by a scalar, we can assume $\mathbf{M} = \mathbf{I}$. If this is the case, let $\mathbf{b} = \frac{1}{2}\mathbf{c}$. By **Transformation Theorem**, $F_{\mathbf{I}, \mathbf{b}}\left(\mathfrak{C}(\mathbf{I}, \mathbf{c}, f)\right) = \mathfrak{C}(\mathbf{I}, \mathbf{0}, g)$ where $g = f + \frac{1}{4}\mathbf{c} \cdot \mathbf{c}$, and this is either a circle ($g > 0$), a point ($g = 0$) or empty, otherwise.

Example 7. *The case* $\det \mathbf{M} = 0$. We have $\mathfrak{C}(\mathbf{M}, \mathbf{c}, f)$ with $\det \mathbf{M} = 0$. Without loss, since we can always multiply by a scalar, we can assume the eigenvalues of $\mathbf{M}$ are 1 and 0. Let $\mathbf{u}$ be a unit eigenvector for $\lambda = 1$, and $\mathbf{v}$ a unit vector in the null space. Let $\mathbf{P} = (\mathbf{u} \quad \mathbf{v})$. Consider $\mathbf{P}^{\mathrm{T}}\mathbf{c} = \begin{pmatrix} m \\ n \end{pmatrix}$. Let $\mathbf{b} = \frac{1}{2}\begin{pmatrix} m \\ 0 \end{pmatrix}$. Then $F_{\mathbf{P}^{\mathrm{T}}, \mathbf{b}}\left(\mathfrak{C}(\mathbf{M}, \mathbf{c}, f)\right) = \mathfrak{C}(\mathbf{N}, \mathbf{k}, h)$ where $\mathbf{N} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $h = f + \frac{1}{4}m^2$ and $\mathbf{k} = \mathbf{P}^{\mathrm{T}}\mathbf{c} - 2\mathbf{N}\mathbf{b} = \begin{pmatrix} m \\ n \end{pmatrix} - \begin{pmatrix} m \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ n \end{pmatrix}$. Thus the equation simply becomes

$$x^2 + ny = f + \tfrac{1}{4}m^2.$$

Two cases occur then, one when $n = 0$, which is tantamount to $\mathbf{P}^{\mathrm{T}}\mathbf{c} \in \mathcal{C}(\mathbf{N})$, or equivalently, $\mathbf{c} \in \mathcal{C}(\mathbf{M})$, and then the equation simply becomes $x^2 = h$, and this will represent either two parallel vertical lines, or a point, or an empty set. Second, $n \neq 0$, and then we can see the equation as a parabola, depending on the sign of n: 

Example 8. Consider $4x^2 - 4xy + y^2 + 6x - 3y = 12$. Here $\mathbf{M} = \begin{pmatrix} 4 & -2 \\ -2 & 1 \end{pmatrix}$, which has determinant 0 and since $\mathbf{c} = \begin{pmatrix} 6 \\ -3 \end{pmatrix} \in \mathcal{C}(\mathbf{M})$, we know we will have two parallel lines. On the other hand, the equation $4x^2 - 4xy + y^2 + 5x - 3y = 12$ will represent a parabola.

We are left to consider the situation when $\mathbf{M}$ is invertible (not the identity) and so its eigenvalues are nonzero, and different.

Example 9. *The case* $\det \mathbf{M} \neq 0$. We have $\mathfrak{C}(\mathbf{M}, \mathbf{c}, f)$ with $\det \mathbf{M} \neq 0$. Let λ and μ be its eigenvalues. Let $\mathbf{u}$, $\mathbf{v}$, $\mathbf{P}$, and $\mathbf{N}$ be as usual. Let $\mathbf{b} = \frac{1}{2}\mathbf{N}^{-1}\mathbf{P}^{\mathrm{T}}\mathbf{c}$. Then $F_{\mathbf{P}^{\mathrm{T}}, \mathbf{b}}\left(\mathfrak{C}(\mathbf{M}, \mathbf{c}, f)\right) = \mathfrak{C}(\mathbf{N}, \mathbf{0}, h)$, and $h = f + \mathbf{b} \cdot \mathbf{P}^{\mathrm{T}}\mathbf{c} - \mathbf{b}^{\mathrm{T}}\mathbf{N}\mathbf{b} = f + \frac{1}{4}\mathbf{c}^{\mathrm{T}}\mathbf{M}^{-1}\mathbf{c}$. So our equation reduces to one of the form

$$\lambda x^2 + \mu y^2 = h$$

and if $\lambda\mu > 0$, then this is either an ellipse, or a point ($h = 0$), or empty, while if $\lambda\mu < 0$, then this is a hyperbola or two intersecting lines ($h = 0$).

Example 10. Consider $2x^2 + 6xy + 5y^2 + 8x + 8y = f$. Now $\mathbf{M} = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$ has $\dfrac{7 \pm 3\sqrt{5}}{2}$ for its eigenvalues, both positive. Now $h = f + \frac{1}{4}\mathbf{c}^{\mathrm{T}}\mathbf{M}^{-1}\mathbf{c}$ and since $\mathbf{M}^{-1} = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}$, we have $h = f + 2$. So if $f > -2$ we have an ellipse while $f = -2$ produces a point.

Consider $112x^2 - 74\sqrt{3}xy + 38y^2 + x + y = f$. Here $\mathbf{M} = \begin{pmatrix} 112 & -37\sqrt{3} \\ -37\sqrt{3} & 38 \end{pmatrix}$, which has clearly positive determinant. The eigenvalues are 149 and 1, so $\mathbf{u} = \frac{1}{2}\begin{pmatrix} \sqrt{3} \\ -1 \end{pmatrix}$ and $\mathbf{v} = \frac{1}{2}\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$, so $\mathbf{P} = \frac{1}{2}\begin{pmatrix} \sqrt{3} & 1 \\ -1 & \sqrt{3} \end{pmatrix}$. But then $\mathbf{M}^{-1} = \frac{1}{149}\begin{pmatrix} 38 & 37\sqrt{3} \\ 37\sqrt{3} & 112 \end{pmatrix}$, and so $h = f + \frac{1}{298}\left(75 + 37\sqrt{3}\right)$. So if $f = -\frac{1}{298}\left(75 + 37\sqrt{3}\right)$, we have a point, while for any bigger *f*'s, we have an ellipse (very thin). For smaller *f*'s we have no graph at all.

Consider now $9x^2 + 34\sqrt{3}xy + 43y^2 + x + y = f$. The matrix is $\mathbf{M} = \begin{pmatrix} 9 & 17\sqrt{3} \\ 17\sqrt{3} & 43 \end{pmatrix}$ which has negative determinant. The eigenvalues are 60 and -8, so $\mathbf{u} = \frac{1}{2}\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$, $\mathbf{v} = \frac{1}{2}\begin{pmatrix} -\sqrt{3} \\ 1 \end{pmatrix}$, so $\mathbf{P} = \frac{1}{2}\begin{pmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$. But then $\mathbf{M}^{-1} = \frac{1}{480}\begin{pmatrix} -43 & 17\sqrt{3} \\ 17\sqrt{3} & -9 \end{pmatrix}$, and so $h = f + \frac{1}{960}\left(-26 + 17\sqrt{3}\right)$. Thus, when $f = \frac{1}{960}\left(26 - 17\sqrt{3}\right)$, we will have two intersecting lines, and otherwise, we will have a hyperbola.

In summary, given a conic $\mathfrak{C}\left(\mathbf{M}, \mathbf{c}, f\right)$, except for the improbable cases (a point in the ellipse case, two intersecting lines in the hyperbolic case and two parallel lines in the parabolic one), the determinant of $\mathbf{M}$ specifies the type of curve we will obtain:

- **positive determinant, or two eigenvalues of the same sign is an ellipse,**
- **negative determinant, or eigenvalues of different signs produces a hyperbola,**
- **while determinant 0 or one of the eigenvalues being zero, we then have a parabola.**

Finally, we may wonder what occurs to $\mathfrak{C}\left(\mathbf{M}, \mathbf{c}, f\right)$ when we apply an arbitrary affine transformation to it. But we know $F_{\mathbf{A},\mathbf{b}}\left(\mathfrak{C}\left(\mathbf{M}, \mathbf{c}, f\right)\right) = \mathfrak{C}\left(\mathbf{N}, \mathbf{k}, h\right)$ where $\mathbf{N} = \left(\mathbf{A}^{-1}\right)^{\mathrm{T}} \mathbf{M}\mathbf{A}^{-1}$, and so $\det \mathbf{N} = \det \mathbf{M}\left(\det \mathbf{A}^{-1}\right)^2$, and since the sign of the determinant does not change, the type of curve does not change.

Appendix of Proofs

❸ Page 22

Theorem. (Transposes.) Let $\mathbf{A}$ be $m \times n$ and let $\mathbf{B}$ be $n \times p$. Then $(\mathbf{AB})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$.

Proof. The easiest way to prove this theorem is to think of the row-by-column model. Let $\mathbf{A} = \begin{pmatrix} \mathbf{v}_1^{\mathrm{T}} \\ \mathbf{v}_2^{\mathrm{T}} \\ \vdots \\ \mathbf{v}_m^{\mathrm{T}} \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_p \end{pmatrix}$, then $\mathbf{AB} = \begin{pmatrix} \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_1 & \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_2 & \cdots & \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_p \\ \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_1 & \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_2 & \cdots & \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_p \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_1 & \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_2 & \cdots & \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_p \end{pmatrix}$. But then

$$(\mathbf{AB})^{\mathrm{T}} = \begin{pmatrix} \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_1 & \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_1 & \cdots & \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_1 \\ \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_2 & \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_2 & \cdots & \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_2 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}_1^{\mathrm{T}}\mathbf{u}_p & \mathbf{v}_2^{\mathrm{T}}\mathbf{u}_p & \cdots & \mathbf{v}_m^{\mathrm{T}}\mathbf{u}_p \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1^{\mathrm{T}}\mathbf{v}_1 & \mathbf{u}_1^{\mathrm{T}}\mathbf{v}_2 & \cdots & \mathbf{u}_1^{\mathrm{T}}\mathbf{v}_m \\ \mathbf{u}_2^{\mathrm{T}}\mathbf{v}_1 & \mathbf{u}_2^{\mathrm{T}}\mathbf{v}_2 & \cdots & \mathbf{u}_2^{\mathrm{T}}\mathbf{v}_m \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{u}_p^{\mathrm{T}}\mathbf{v}_1 & \mathbf{u}_p^{\mathrm{T}}\mathbf{v}_2 & \cdots & \mathbf{u}_p^{\mathrm{T}}\mathbf{v}_m \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{u}_1^{\mathrm{T}} \\ \mathbf{u}_2^{\mathrm{T}} \\ \vdots \\ \mathbf{u}_p^{\mathrm{T}} \end{pmatrix} \begin{pmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_m \end{pmatrix} = \mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}. ⌘$$

---

❹ Page 29

Theorem (Upper Triangular Matrices). Let $\mathbf{M} = \begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1n} \\ \mathbf{0} & \mathbf{A}_{22} & \cdots & \mathbf{A}_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{A}_{nn} \end{pmatrix}$ and $\mathbf{N} = \begin{pmatrix} \mathbf{X}_{11} & \mathbf{X}_{12} & \cdots & \mathbf{X}_{1n} \\ \mathbf{0} & \mathbf{X}_{22} & \cdots & \mathbf{X}_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{X}_{nn} \end{pmatrix}$ be in (block) upper triangular form. Then their product is also in (block) upper triangular form. Moreover, the diagonal blocks of the product are the respective products of the diagonal blocks.

Proof. By induction on the number of blocks on the main diagonal. If $n = 1$, there is nothing to prove since every 1×1 matrix is upper triangular. Let us consider the very special case when $n=2$. But then from the example above if we take $\begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{0} & \mathbf{D} \end{pmatrix}$ and $\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ \mathbf{0} & \mathbf{W} \end{pmatrix}$, then their product is $\begin{pmatrix} \mathbf{AX} & \mathbf{AZ}+\mathbf{CW} \\ \mathbf{0} & \mathbf{DW} \end{pmatrix}$. But we can view $\mathbf{M}$ and $\mathbf{N}$ as being in 2×2 form. Namely, let $\mathbf{A}=\begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1n-1} \\ \mathbf{0} & \mathbf{A}_{22} & \cdots & \mathbf{A}_{2n-1} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{A}_{n-1n-1} \end{pmatrix}$, $\mathbf{C}=\mathbf{A}_{1n}$ and $\mathbf{D}=\mathbf{A}_{nn}$, then $\mathbf{M}=\begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{0} & \mathbf{D} \end{pmatrix}$, and similarly $\mathbf{X}=\begin{pmatrix} \mathbf{X}_{11} & \mathbf{X}_{12} & \cdots & \mathbf{X}_{1n-1} \\ \mathbf{0} & \mathbf{X}_{22} & \cdots & \mathbf{X}_{2n-1} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{X}_{n-1n-1} \end{pmatrix}$, $\mathbf{Z}=\mathbf{X}_{1n}$ and $\mathbf{W}=\mathbf{X}_{nn}$, then $\mathbf{N}=\begin{pmatrix} \mathbf{X} & \mathbf{Z} \\ \mathbf{0} & \mathbf{W} \end{pmatrix}$. And since by induction, $\mathbf{AX}$ is in block upper triangular form, with the diagonal blocks as expected, we have proven the theorem. ⌘

---

❺ Page 39

Theorem (One Side Suffices). Let $\mathbf{A}$ be square. If $\mathbf{AB}=\mathbf{I}$, then $\mathbf{A}$ is invertible and, as before, $\mathbf{B}=\mathbf{A}^{-1}$.

Proof. We are going to proceed by induction (**are you surprised?**). It is obvious when $n=1$. Assume the theorem holds for smaller matrices, and assume $\mathbf{AB}=\mathbf{I}$. If the first row of $\mathbf{A}$ were all zeroes, then the first row of $\mathbf{AB}$ would be all zeroes, which is not the case. Thus, we know that there is a permutation matrix $\mathbf{P}$ such that the $1-1$ entry of $\mathbf{AP}$ is not zero. Note that $\mathbf{APP}^{-1}\mathbf{B}=\mathbf{I}$, so if we call $\mathbf{A}'=\mathbf{AP}$ and $\mathbf{B}'=\mathbf{P}^{-1}\mathbf{B}$, then $\mathbf{A}'\mathbf{B}'=\mathbf{I}$, and so if we prove the theorem for these, then we would have that $\mathbf{B}'\mathbf{A}'=\mathbf{I}$, and so $\mathbf{P}^{-1}\mathbf{BAP}=\mathbf{I}$, which implies that $\mathbf{BA}=\mathbf{I}$, so we would have the theorem. Thus, we can assume without loss, that the $1-1$ entry of $\mathbf{A}$ is nonzero. Consider the matrix $\mathbf{M}=\begin{pmatrix} 1 & \mathbf{0} \\ -\frac{a_{21}}{a_{11}} & \\ \vdots & \mathbf{I}_{n\text{-}1} \\ -\frac{a_{n1}}{a_{11}} & \end{pmatrix}$. This is a lower triangular matrix with ones along the diagonal, so it is invertible. Now let $\mathbf{A}'=\mathbf{MA}$ and suppose we show that it is invertible. Then if we let $\mathbf{B}'=\mathbf{BM}^{-1}$, then since $\mathbf{A}'\mathbf{B}'=\mathbf{MABM}^{-1}=\mathbf{I}$, then we would know necessarily that $\mathbf{B}'=\mathbf{A}'^{-1}$, and so $\mathbf{I}=\mathbf{B}'\mathbf{A}'=\mathbf{BM}^{-1}\mathbf{MA}=\mathbf{BA}$, and we would be done. But what is $\mathbf{A}'=\mathbf{MA}$? Easily, let us compute the $2-1$ position of this product (the $1-1$ position is just a_{11}). We are multiplying the row $\begin{pmatrix} -\frac{a_{21}}{a_{11}} & 1 & 0 & \cdots & 0 \end{pmatrix}$ by the column $\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \vdots \\ a_{n1} \end{pmatrix}$, and so we have as an end result $-a_{21}+a_{21}=0$. Similarly, if we compute the $3-1$ position, we would be multiplying the row $\begin{pmatrix} -\frac{a_{31}}{a_{11}} & 0 & 1 & \cdots & 0 \end{pmatrix}$ by the column $\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \vdots \\ a_{n1} \end{pmatrix}$, and so we have as an end result $-a_{31}+a_{31}=0$. Thus $\mathbf{A}'$ is of the form $\begin{pmatrix} a_{11} & * & \cdots & * \\ 0 & & & \\ \vdots & & \mathbf{C} & \\ 0 & & & \end{pmatrix}$ where $\mathbf{C}$ is an $(n-1)\times(n-1)$ matrix. Since $a_{11}\neq 0$, if we can show that $\mathbf{C}$ is invertible, then by block upper triangularity, we will have that $\mathbf{A}'$ is invertible, and we will be finished. Let $\mathbf{B}'=\begin{pmatrix} b_{11} & \mathbf{v}^{\mathrm{T}} \\ \mathbf{u} & \mathbf{D} \end{pmatrix}$ where $\mathbf{D}$ is also $(n-1)\times(n-1)$. It would then suffice to show that $\mathbf{CD}=\mathbf{I}$, because then by induction we would have that $\mathbf{C}$ is invertible. But we know that $\mathbf{A}'\mathbf{B}'=\mathbf{I}$, and so by simple block multiplication, $\mathbf{CD}=\mathbf{I}$. ⌘

❻ Page 50

Theorem (Uniqueness of the form). Let $\mathbf{A}$ be an arbitrary $m\times n$ matrix. Then $\mathbf{A}$ is row equivalent to a unique matrix in row echelon form.

Proof. By induction on *n*. If $n=1$, it is trivial, since if $\mathbf{A}=\mathbf{0}$ that is its unique form while if $\mathbf{A}\neq\mathbf{0}$, then by permuting rows if necessary, we can assume the 1-1 position is nonzero, and then by pivoting in the 1-1 position, we arrive at the reduced form $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, of size *m*, and that is clearly unique. Assume now the theorem holds for all matrices of size $m\times n$, and let $\mathbf{B}$ be a matrix of size $m\times(n+1)$. Let $\mathbf{B}=\begin{pmatrix}\mathbf{A} & \mathbf{u}\end{pmatrix}$ where $\mathbf{A}$ is an $m\times n$ matrix and $\mathbf{u}$ is $m\times 1$. We know by induction there exists a sequence of steps in the Gaussian elimination process, which when multiplied together give an invertible matrix

$\mathbf{P}$ such that $\mathbf{PA}=\mathbf{M}$, and that the matrix $\mathbf{M}$ is row reduced, and hence uniquely determined. Note this implies that anytime we reduce $\mathbf{B}$, we will have the $\mathbf{M}$ as the first n columns. But then we have $\mathbf{PB}=\begin{pmatrix}\mathbf{PA} & \mathbf{Pu}\end{pmatrix}$. Two cases occur, either there is a solution to $\mathbf{Ax}=\mathbf{u}$ or there is not. Assume first that $\mathbf{Ax}=\mathbf{u}$ is not solvable. But then neither is $\mathbf{PAx}=\mathbf{Pu}$, which is $\mathbf{Mx}=\mathbf{Pu}$. But by the special form of $\mathbf{M}$, we can conclude, by the **Lemma**, that $\mathbf{Pu}$ must have a nonzero entry in a row in which $\mathbf{M}$ has all 0's. Without loss we can make this entry a 1. Let t be the number of nonzero rows in $\mathbf{M}$. Then by permuting rows below the t^{th} row of $\mathbf{M}$, we can put the 1 in row $t+1$, and then by pivoting in the $t+1, n+1-$position, which leaves $\mathbf{M}$ unchanged, we can make the last column be $\mathbf{w}=\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix}$, where again the 1 is in row $t+1$. Clearly then $\mathbf{B}$ is row equivalent to the matrix $\begin{pmatrix}\mathbf{M} & \mathbf{w}\end{pmatrix}$ which is reduced, moreover since the assumption that $\mathbf{Ax}=\mathbf{u}$ is not solvable is independent of all that has occurred, the form is unique, and we are done in this case.

Assume now that $\mathbf{Ax}=\mathbf{u}$ is solvable. But if that is the case, since there are no new pivots, the matrix $\mathbf{PB}=\begin{pmatrix}\mathbf{PA} & \mathbf{Pu}\end{pmatrix}$ is already reduced, so the only issue is the uniqueness of the form. So assume $\mathbf{QB}=\begin{pmatrix}\mathbf{QA} & \mathbf{Qu}\end{pmatrix}$ is also reduced. Then, by the induction hypothesis we know that $\mathbf{PA}=\mathbf{QA}$, but then $\mathbf{Qu}=\mathbf{QAx}=\mathbf{PAx}=\mathbf{Pu}$ and we are done. ⌘

❶❶ Page 94

> **Theorem** (Basis). Let V be a vector space. Then V has a basis. Furthermore, any two bases of V have the same number of elements.

In order to prove this fundamental theorem we need several lemmas.

> **Lemma 1 (Spanning Set).** Let V be a subspace of $\mathbb{R}^n$. Then V has a subset $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ such that $V=[\mathbf{u}_1,\mathbf{u}_2,\ldots,\mathbf{u}_t]$. Moreover, $t\le n$.

Proof. For each coordinate $1\le i\le n$, we say that i contributes if there is a vector in V which is 0 in all coordinates less than i, but not 0 in that coordinate. Since it is not zero in that coordinate, by dividing by that nonzero number, we can assume the vector is actually 1 in that coordinate. Thus we say a coordinate i contributes if V has a vector of the form $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ * \end{pmatrix}$ where the 1 occurs in the i^{th} coordinate. Let $i_1 < i_2 < \cdots < i_t$ be the contributing coordinates, and for each of them choose a vector as described above: $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$. Certainly $t \le n$ since there are at most *n* contributing coordinates. We claim $V = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n]$. Let $\mathbf{v}^{\mathrm{T}} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \in V$ be arbitrary. Then certainly, for $j < i_1$, $a_j = 0$. Consider $\mathbf{v} - a_{i_1}\mathbf{u}_1 \in V$. Then for all coordinates $j < i_2$, this vector must have 0 entries since there are no contributing coordinates between i_1 and i_2. Again, by subtracting the appropriate multiple of $\mathbf{u}_2$, we will obtain a vector with zeroes entries in all coordinates $j < i_3$. Proceeding in this fashion, we will eventually arrive at the $\mathbf{0}$ vector, and so $\mathbf{v} \in [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n]$. ⌘

The astute reader will observe that this argument is just a formalization of Gaussian Elimination in a sense that starting with a matrix, and the subspace spanned by its rows, the algorithm proceeds to find the **u**'s in an even better form.

Observe that the **u**'s selected in the **Spanning Set Theorem** are linearly independent.

This argument should be familiar

> **Lemma 2 (Reduction).** Let $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_t$ be given. Then there is a subset of the **u**'s such that it is linearly independent, and their span is the span of all the **u**'s, $[\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_t]$.

Proof. The proof is by induction on *t*. If $\mathbf{u}_1 = \mathbf{0}$, drop it from the collection and proceed. Assume then $\mathbf{u}_1 \ne \mathbf{0}$. If $\mathbf{u}_2 \in [\mathbf{u}_1]$, then $[\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_t] = [\mathbf{u}_1, \mathbf{u}_3, \ldots, \mathbf{u}_t]$, so we can drop $\mathbf{u}_2$. Otherwise, $\mathbf{u}_1$ and $\mathbf{u}_2$ are linearly independent. If $\mathbf{u}_3 \in [\mathbf{u}_1, \mathbf{u}_2]$, then we can drop $\mathbf{u}_3$, if not the three vectors are linearly independent. Etcetera. ⌘

In fact, Gaussian Elimination does exactly this to the columns of a matrix, picking the pivotal ones as the linearly independent set while describing each **nonpivotal** column as a linear combination of the previous ones:

Note that we already have that every vector space has a basis, but we are missing the more crucial fact that any two bases have the same size! Thus we need one more lemma.

> **Lemma 3 (Size).** Let $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_t\}$ and $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be collections of linearly independent vectors. Suppose $[\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_t]$ is contained in $[\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k]$. Then $t \le k$.

Proof. It is by induction on the number of elements that are in $\{\mathbf{u}_1,\mathbf{u}_2,\dots,\mathbf{u}_t\}$, but not in $\{\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_k\}$. If there are none, then $\{\mathbf{u}_1,\mathbf{u}_2,\dots,\mathbf{u}_t\}$ is contained in $\{\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_k\}$, and clearly $t \le k$. Otherwise, without loss of generality, let $\mathbf{u}_1 \notin \{\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_k\}$. But since $\mathbf{u}_1 \in [\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_k]$, $\mathbf{u}_1 = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$ for some scalars a's. Consider only the $\mathbf{v}$'s with nonzero coefficients. If all of them were $\mathbf{u}$'s, then the set of $\mathbf{u}$'s would not be linearly independent. So at least one of the $\mathbf{v}$'s with nonzero coefficient is not a $\mathbf{u}$. Without loss let it be $\mathbf{v}_1$. Consider now the set $\{\mathbf{u}_1,\mathbf{v}_2,\dots,\mathbf{v}_k\}$, in other words we drop $\mathbf{v}_1$ and pick up $\mathbf{u}_1$. We next claim that $[\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_k] = [\mathbf{u}_1,\mathbf{v}_2,\dots,\mathbf{v}_k]$. Since $\mathbf{u}_1 = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$, we can solve for $\mathbf{v}_1$, and prove that $\mathbf{v}_1 \in [\mathbf{u}_1,\mathbf{v}_2,\dots,\mathbf{v}_k]$. The other containment is trivial. But then if we consider $\{\mathbf{u}_1,\mathbf{u}_2,\dots,\mathbf{u}_t\}$ and $\{\mathbf{u}_1,\mathbf{v}_2,\dots,\mathbf{v}_k\}$, then the hypothesis applies, but now the two sets have one more vector in common, and hence the induction takes over, and we have that $t \le k$, as promised. ⌘

Now the theorem follows from the three lemmas.

❶❸ Page 117

> **Theorem (Adjoints).** Let $\mathbf{A}$ be an $n \times n$ matrix. Then there is a scalar a such that
> $$\mathbf{A}\tilde{\mathbf{A}} = \tilde{\mathbf{A}}\mathbf{A} = a\mathbf{I}.$$

Also recall that the scalar in the theorem is by definition the determinant of $\mathbf{A}$. So in fact we have to prove that

$$\mathbf{A}\tilde{\mathbf{A}} = \tilde{\mathbf{A}}\mathbf{A} = (\det \mathbf{A})\mathbf{I}.$$

We will be using the expression: **The theorem holds for A**, that will in particular imply that the determinant of $\mathbf{A}$ is defined by this equation.

As before, if we let $\mathbf{A}_{ij}$ denote the matrix obtained from $\mathbf{A}$ by deleting the i^{th} row and j^{th} column, then the i,j – position of $\tilde{\mathbf{A}}$, $\tilde{a}_{ij}$, is given by

$$\tilde{a}_{ij} = (-1)^{i+j} \det \mathbf{A}_{ji}.$$

The proof of the theorem is by induction. Observe that once the theorem is verified for matrices of size $n \times n$, then we can define the adjoint of any $n+1 \times n+1$. We have seen the theorem holds $n = 1,2,3$. So we assume the theorem holds for all matrices of size

$n\times n$ or smaller, and at the same time we can discuss the adjoint of any $n+1\times n+1$ matrix.

For the rest of the section, **we assume A, B and C are $n\times n$ or smaller while M and N are $n+1\times n+1$.**

We need to prove a few facts before we can finish proving the theorem. If two matrices **A** and **B** are identical in all rows except possibly the first one, then we can create a new matrix **C** by adding the two first rows of **A** and **B**, and leaving all other rows the same. We will use $\mathbf{C}=\mathbf{A}\overset{1}{+}\mathbf{B}$ to denote this construction. For example, $\begin{pmatrix}3&5\\2&4\end{pmatrix}\overset{1}{+}\begin{pmatrix}2&3\\2&4\end{pmatrix}=\begin{pmatrix}5&8\\2&4\end{pmatrix}$.

Lemma 1. Let $\mathbf{C}=\mathbf{A}\overset{1}{+}\mathbf{B}$. Then $\det\mathbf{C}=\det\mathbf{A}+\det\mathbf{B}$.

Proof. Now for any j, $\mathbf{C}_{1j}=\mathbf{A}_{1j}=\mathbf{B}_{1j}$, so $\tilde{c}_{j1}=\tilde{a}_{j1}=\tilde{b}_{j1}$, but $c_{1j}=a_{1j}+b_{1j}$, so computing the $1,1-$entry of $\mathbf{C}\tilde{\mathbf{C}}$ we get $\det\mathbf{C}=\det\mathbf{A}+\det\mathbf{B}$. ⌘

Lemma 2 (Permutation). Let **M** be a matrix for which the theorem holds. Let **P** be the permutation matrix obtained from **I** by switching rows k and $k+1$. Let $\mathbf{N}=\mathbf{PM}$, so **N** is obtained from **M** by switching rows k and $k+1$. Then

❶ $\tilde{\mathbf{N}}$ can be obtained from $\tilde{\mathbf{M}}$ by multiplying by -1 and switching columns k and $k+1$. In other words, $\tilde{\mathbf{N}}=-\tilde{\mathbf{M}}\mathbf{P}$.

❷ The theorem holds for **N**.

❸ $\det\mathbf{N}=-\det\mathbf{M}$.

Proof. By induction on n once more. All claims are trivial in the case $n=1$: $\mathbf{M}=\begin{pmatrix}a&b\\c&d\end{pmatrix}$, $\mathbf{N}=\begin{pmatrix}c&d\\a&b\end{pmatrix}$, $\tilde{\mathbf{M}}=\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$ and $\tilde{\mathbf{N}}=\begin{pmatrix}b&-d\\-a&c\end{pmatrix}$. Assume the lemma holds for smaller matrices. If $i\neq k,k+1$, then easily $\mathbf{N}_{ij}$ is obtained from $\mathbf{M}_{ij}$ by switching two consecutive rows. So by induction $\det\mathbf{N}_{ij}=-\det\mathbf{M}_{ij}$, so if $i\neq k,k+1$, $\tilde{n}_{ji}=-\tilde{m}_{ji}$. But also $\mathbf{N}_{kj}=\mathbf{M}_{k+1j}$ and $\mathbf{N}_{k+1j}=\mathbf{M}_{kj}$, so $\tilde{n}_{jk}=-\tilde{m}_{jk+1}$ and $\tilde{n}_{jk+1}=-\tilde{m}_{jk}$ since $j+k$ and $j+k+1$ differ in parity. And ❶ has been proven. Since **P** is symmetric, $\mathbf{P}^2=\mathbf{I}$. So

$$\mathbf{N}\tilde{\mathbf{N}}=\mathbf{PM}\tilde{\mathbf{M}}\mathbf{P}=\mathbf{P}\left(-\det\mathbf{M}\right)\mathbf{IP}=-\left(\det\mathbf{M}\right)\mathbf{I}$$

and

$$\tilde{\mathbf{N}}\mathbf{N}=\tilde{\mathbf{M}}\mathbf{PPM}=-\left(\det\mathbf{M}\right)\mathbf{I},$$

and all claims are proven. ⌘

It is worth noting that actually we have the lemma for any swap of rows since any such permutation can be accomplished by a sequence of consecutive swaps. For example, to swap 2 and 7, first swap 2 and 3, followed by 3 and 4, 4 and 5, 5 and 6, 6 and 7, 6 and 5, 5 and 4, 4 and 3 and finally 3 and 2. The end result is that 2 and 7 have been swapped but nothing else has changed.

Lemma 3 (Multiple of a Row). Let $\mathbf{M}$ be a matrix for which the theorem holds. Let $\mathbf{D}$ be the diagonal matrix with 1's along the diagonal except in the $1,1-$position where there is a nonzero x. Let $\mathbf{N}=\mathbf{DM}$, so $\mathbf{N}$ is obtained from $\mathbf{M}$ by multiplying the first row by x. Then

❶ $\tilde{\mathbf{N}}$ is identical to $x\tilde{\mathbf{M}}$ except the first column is divided by x. In other words, $\tilde{\mathbf{N}}=x\tilde{\mathbf{M}}\mathbf{D}^{-1}$.

❷ The theorem holds for $\mathbf{N}$.

❸ $\det\mathbf{N}=x\det\mathbf{M}$.

Proof. By induction on n once more. All claims are trivial in the case $n=1$: $\mathbf{M}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\mathbf{N}=\begin{pmatrix} xa & xb \\ c & d \end{pmatrix}$, $\tilde{\mathbf{M}}=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and $\tilde{\mathbf{N}}=\begin{pmatrix} d & -xb \\ -c & xa \end{pmatrix}$. Assume the lemma holds for smaller matrices. If $i\neq 1$, then easily $\mathbf{N}_{ij}$ is obtained from $\mathbf{M}_{ij}$ by multiplying the first row by x, so by induction $\det\mathbf{N}_{ij}=x\det\mathbf{M}_{ij}$, so if $i\neq 1$, $\tilde{n}_{ji}=x\tilde{m}_{ji}$. But also $\mathbf{N}_{1j}=\mathbf{M}_{1j}$, so $\tilde{n}_{j1}=\tilde{m}_{j1}$. And ❶ has been proven. So

$$\mathbf{N}\tilde{\mathbf{N}}=\mathbf{DM}x\tilde{\mathbf{M}}\mathbf{D}^{-1}=x\mathbf{D}\left(\det\mathbf{M}\right)\mathbf{ID}^{-1}=x\left(\det\mathbf{M}\right)\mathbf{I}$$

and

$$\tilde{\mathbf{N}}\mathbf{N}=x\tilde{\mathbf{M}}\mathbf{D}^{-1}\mathbf{DM}=x\left(\det\mathbf{M}\right)\mathbf{I},$$

and all claims are proven. ⌘

Note that **Lemma 3** combined with **Lemma 2** gives the ability to multiply any row by a nonzero number, and be able to conclude as in the last.

Lemma 4 (Add a Multiple of a Row). Let $\mathbf{M}$ be a matrix for which the theorem holds. Let $\mathbf{K}$ be the matrix with 1's along the diagonal and zeroes everywhere else, except for an x in the $2,1-$position. Let $\mathbf{N}=\mathbf{KM}$, so $\mathbf{N}$ is obtained from $\mathbf{M}$ by adding x times the first row to the second row. Then

❶ $\tilde{\mathbf{N}}$ is identical to $\tilde{\mathbf{M}}$ except for the first column, from which x times the second column has been subtracted. In other words, $\tilde{\mathbf{N}}=\tilde{\mathbf{M}}\mathbf{K}^{-1}$.

❷ The theorem holds for $\mathbf{N}$.

❸ $\det\mathbf{N}=\det\mathbf{M}$.

Proof. By induction on n once more. All claims are trivial in the case $n=1$: $\mathbf{M}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\mathbf{N}=\begin{pmatrix} a & b \\ c+xa & d+xb \end{pmatrix}$, $\tilde{\mathbf{M}}=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ and $\tilde{\mathbf{N}}=\begin{pmatrix} d+xb & -b \\ -c-xa & a \end{pmatrix}$. Assume the lemma holds for smaller matrices. If $i \neq 1,2$, then easily $\mathbf{N}_{ij}$ is obtained from $\mathbf{M}_{ij}$ by adding x times the first row to the second row, so by induction $\det \mathbf{N}_{ij} = \det \mathbf{M}_{ij}$. If $i \neq 1,2$, $\tilde{n}_{ji} = \widetilde{m}_{ji}$. If $i = 2$, $\mathbf{N}_{2j} = \mathbf{M}_{2j}$, so $\tilde{n}_{j2} = \widetilde{m}_{j2}$. Finally, if $i = 1$, $\mathbf{N}_{1j} = \mathbf{M}_{1j} \overset{\mathbf{1}}{+} \mathbf{DM}_{2j}$ where $\mathbf{D}$ is as in the previous lemma. So by **Lemma 1**, $\det \mathbf{N}_{1j} = \det \mathbf{M}_{1j} + \det \mathbf{DM}_{2j}$. By **Lemma 3**, $\det \mathbf{DM}_{2j} = x \det \mathbf{M}_{2j}$. Also $\det \mathbf{M}_{2j} = (-1)^{2+j}\, \widetilde{m}_{j2}$, so $\tilde{n}_{j1} = \widetilde{m}_{j1} - x\widetilde{m}_{j2}$ and ❶ has been proven. So

$$\mathbf{N}\tilde{\mathbf{N}} = \mathbf{K}\mathbf{M}\widetilde{\mathbf{M}}\mathbf{K}^{-1} = \mathbf{K}\left(\det \mathbf{M}\right)\mathbf{I}\mathbf{K}^{-1} = \left(\det \mathbf{M}\right)\mathbf{I}$$

and

$$\tilde{\mathbf{N}}\mathbf{N} = \widetilde{\mathbf{M}}\mathbf{K}^{-1}\mathbf{K}\mathbf{M} = \left(\det \mathbf{M}\right)\mathbf{I},$$

and all claims are proven. ⌘

Lemma 5 (Add a Multiple of a Row Further Down). Let $\mathbf{M}$ be a matrix for which the theorem holds. Let $\mathbf{L}$ be the matrix with 1's along the diagonal and zeroes everywhere else, except for an x in the $i,1-$position where $i \neq 1$. Let $\mathbf{N} = \mathbf{LM}$, so $\mathbf{N}$ is obtained from $\mathbf{M}$ by adding x times the first row to the i^{th}-row. Then

❶ $\tilde{\mathbf{N}}$ is identical to $\widetilde{\mathbf{M}}$ except for the first column, from which x times the i^{th}-column has been subtracted. In other words, $\tilde{\mathbf{N}} = \widetilde{\mathbf{M}}\mathbf{L}^{-1}$.

❷ The theorem holds for $\mathbf{N}$.

❸ $\det \mathbf{N} = \det \mathbf{M}$.

Proof. We will do the third row and then proceed to do the fourth row, et cetera. Let $\mathbf{P}$ be the matrix that switches the second and third rows, and let $\mathbf{K}$ be as in the previous lemma. Then $\mathbf{N} = \mathbf{PKPM}$, and so

$$\tilde{\mathbf{N}} = -\widetilde{\mathbf{KPM}}\mathbf{P}^{-1} = -\widetilde{\mathbf{PM}}\mathbf{K}^{-1}\mathbf{P}^{-1} = \widetilde{\mathbf{M}}\mathbf{P}^{-1}\mathbf{K}^{-1}\mathbf{P}^{-1}$$

and $\det \mathbf{N} = (-1)(-1)\det \mathbf{M}$, and we are done. The remainder is similar. ⌘

Before the next lemma, observe that if the theorem holds for a matrix and it has a row (or column) of zeroes, then its determinant must be 0 since that row (or column) of zeroes will produce a row (or column) of zeroes in the product.

Lemma 6 (Extension). Let $\mathbf{A}$ be $n \times n$. Then the theorem holds for any matrix of the form $\mathbf{M} = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathbf{A} & \\ 0 & & & \end{pmatrix}$. Moreover, $\widetilde{\mathbf{M}} = \begin{pmatrix} \det \mathbf{A} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & a\widetilde{\mathbf{A}} & \\ 0 & & & \end{pmatrix}$,

and $\det \mathbf{M} = a \det \mathbf{A}$.

Proof. When computing stage 1 of the process, it is clear we first get, $\begin{pmatrix} \det \mathbf{A} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$ by the remark before. Now we do the rest by induction. Scratching out any other row and column leaves a matrix of the form $\mathbf{M}_{i+1\,j+1} = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathbf{A}_{ij} & \\ 0 & & & \end{pmatrix}$ whose determinant is (by induction) the same as $a \det \mathbf{A}_{ij}$. Since the oddness of a position does not change when one adds 1 to both row and column, and finally by transposing, we get that $\widetilde{\mathbf{M}}$ is of the form $\begin{pmatrix} \det \mathbf{A} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & a\widetilde{\mathbf{A}} & \\ 0 & & & \end{pmatrix}$. Now by block multiplication and induction, we get

$$\mathbf{M}\widetilde{\mathbf{M}} = \widetilde{\mathbf{M}}\mathbf{M} = \left(a \det \mathbf{A}\right)\mathbf{I}.$$

So the theorem is true for $\mathbf{M}$ and all claims follow readily. ⌘

Now we are ready for the proof of the theorem. Note we have already shown that if the theorem is true for $\mathbf{M}$, then it is also true for $\mathbf{M}^{\mathrm{T}}$ (see Section ❶❸ for the argument).

So let $\mathbf{M}$ be an arbitrary matrix of size $n+1 \times n+1$. If the first row and column of $\mathbf{M}$ is all zeroes, then we are done by the last lemma. If the first column of $\mathbf{M}$ is all zeroes but not the first column, we will tackle $\mathbf{M}^{\mathrm{T}}$ first. So without loss, assume the first column of $\mathbf{M}$ is not all zeroes. We can switch the first row (by **Lemma 2**) with any other row if necessary, so again we can assume the $1,1-$position is not 0. Now by **Lemma 5**, we can assume the rest of the entries of the first column are all 0. Now we can transpose, and do the same to the first row, and so we arrive at a matrix of the form for **Lemma 6**, and since it is true for this matrix, we are done.

❶❸ Page 121

Theorem (Multiplicativity). Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$. Then $\widetilde{\mathbf{AB}} = \widetilde{\mathbf{B}}\widetilde{\mathbf{A}}$ and $\det \mathbf{AB} = \det \mathbf{A} \det \mathbf{B}$.

Observe that if we have the first claim, then

$$\det\left(\mathbf{AB}\right)\mathbf{I} = \left(\mathbf{AB}\right)\left(\widetilde{\mathbf{AB}}\right) = \mathbf{AB}\widetilde{\mathbf{B}}\widetilde{\mathbf{A}} = \mathbf{A}\left(\det \mathbf{B}\right)\mathbf{I}\widetilde{\mathbf{A}} = \left(\det \mathbf{B}\right)\left(\det \mathbf{A}\right)\mathbf{I}$$

and the second claims follows immediately.

Recall that for an invertible matrix, $\widetilde{\mathbf{A}} = (\det \mathbf{A})\mathbf{A}^{-1}$.

Call a matrix $\mathbf{A}$ *good* if $\widetilde{\mathbf{AX}} = \widetilde{\mathbf{X}}\widetilde{\mathbf{A}}$ and $\widetilde{\mathbf{XA}} = \widetilde{\mathbf{A}}\widetilde{\mathbf{X}}$ for all square matrixes $\mathbf{X}$. We proceed to show that every matrix is good. As in the case of the **Adjoint Theorem**, we need several simpler facts.

① Since $\det \mathbf{I} = 1$, $\widetilde{\mathbf{I}} = \mathbf{I}$, so $\mathbf{I}$ is good.

② If $\mathbf{A}$ is good, then so is $\mathbf{A}^{\mathrm{T}}$ since

$$\widetilde{\mathbf{XA}^{\mathrm{T}}} = \widetilde{\left(\mathbf{AX}^{\mathrm{T}}\right)^{\mathrm{T}}} = \left(\widetilde{\mathbf{AX}^{\mathrm{T}}}\right)^{\mathrm{T}} = \left(\widetilde{\mathbf{X}^{\mathrm{T}}}\widetilde{\mathbf{A}}\right)^{\mathrm{T}} = \widetilde{\mathbf{A}}^{\mathrm{T}}\widetilde{\mathbf{X}^{\mathrm{T}}}^{\mathrm{T}} = \widetilde{\mathbf{A}^{\mathrm{T}}}\widetilde{\mathbf{X}},$$

and similarly for the other side.

③ If $\mathbf{A}$ and $\mathbf{B}$ are good, so is $\mathbf{AB}$ because

$$\widetilde{(\mathbf{AB})\mathbf{X}} = \widetilde{\mathbf{A}(\mathbf{BX})} = \widetilde{(\mathbf{BX})}\widetilde{\mathbf{A}} = \left(\widetilde{\mathbf{X}}\widetilde{\mathbf{B}}\right)\widetilde{\mathbf{A}} = \widetilde{\mathbf{X}}\left(\widetilde{\mathbf{B}}\widetilde{\mathbf{A}}\right) = \widetilde{\mathbf{X}}\left(\widetilde{\mathbf{AB}}\right)$$

and similarly for the other side.

④ If $\widetilde{\mathbf{AX}} = \widetilde{\mathbf{X}}\widetilde{\mathbf{A}}$ and $\widetilde{\mathbf{A}^{\mathrm{T}}\mathbf{X}} = \widetilde{\mathbf{X}}\widetilde{\mathbf{A}^{\mathrm{T}}}$ for every $\mathbf{X}$, then $\mathbf{A}$ is good. This follows from the following equation:

$$\widetilde{\mathbf{XA}}^{\mathrm{T}} = \widetilde{(\mathbf{XA})^{\mathrm{T}}} = \widetilde{\mathbf{A}^{\mathrm{T}}\mathbf{X}^{\mathrm{T}}} = \widetilde{\mathbf{X}^{\mathrm{T}}}\widetilde{\mathbf{A}^{\mathrm{T}}} = \left(\widetilde{\mathbf{A}}^{\mathrm{T}}\widetilde{\mathbf{X}^{\mathrm{T}}}^{\mathrm{T}}\right)^{\mathrm{T}} = \left(\widetilde{\mathbf{A}}\widetilde{\mathbf{X}}\right)^{\mathrm{T}}$$

so $\widetilde{\mathbf{XA}} = \widetilde{\mathbf{A}}\widetilde{\mathbf{X}}$.

⑤ Let $\mathbf{P}$ be the permutation matrix obtained from $\mathbf{I}$ by switching two rows. Then $\mathbf{P}$ is good and $\det \mathbf{P} = -1$.

Proof. Let $\mathbf{P}_j$ be the permutation matrix obtained from $\mathbf{I}$ by switching rows j and $j+1$. By **Lemma 2** from the previous section we have $\widetilde{\mathbf{P}_j\mathbf{X}} = -\widetilde{\mathbf{X}}\mathbf{P}_j$ for any matrix $\mathbf{X}$. Also we have $\mathbf{P}_j^2 = \mathbf{I}$. So $\widetilde{\mathbf{I}} = \widetilde{\mathbf{P}_j\mathbf{P}_j} = -\widetilde{\mathbf{P}}_j\mathbf{P}_j$, so $\widetilde{\mathbf{P}}_j = -\mathbf{P}_j$, so $\det \mathbf{P}_j = -1$ and $\widetilde{\mathbf{P}_j\mathbf{X}} = \widetilde{\mathbf{X}}\widetilde{\mathbf{P}}_j$. Since $\mathbf{P}_j$ is symmetric, $\mathbf{P}_j$ is good by ④. We have seen before that $\mathbf{P}$ is the product of an odd number of $\mathbf{P}_j$'s. For example, if $\mathbf{P}$ swaps rows 2 and 7, then we saw that $\mathbf{P} = \mathbf{P}_2\mathbf{P}_3\mathbf{P}_4\mathbf{P}_5\mathbf{P}_6\mathbf{P}_7\mathbf{P}_6\mathbf{P}_5\mathbf{P}_4\mathbf{P}_3\mathbf{P}_2$, and so by ③, we are done. ⌘

⑥ Let $\mathbf{D}$ be the diagonal matrix with 1's along the diagonal except in the $i,i-$position where there is a nonzero x. Then $\mathbf{D}$ is good and $\det \mathbf{D} = x$.

Proof. That $\det \mathbf{D} = x$ is trivial since $\mathbf{D}$ is diagonal. Observe that if we let $\mathbf{E}$ be the diagonal matrix with 1's along the diagonal except in the $1,1-$position where there is a nonzero x, and we let $\mathbf{P}$ be the swap of rows 1 and i, then $\mathbf{PEP} = \mathbf{D}$. By **Lemma 3** from the previous section, $\widetilde{\mathbf{EX}} = x\tilde{\mathbf{X}}\mathbf{E}^{-1}$. But $\tilde{\mathbf{E}} = (\det \mathbf{E})\mathbf{E}^{-1}$, so $\widetilde{\mathbf{EX}} = \tilde{\mathbf{X}}\tilde{\mathbf{E}}$. And since $\mathbf{E}$ is symmetric, we have that $\mathbf{E}$, and hence $\mathbf{D}$ is good. ⌘

⑦ Let $\mathbf{L}$ be the matrix with 1's along the diagonal and zeroes everywhere else, except for an x in the $i,j-$position where $i \neq j$. Then $\det \mathbf{L} = 1$, and $\mathbf{L}$ is good.

Proof. That $\mathbf{L}$ has determinant 1 is trivial since it is upper triangular. Let $\mathbf{K}$ be the matrix with 1's along the diagonal and zeroes everywhere else, except for an x in the $2,1-$position. By **Lemma 4** from the previous section, for any matrix $\mathbf{X}$, $\widetilde{\mathbf{KX}} = \tilde{\mathbf{X}}\mathbf{K}^{-1}$, but since $\det \mathbf{K} = 1$, $\mathbf{K}^{-1} = \tilde{\mathbf{K}}$, so $\widetilde{\mathbf{KX}} = \tilde{\mathbf{X}}\tilde{\mathbf{K}}$. Easily if we let $\mathbf{P}$ be the swap of the first and second rows, then $\mathbf{K}^{\mathrm{T}} = \mathbf{PKP}$, so

$$\widetilde{\mathbf{K}^{\mathrm{T}}\mathbf{X}} = \widetilde{\mathbf{PKPX}} = \widetilde{\mathbf{KPX}}\tilde{\mathbf{P}} = \widetilde{\mathbf{PX}}\tilde{\mathbf{K}}\tilde{\mathbf{P}} = \tilde{\mathbf{X}}\tilde{\mathbf{P}}\tilde{\mathbf{K}}\tilde{\mathbf{P}} = \tilde{\mathbf{X}}\widetilde{\mathbf{KP}}\tilde{\mathbf{P}} = \tilde{\mathbf{X}}\widetilde{\mathbf{PKP}} = \tilde{\mathbf{X}}\widetilde{\mathbf{K}^{\mathrm{T}}}$$

and by ④, $\mathbf{K}$ is good. Returning to $\mathbf{L}$, if we let $\mathbf{P}$ now be the swap of the second and i rows, then $\mathbf{PLP}$ will have ones on the main diagonal and x in the $i,1-$position, and finally if $\mathbf{Q}$ is the swap of the first and j rows, then $\mathbf{L} = \mathbf{QPKPQ}$, and we are done. ⌘

⑧ Every invertible matrix is good. This follows directly from the previous three facts since by Gaussian elimination, every invertible matrix is the product of good matrices.

⑨ If $\mathbf{A} = \mathbf{I}_k \oplus \mathbf{O}_{n-k} = \begin{pmatrix} \mathbf{I}_k & \mathbf{O} \\ \mathbf{O} & \mathbf{O} \end{pmatrix}$, then $\mathbf{A}$ is good.

Proof. If $k = n$, we are done. If $k \le n-2$, then $\tilde{\mathbf{A}} = \mathbf{O}$, and since $r(\mathbf{AX}) \le r(\mathbf{A})$ and $r(\mathbf{XA}) \le r(\mathbf{A})$, we have $\widetilde{\mathbf{AX}} = \tilde{\mathbf{O}} = \widetilde{\mathbf{XA}}$, and we are done. Thus the only interesting case is $k = n-1$, so $\mathbf{A} = \begin{pmatrix} \mathbf{I}_{n-1} & \mathbf{O} \\ \mathbf{O} & 0 \end{pmatrix}$. Then $\tilde{\mathbf{A}} = \begin{pmatrix} \mathbf{O}_{n-1} & \mathbf{O} \\ \mathbf{O} & 1 \end{pmatrix}$ since the only occurrence of a submatrix without a zero row or column is in $\mathbf{A}_{nn}$. Let $\mathbf{X} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}$ where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n \in \mathbb{R}^{n-1}$. So $\mathbf{AX} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \\ 0 & 0 & \cdots & 0 \end{pmatrix}$. But then we have

$$\tilde{\mathbf{X}} = \begin{pmatrix} * & \cdots & * & (-1)^n \det(\mathbf{u}_2 \ \cdots \ \mathbf{u}_n) \\ \vdots & & \vdots & \vdots \\ * & \cdots & * & (-1)^{n+n} \det(\mathbf{u}_1 \ \cdots \ \mathbf{u}_{n-1}) \end{pmatrix},$$

$$\tilde{\mathbf{X}}\tilde{\mathbf{A}} = \begin{pmatrix} 0 & \cdots & 0 & (-1)^n \det(\mathbf{u}_2 \ \cdots \ \mathbf{u}_n) \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & (-1)^{n+n} \det(\mathbf{u}_1 \ \cdots \ \mathbf{u}_{n-1}) \end{pmatrix} = \widetilde{\mathbf{AX}},$$

so we are done since $\mathbf{A}$ is symmetric. ⌘

Now we are ready to finish the theorem by proving that every matrix is good. Let $\mathbf{A}$ be given. Then there exists an invertible matrix $\mathbf{P}$ so that $\mathbf{PA} = \mathbf{M}$ is in reduced form. Easily then there exists an invertible matrix $\mathbf{Q}$ such that $\mathbf{QM}^{\mathrm{T}} = \mathbf{N}$ is in reduced form. But readily $\mathbf{N} = \mathbf{I} \oplus \mathbf{0}$. And since $\mathbf{A} = \mathbf{P}^{-1}\mathbf{N}\left(\mathbf{Q}^{\mathrm{T}}\right)^{-1}$, we are done.

---

❶❺ Page 141

Theorem (Triangularity). Let $\mathbf{A}$ have real eigenvalues. Then there exists an invertible matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{T}$ is triangular.

Proof. Actually we will prove we can find a $\mathbf{P}$ of determinant 1. The proof is by induction on *n*. If $n = 1$, it is obvious. Otherwise, let $\mathbf{u}$ be an eigenvector of $\mathbf{A}$ with eigenvalue λ. So $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{Au} = \lambda\mathbf{u}$. Complete $\mathbf{u} = \mathbf{u}_1$ to a basis, $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$. Let $\mathbf{R} = \begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}$, and since we could have chosen any multiple of any of the columns for that column, we can assume without loss that $\det \mathbf{R} = 1$. Now

$$\mathbf{AR} = \begin{pmatrix} \mathbf{Au}_1 & \mathbf{Au}_2 & \cdots & \mathbf{Au}_n \end{pmatrix} = \begin{pmatrix} \lambda\mathbf{u}_1 & \mathbf{Au}_2 & \cdots & \mathbf{Au}_n \end{pmatrix} =$$

$$\begin{pmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_n \end{pmatrix}\begin{pmatrix} \lambda & \mathbf{v}^{\mathrm{T}} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} = \mathbf{R}\begin{pmatrix} \lambda & \mathbf{v}^{\mathrm{T}} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}$$

where $\mathbf{v}$ is a vector of size $n-1$ and $\mathbf{B}$ is an $(n-1)\times(n-1)$ matrix. Since $c_{\mathbf{A}}(x) = (x-\lambda)c_{\mathbf{B}}(x)$, $\mathbf{B}$ has real eigenvalues. By the induction hypothesis then we can find a matrix real matrix $\mathbf{Q}$ of determinant 1, and an upper triangular matrix $\mathbf{S}$ so that $\mathbf{BQ} = \mathbf{QS}$. Let $\mathbf{P} = \mathbf{R}\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}$. Then clearly $\det \mathbf{P} = 1$. Also

$$\mathbf{AP} = \mathbf{AR}\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix} = \mathbf{R}\begin{pmatrix} \lambda & \mathbf{v}^{\mathrm{T}} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix} = \mathbf{R}\begin{pmatrix} \lambda & \mathbf{v}^{\mathrm{T}}\mathbf{Q} \\ \mathbf{0} & \mathbf{BQ} \end{pmatrix} =$$

$$\mathbf{R}\begin{pmatrix} \lambda & \mathbf{v}^{\mathrm{T}}\mathbf{Q} \\ \mathbf{0} & \mathbf{QS} \end{pmatrix} = \mathbf{R}\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{Q} \end{pmatrix}\begin{pmatrix} \lambda & \mathbf{v}^{\mathrm{T}}\mathbf{Q} \\ \mathbf{0} & \mathbf{S} \end{pmatrix} = \mathbf{PT}$$

where $\mathbf{T} = \begin{pmatrix} \lambda & \mathbf{v}^{\mathrm{T}}\mathbf{Q} \\ \mathbf{0} & \mathbf{S} \end{pmatrix}$, an upper triangular matrix, and we are done.⌘

---

❶❺ Page 149

Theorem (Minimum Polynomials and Diagonability). Let $\mathbf{A}$ be square. Then the following are equivalent:

① $\mathbf{A}$ is diagonable.

② $m_{\mathbf{A}}(x)$ has no repeated roots.

③ There exists a polynomial $p(x)$ with no repeated roots that $\mathbf{A}$ satisfies, *i.e.*, $p(\mathbf{A}) = \mathbf{0}$.

Proof. Clearly, since $m_{\mathbf{A}}(x)$ is a factor of every polynomial that $\mathbf{A}$ satisfies, ② and ③ are equivalent. If we assume ①, then since two similar matrices have the same minimum polynomial, it suffices it to prove ② for a diagonal matrix. But in order to produce a zero matrix from a diagonal one, all we need to is take one factor for each of the different elements in the diagonal, and we have ②. So we only have to show that ② implies ①. So assume that for some distinct numbers λ_1, $\lambda_2, \ldots, \lambda_t$,

$$m_{\mathbf{A}}(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_t).$$

Of course, each of these is an eigenvalue of $\mathbf{A}$. We will produce enough eigenvectors for each of these eigenvalues. It suffices it to do it for λ_1. Without loss, by the **Triangularity Theorem**, we can assume we can find an invertible matrix $\mathbf{P}$ such $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{T}$ is triangular and $\mathbf{T} = \begin{pmatrix} \mathbf{M} & \mathbf{X} \\ \mathbf{0} & \mathbf{N} \end{pmatrix}$ where $\mathbf{M}$ is upper triangular of size $k \times k$ with λ_1's along the main diagonal and $\mathbf{N}$ is upper triangular and none of its diagonal entries is λ_1. Hence k is the algebraic multiplicity of λ_1 in $c_{\mathbf{A}}(x)$, so in order for $\mathbf{A}$ to be diagonable, we need to find k eigenvectors for λ_1. But if we show that $\mathbf{M} = \lambda_1\mathbf{I}$, then the first k columns of $\mathbf{P}$ will all be such eigenvectors, and we will be done. We have $(\mathbf{T} - \lambda_1\mathbf{I})(\mathbf{T} - \lambda_2\mathbf{I})\cdots(\mathbf{T} - \lambda_t\mathbf{I}) = \mathbf{0}$ so by block multiplication $(\mathbf{M} - \lambda_1\mathbf{I})(\mathbf{M} - \lambda_2\mathbf{I})\cdots(\mathbf{M} - \lambda_t\mathbf{I}) = \mathbf{0}$. However, for $i > 1$, $\mathbf{M} - \lambda_i\mathbf{I}$, is an invertible matrix, and so $\mathbf{M} - \lambda_1\mathbf{I} = \mathbf{0}$. ⌘

❶❻ Page 162

Lemma (Real Eigenvalues). Let $\mathbf{A}$ be a real symmetric matrix. Then $\mathbf{A}$ has real eigenvalues.

Ironically, in order to prove this we need to explore complex numbers further. We assume the reader is familiar with the complex numbers as being the set of all numbers of the form $a + b\mathbf{i}$ where $\mathbf{i}^2 = -1$ (one could think of these as 2-vectors. Thus complex numbers correspond to points in the plane, as real numbers correspond to points in the line.

The addition is like vector addition, coordinate-wise,

$$(a+b\mathbf{i})+(c+d\mathbf{i})=(a+c)+(b+d)\mathbf{i}$$

where a,b,c,d are real numbers.

Subtraction is easily understood since negatives are available readily:

$$-(a+b\mathbf{i})=-a-b\mathbf{i}.$$

and subtraction is nothing but addition of the negative.

What about multiplication? Just use the distributive law:

$$(2+3\mathbf{i})(1+\mathbf{i})=2(1+\mathbf{i})+3\mathbf{i}(1+\mathbf{i})\ =2+2\mathbf{i}+3\mathbf{i}+3\mathbf{i}^2.$$

The only confusing term is $3\mathbf{i}^2$, but recalling what $\mathbf{i}$ is all about, $\mathbf{i}^2=-1$, so $3\mathbf{i}^2=-3$, hence

$$(2+3\mathbf{i})(1+\mathbf{i})=-1+5\mathbf{i}.$$

And in general,

$$(a+b\mathbf{i})(c+d\mathbf{i})=ac+ad\mathbf{i}+bc\mathbf{i}+bd\mathbf{i}^2=(ac-bd)+(ad+bc)\mathbf{i}.$$

As usual, to understand division, we need to understand reciprocals. Some pose no problem, for example, $\frac{1}{\mathbf{i}}=-\mathbf{i}$ since $\mathbf{i}(-\mathbf{i})=1$. But what about $\frac{1}{1+\mathbf{i}}$?

To accomplish this, we need to define the **conjugate** of a complex number. If $z=a+b\mathbf{i}$ is a complex number, then its conjugate, denoted by $\overline{z}$, is defined by $\overline{z}=a-b\mathbf{i}$. The conjugate satisfies $z\overline{z}=a^2+b^2$, which is a positive real number for any $z\neq 0$. Also $\overline{z}=z$ exactly when z is a real number. We also have $\overline{z+u}=\overline{z}+\overline{u}$ (conjugate of a sum is the sum of the conjugates) and $\overline{zu}=\overline{z}\,\overline{u}$ (conjugate of a product is the product of the conjugates).

Returning to $\frac{1}{1+\mathbf{i}}$, if we multiply both numerator and denominator by the conjugate of $1+\mathbf{i}$, $1-\mathbf{i}$, we get that $\frac{1}{1+\mathbf{i}}=\frac{1-\mathbf{i}}{(1+\mathbf{i})(1-\mathbf{i})}=\frac{1-\mathbf{i}}{2}=\frac{1}{2}-\frac{\mathbf{i}}{2}$ and we have succeeded in finding the reciprocal., and indeed this exemplifies the general technique for division.

The key distinction between the complex numbers and the real numbers when it comes to vectors is the fact that for any real nonzero vector, $\mathbf{u}^{\mathrm{T}}\mathbf{u}>0$. But as we can see if we let $\mathbf{u}=\begin{pmatrix}1\\ \mathbf{i}\end{pmatrix}$, the same is not true for complex vectors. Rather, when one discusses complex matrices and vectors, rather than the transpose of it, one considers the **conjugate transpose** of it, denoted by $\mathbf{A}^*=\overline{\mathbf{A}^{\mathrm{T}}}=\overline{\mathbf{A}}^{\mathrm{T}}$. For example $\begin{pmatrix}1+\mathbf{i} & \mathbf{i}\\ 2 & 3\end{pmatrix}^*=\begin{pmatrix}1-\mathbf{i} & 2\\ -\mathbf{i} & 3\end{pmatrix}$. Some of the properties of the conjugate transpose are reminiscent of the properties of the transpose and they include:

① $(\mathbf{A}+\mathbf{B})^* = \mathbf{A}^* + \mathbf{B}^*$

② $(\mathbf{AB})^* = \mathbf{B}^*\mathbf{A}^*$

③ $\mathbf{A}^* = \mathbf{A}^{\mathrm{T}}$ if and only if $\mathbf{A}$ has real entries.

④ If $\mathbf{u} \neq \mathbf{0}$, then $\mathbf{u}^*\mathbf{u} > 0$.

There is one theorem about complex numbers that we will not prove. It is known as the **Fundamental Theorem of Algebra** and it simply states that

every real polynomial has a complex root.

For our course, it would be equivalently stated as

every real matrix has a complex eigenvalue.

Actually, more is true, every complex matrix of size n has n complex eigenvalues.

And now we are ready to return to our goal lemma. So let $\mathbf{A}$ be real symmetric. By the **Fundamental Theorem of Algebra**, it has a complete set of eigenvalues. All we need to show is that they are real. So let $\mathbf{Au} = \lambda\mathbf{u}$. But then by conjugate transposing, we get $\mathbf{u}^*\mathbf{A}^* = \overline{\lambda}\mathbf{u}^*$. But now let us compute $\mathbf{u}^*\mathbf{A}^*\mathbf{u}$:

$$\overline{\lambda}\mathbf{u}^*\mathbf{u} = (\mathbf{u}^*\mathbf{A}^*)\mathbf{u} = \mathbf{u}^*(\mathbf{A}^*\mathbf{u}) = \mathbf{u}^*(\mathbf{Au}) = \mathbf{u}^*(\lambda\mathbf{u}) = \lambda\mathbf{u}^*\mathbf{u}$$

and since $\mathbf{u}^*\mathbf{u} > 0$, we can conclude $\lambda = \overline{\lambda}$, it is real.

❶❻ Page 163

> **Lemma (Schur's Lemma).** Let $\mathbf{A}$ have real eigenvalues. Then there exists an orthogonal matrix $\mathbf{P}$ such that $\mathbf{P}^{-1}\mathbf{AP} = \mathbf{P}^{\mathrm{T}}\mathbf{AP} = \mathbf{T}$, an upper triangular matrix.

Proof. By induction on n, the size of $\mathbf{A}$. If $n = 1$, there is nothing to prove. Assume it true then for smaller matrices, and let $\mathbf{u}$ be an eigenvector of $\mathbf{A}$ with eigenvalue λ. So $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{Au} = \lambda\mathbf{u}$, moreover we can assume $\mathbf{u}^{\mathrm{T}}\mathbf{u} = 1$. Since every orthonormal set can be completed to an orthonormal basis, we can find an orthogonal matrix $\mathbf{Q}$ with first column $\mathbf{u}$. But then, as we have seen several times before,

$$\mathbf{AQ} = \begin{pmatrix}\mathbf{Au} & \mathbf{Au}_2 & \cdots & \mathbf{Au}_n\end{pmatrix} = \begin{pmatrix}\lambda\mathbf{u} & \mathbf{Au}_2 & \cdots & \mathbf{Au}_n\end{pmatrix} =$$

$$\begin{pmatrix}\mathbf{u} & \mathbf{u}_2 & \cdots & \mathbf{u}_n\end{pmatrix}\begin{pmatrix}\lambda & \mathbf{v}^{\mathrm{T}} \\ \mathbf{0} & \mathbf{B}\end{pmatrix} = \mathbf{Q}\begin{pmatrix}\lambda & \mathbf{v}^{\mathrm{T}} \\ \mathbf{0} & \mathbf{B}\end{pmatrix}$$

where $\mathbf{v}$ is a vector of size $n-1$ and $\mathbf{B}$ is an $(n-1)\times(n-1)$ matrix. Since $c_{\mathbf{A}}(x) = (x-\lambda)c_{\mathbf{B}}(x)$, $\mathbf{B}$ also has real eigenvalues. By the induction hypothesis then we can find an orthogonal matrix $\mathbf{M}$ such that $\mathbf{M}^{\mathrm{T}}\mathbf{B}\mathbf{M}=\mathbf{S}$ where $\mathbf{S}$ is an upper triangular matrix. Let $\mathbf{P}=\mathbf{Q}\begin{pmatrix}1 & \mathbf{0}\\ \mathbf{0} & \mathbf{M}\end{pmatrix}$. Then trivially, $\mathbf{P}$ is orthogonal and

$$\mathbf{P}^{\mathrm{T}}\mathbf{A}\mathbf{P}=\begin{pmatrix}1 & \mathbf{0}\\ \mathbf{0} & \mathbf{M}^{\mathrm{T}}\end{pmatrix}\mathbf{Q}^{\mathrm{T}}\mathbf{A}\mathbf{Q}\begin{pmatrix}1 & \mathbf{0}\\ \mathbf{0} & \mathbf{M}\end{pmatrix}=\begin{pmatrix}1 & \mathbf{0}\\ \mathbf{0} & \mathbf{M}^{\mathrm{T}}\end{pmatrix}\begin{pmatrix}\lambda & \mathbf{v}^{\mathrm{T}}\\ \mathbf{0} & \mathbf{B}\end{pmatrix}\begin{pmatrix}1 & \mathbf{0}\\ \mathbf{0} & \mathbf{M}\end{pmatrix}=\begin{pmatrix}1 & \mathbf{0}\\ \mathbf{0} & \mathbf{M}^{\mathrm{T}}\end{pmatrix}\begin{pmatrix}\lambda & \mathbf{v}^{\mathrm{T}}\mathbf{M}\\ \mathbf{0} & \mathbf{B}\mathbf{M}\end{pmatrix}=$$

$$\begin{pmatrix}\lambda & \mathbf{v}^{\mathrm{T}}\mathbf{M}\\ \mathbf{0} & \mathbf{M}^{\mathrm{T}}\mathbf{B}\mathbf{M}\end{pmatrix}=\begin{pmatrix}\lambda & \mathbf{v}^{\mathrm{T}}\mathbf{M}\\ \mathbf{0} & \mathbf{S}\end{pmatrix}=\mathbf{T},$$

an upper triangular matrix. ⌘

On Conics Page 166

> **Theorem (Five Points).** Any five points lie on a conic. Moreover, the conic is unique if and only if no four of the points are collinear.

By our discussion in the text, we need to show that $\mathbf{A}=\begin{pmatrix}x_1^2 & 2x_1y_1 & y_1^2 & x_1 & y_1 & -1\\ x_2^2 & 2x_2y_2 & y_2^2 & x_2 & y_2 & -1\\ x_3^2 & 2x_3y_3 & y_3^2 & x_3 & y_3 & -1\\ x_4^2 & 2x_4y_4 & y_4^2 & x_4 & y_4 & -1\\ x_5^2 & 2x_5y_5 & y_5^2 & x_5 & y_5 & -1\end{pmatrix}$ has rank 5 unless 4 of the points are collinear.

For $\mathbf{u}_i=\begin{pmatrix}x_i\\ y_i\end{pmatrix}$ for $i=1,\ldots,5$, define $F\left(\mathbf{u}_1 \quad \mathbf{u}_2 \quad \cdots \quad \mathbf{u}_5\right)=r\left(\mathbf{A}\right)$ where $\mathbf{A}$ is as defined above.

Trivially, by the symmetry in the x's and the y's, if $\mathbf{P}$ is a permutation matrix

① $\quad F\left(\mathbf{P}\mathbf{u}_1 \quad \mathbf{P}\mathbf{u}_2 \quad \cdots \quad \mathbf{P}\mathbf{u}_5\right)=F\left(\mathbf{u}_1 \quad \mathbf{u}_2 \quad \cdots \quad \mathbf{u}_5\right)$

② $\quad F\left(\mathbf{u}_1+\mathbf{v} \quad \mathbf{u}_2+\mathbf{v} \quad \cdots \quad \mathbf{u}_5+\mathbf{v}\right)=F\left(\mathbf{u}_1 \quad \mathbf{u}_2 \quad \cdots \quad \mathbf{u}_5\right)$.

Proof. It suffices to show it if $\mathbf{v}=\begin{pmatrix}a\\ 0\end{pmatrix}$ by ②. But by simple column reductions:

$$r\begin{pmatrix} x_1^2+2ax_1+a^2 & 2x_1y_1+2ay_1 & y_1^2 & x_1+a & y_1 & -1 \\ x_2^2+2ax_2+a^2 & 2x_2y_2+2ay_2 & y_2^2 & x_2+a & y_2 & -1 \\ x_3^2+2ax_3+a^2 & 2x_3y_3+2ay_3 & y_3^2 & x_3+a & y_3 & -1 \\ x_4^2+2ax_4+a^2 & 2x_4y_4+2ay_4 & y_4^2 & x_4+a & y_4 & -1 \\ x_5^2+2ax_5+a^2 & 2x_5y_5+2ay_5 & y_5^2 & x_5+a & y_5 & -1 \end{pmatrix}$$

$$=r\begin{pmatrix} x_1^2+2ax_1+a^2 & 2x_1y_1+2ay_1 & y_1^2 & x_1 & y_1 & -1 \\ x_2^2+2ax_2+a^2 & 2x_2y_2+2ay_2 & y_2^2 & x_2 & y_2 & -1 \\ x_3^2+2ax_3+a^2 & 2x_3y_3+2ay_3 & y_3^2 & x_3 & y_3 & -1 \\ x_4^2+2ax_4+a^2 & 2x_4y_4+2ay_4 & y_4^2 & x_4 & y_4 & -1 \\ x_5^2+2ax_5+a^2 & 2x_5y_5+2ay_5 & y_5^2 & x_5 & y_5 & -1 \end{pmatrix}$$

$$=r\begin{pmatrix} x_1^2+2ax_1 & 2x_1y_1+2ay_1 & y_1^2 & x_1 & y_1 & -1 \\ x_2^2+2ax_2 & 2x_2y_2+2ay_2 & y_2^2 & x_2 & y_2 & -1 \\ x_3^2+2ax_3 & 2x_3y_3+2ay_3 & y_3^2 & x_3 & y_3 & -1 \\ x_4^2+2ax_4 & 2x_4y_4+2ay_4 & y_4^2 & x_4 & y_4 & -1 \\ x_5^2+2ax_5 & 2x_5y_5+2ay_5 & y_5^2 & x_5 & y_5 & -1 \end{pmatrix}$$

$$=r\begin{pmatrix} x_1^2+2ax_1 & 2x_1y_1 & y_1^2 & x_1 & y_1 & -1 \\ x_2^2+2ax_2 & 2x_2y_2 & y_2^2 & x_2 & y_2 & -1 \\ x_3^2+2ax_3 & 2x_3y_3 & y_3^2 & x_3 & y_3 & -1 \\ x_4^2+2ax_4 & 2x_4y_4 & y_4^2 & x_4 & y_4 & -1 \\ x_5^2+2ax_5 & 2x_5y_5 & y_5^2 & x_5 & y_5 & -1 \end{pmatrix}=r\begin{pmatrix} x_1^2 & 2x_1y_1 & y_1^2 & x_1 & y_1 & -1 \\ x_2^2 & 2x_2y_2 & y_2^2 & x_2 & y_2 & -1 \\ x_3^2 & 2x_3y_3 & y_3^2 & x_3 & y_3 & -1 \\ x_4^2 & 2x_4y_4 & y_4^2 & x_4 & y_4 & -1 \\ x_5^2 & 2x_5y_5 & y_5^2 & x_5 & y_5 & -1 \end{pmatrix}.$$

For any invertible diagonal matrix $\mathbf{D}$,

③ $$F\begin{pmatrix}\mathbf{Du}_1 & \mathbf{Du}_2 & \cdots & \mathbf{Du}_5\end{pmatrix}=F\begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_5\end{pmatrix}.$$

Simply, if $\mathbf{D}=\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, then

$$\begin{pmatrix} a^2x_1^2 & 2abx_1y_1 & b^2y_1^2 & ax_1 & by_1 & -1 \\ a^2x_2^2 & 2abx_2y_2 & b^2y_2^2 & ax_2 & by_2 & -1 \\ a^2x_3^2 & 2abx_3y_3 & b^2y_3^2 & ax_3 & by_3 & -1 \\ a^2x_4^2 & 2abx_4y_4 & b^2y_4^2 & ax_4 & by_4 & -1 \\ a^2x_5^2 & 2abx_5y_5 & b^2y_5^2 & ax_5 & by_5 & -1 \end{pmatrix}$$

$$=\begin{pmatrix} x_1^2 & 2x_1y_1 & y_1^2 & x_1 & y_1 & -1 \\ x_2^2 & 2x_2y_2 & y_2^2 & x_2 & y_2 & -1 \\ x_3^2 & 2x_3y_3 & y_3^2 & x_3 & y_3 & -1 \\ x_4^2 & 2x_4y_4 & y_4^2 & x_4 & y_4 & -1 \\ x_5^2 & 2x_5y_5 & y_5^2 & x_5 & y_5 & -1 \end{pmatrix}\begin{pmatrix} a^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & ab & 0 & 0 & 0 & 0 \\ 0 & 0 & b^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

so they have the same rank.

For any matrix $\mathbf{B}$ of the form $\mathbf{B}=\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$

④ $\qquad F\left(\mathbf{Bu}_1 \quad \mathbf{Bu}_2 \quad \cdots \quad \mathbf{Bu}_5\right)=F\left(\mathbf{u}_1 \quad \mathbf{u}_2 \quad \cdots \quad \mathbf{u}_5\right)$.

$$\begin{pmatrix} x_1^2+2bx_1y_1+b^2y_1^2 & 2x_1y_1+2by_1^2 & y_1^2 & x_1+by_1 & y_1 & -1\\ x_2^2+2bx_2y_2+b^2y_2^2 & 2x_2y_2+2by_2^2 & y_2^2 & x_2+by_2 & y_2 & -1\\ x_3^2+2bx_3y_3+b^2y_3^2 & 2x_3y_3+2by_3^2 & y_3^2 & x_3+by_3 & y_3 & -1\\ x_4^2+2bx_4y_4+b^2y_4^2 & 2x_4y_4+2by_4^2 & y_4^2 & x_4+by_4 & y_4 & -1\\ x_5^2+2bx_5y_5+b^2y_5^2 & 2x_5y_5+2by_5^2 & y_5^2 & x_5+by_5 & y_5 & -1 \end{pmatrix}$$
$$=\begin{pmatrix} x_1^2 & 2x_1y_1 & y_1^2 & x_1 & y_1 & -1\\ x_2^2 & 2x_2y_2 & y_2^2 & x_2 & y_2 & -1\\ x_3^2 & 2x_3y_3 & y_3^2 & x_3 & y_3 & -1\\ x_4^2 & 2x_4y_4 & y_4^2 & x_4 & y_4 & -1\\ x_5^2 & 2x_5y_5 & y_5^2 & x_5 & y_5 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0\\ b & 1 & 0 & 0 & 0 & 0\\ b^2 & 2b & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & b & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

so again they have the same rank.

Finally by putting ①, ③ and ④ together, we have that
For any invertible matrix $\mathbf{C}$

⑤ $\qquad F\left(\mathbf{Cu}_1 \quad \mathbf{Cu}_2 \quad \cdots \quad \mathbf{Cu}_5\right)=F\left(\mathbf{u}_1 \quad \mathbf{u}_2 \quad \cdots \quad \mathbf{u}_5\right)$.

Now we are ready to prove the claim about the rank. Clearly if 4 points are collinear, then take that line together with any line going through the other point, and that will be a conic containing all five points. Clearly there are infinitely many such possibilities. So assume no four points are collinear. Without loss by ② we can assume $\mathbf{u}_1=\mathbf{0}$. Now we can assume $\mathbf{u}_2$ and $\mathbf{u}_3$ are linearly independent. Let $\mathbf{C}^{-1}=\left(\mathbf{u}_2 \quad \mathbf{u}_3\right)$. Then

$$F\left(\mathbf{u}_1 \quad \mathbf{u}_2 \quad \cdots \quad \mathbf{u}_5\right)=F\left(\mathbf{Cu}_1 \quad \mathbf{Cu}_2 \quad \cdots \quad \mathbf{Cu}_5\right)=F\left(\begin{pmatrix}0\\0\end{pmatrix} \quad \begin{pmatrix}1\\0\end{pmatrix} \quad \begin{pmatrix}0\\1\end{pmatrix} \quad \begin{pmatrix}p\\q\end{pmatrix} \quad \begin{pmatrix}r\\s\end{pmatrix}\right).$$

But the matrix then is of the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1\\ 1 & 0 & 0 & 1 & 0 & -1\\ 0 & 0 & 1 & 0 & 1 & -1\\ p^2 & 2pq & q^2 & p & q & -1\\ r^2 & 2rs & s^2 & r & s & -1 \end{pmatrix}.$$

which after a little reduction becomes

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ p^2-p & 2pq & q^2-q & 0 & 0 & 0 \\ r^2-r & 2rs & s^2-s & 0 & 0 & 0 \end{pmatrix}$$

and we need to argue the last two rows have rank 2. All we need to find is a 2×2 subdeterminant that is not 0. If $p=0$, then $q\neq 0,1$ since the points are different, and so $q^2-q\neq 0$. Also $r\neq 0$ for otherwise there would 4 collinear points. If $r\neq 1$, then consider the submatrix consisting of the first and third columns (and the last two rows of course): $\begin{pmatrix} 0 & q^2-q \\ r^2-r & s^2-s \end{pmatrix}$. If $r=1$, then $s\neq 0$, and then take the second and third columns: $\begin{pmatrix} 0 & q^2-q \\ 2s & s^2-s \end{pmatrix}$. Similarly, if either $q=0$, or $r=0$ or $s=0$. So we can assume none of them is 0. If $p=1$, then our submatrix is $\begin{pmatrix} 0 & 2q & q^2-q \\ r^2-r & 2rs & s^2-s \end{pmatrix}$. This is reduced to $\begin{pmatrix} 0 & 2 & q-1 \\ r^2-r & 2rs & s^2-s \end{pmatrix}$, and if $r\neq 1$, we are done. If on the other hand $r=1$, then we can reduce the matrix to $\begin{pmatrix} 0 & 2 & q-1 \\ 0 & 2 & s-1 \end{pmatrix}$, and since $q\neq s$ then, we are done. So we can assume none of them are 1. By dividing the first row of $\begin{pmatrix} p^2-p & 2pq & q^2-q \\ r^2-r & 2rs & s^2-s \end{pmatrix}$ by pq and the second one by *rs*, we obtain $\begin{pmatrix} \dfrac{p-1}{q} & 2 & \dfrac{q-1}{p} \\ \dfrac{r-1}{s} & 2 & \dfrac{s-1}{r} \end{pmatrix}$, and if this matrix were to be of rank 1 then $\dfrac{p-1}{q}=\dfrac{r-1}{s}$ and $\dfrac{q-1}{p}=\dfrac{s-1}{r}$ would have to happen. By cross-multiplying and subtracting, we get $p-s=r-q$. Thus we have $p+q=r+s=n\neq 1$. Now $n\neq 1$, for if it were 1, then we would have four points on the line $x+y=1$. By letting $q=n-p$ and $s=n-r$ in the first equation, we get

$$\frac{p-1}{n-p}=\frac{r-1}{n-r},$$

and when denominators are cleared, one gets $np-n-pr+r=nr-n-pr+p$, and so $(n-1)p=(n-1)r$, and since $n\neq 1$, we conclude $p=r$. But this is a contradiction since that would imply $q=s$, and we would equal points. Hence we do have a submatrix of rank 2, and so the whole matrix is of rank 5. ⌘

On Conics   Page 167

Theorem (Affine Transformations & Conics). Let $\mathbf{A}$ be an invertible matrix and let $\mathbf{b}$ be any vector.

① $F_{\mathbf{A},\mathbf{0}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)=\mathfrak{C}\left(\mathbf{N},\mathbf{d},f\right)$ where

$$\mathbf{N}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{M}\mathbf{A}^{-1} \text{ and } \mathbf{d}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c};$$

② $F_{\mathbf{I},\mathbf{b}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)=\mathfrak{C}\left(\mathbf{M},\mathbf{e},g\right)$ where

$$\mathbf{e}=\mathbf{c}-2\mathbf{M}\mathbf{b} \text{ and } g=f+\mathbf{b}\cdot\mathbf{c}-\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{b}$$

So combining ① and ②, we get

③ $F_{\mathbf{A},\mathbf{b}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)=\mathfrak{C}\left(\mathbf{N},\mathbf{k},h\right)$ where

$$\mathbf{N}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{M}\mathbf{A}^{-1},\ \mathbf{k}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}-2\mathbf{N}\mathbf{b} \text{ and}$$

$$h=f+\mathbf{b}\cdot\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}\mathbf{c}-\mathbf{b}^{\mathrm{T}}\mathbf{N}\mathbf{b}.$$

Proof. Let $\mathbf{z}\in\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)$, so $\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{z}+\mathbf{z}^{\mathrm{T}}\mathbf{c}=f$. But then, for ①,

$$\left(\mathbf{A}\mathbf{z}\right)^{\mathrm{T}}\mathbf{N}\left(\mathbf{A}\mathbf{z}\right)+\left(\mathbf{A}\mathbf{z}\right)^{\mathrm{T}}\mathbf{d}=\left(\mathbf{A}\mathbf{z}\right)^{\mathrm{T}}\left(\mathbf{A}^{\mathrm{T}}\right)^{-1}\mathbf{M}\mathbf{A}^{-1}\left(\mathbf{A}\mathbf{z}\right)+\left(\mathbf{A}\mathbf{z}\right)^{\mathrm{T}}\left(\mathbf{A}^{\mathrm{T}}\right)^{-1}\mathbf{c}=\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{z}+\mathbf{z}^{\mathrm{T}}\mathbf{c}=f$$

since $\left(\mathbf{A}^{\mathrm{T}}\right)^{-1}=\left(\mathbf{A}^{-1}\right)^{\mathrm{T}}$. Thus $F_{\mathbf{A},\mathbf{0}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)$ is contained in $\mathfrak{C}\left(\mathbf{N},\mathbf{d},f\right)$. But by applying what we have just proven to $\mathfrak{C}\left(\mathbf{N},\mathbf{d},f\right)$ and $\mathbf{A}^{-1}$, we get $F_{\mathbf{A}^{-1},\mathbf{0}}\left(\mathfrak{C}\left(\mathbf{N},\mathbf{d},f\right)\right)$ is contained in $\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)$, and so multiplying by $F_{\mathbf{A},\mathbf{0}}$, we get $\mathfrak{C}\left(\mathbf{N},\mathbf{d},f\right)$ is contained in $F_{\mathbf{A},\mathbf{0}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)$, and so we obtain ①. For ②, if $\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{z}+\mathbf{z}^{\mathrm{T}}\mathbf{c}=f$, then

$$\left(\mathbf{z}+\mathbf{b}\right)^{\mathrm{T}}\mathbf{M}\left(\mathbf{z}+\mathbf{b}\right)+\left(\mathbf{z}+\mathbf{b}\right)^{\mathrm{T}}\mathbf{e}=\left(\mathbf{z}+\mathbf{b}\right)^{\mathrm{T}}\mathbf{M}\left(\mathbf{z}+\mathbf{b}\right)+\left(\mathbf{z}+\mathbf{b}\right)^{\mathrm{T}}\left(\mathbf{c}-2\mathbf{M}\mathbf{b}\right)=$$

$$\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{z}+\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{z}+\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{b}+\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{b}+\mathbf{z}^{\mathrm{T}}\mathbf{c}+\mathbf{b}^{\mathrm{T}}\mathbf{c}-2\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{b}-2\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{b}=$$

$$\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{z}+\mathbf{z}^{\mathrm{T}}\mathbf{c}+2\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{b}+\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{b}+\mathbf{b}^{\mathrm{T}}\mathbf{c}-2\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{b}-2\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{b}=f+\mathbf{b}^{\mathrm{T}}\mathbf{c}-\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{b}=g$$

where we used the fact that $\mathbf{b}^{\mathrm{T}}\mathbf{M}\mathbf{z}=\mathbf{z}^{\mathrm{T}}\mathbf{M}\mathbf{b}$ since $\mathbf{M}$ is a symmetric matrix. So we obtain $F_{\mathbf{I},\mathbf{b}}\left(\mathfrak{C}\left(\mathbf{M},\mathbf{c},f\right)\right)$ is contained in $\mathfrak{C}\left(\mathbf{M},\mathbf{e},g\right)$. To finish the proof of ②, we apply what just been proven to $\mathfrak{C}\left(\mathbf{M},\mathbf{e},g\right)$ and $F_{\mathbf{I},-\mathbf{b}}$, and the rest is just as in ①. Finally, ③ follows immediately from ① and ② since $F_{\mathbf{A},\mathbf{b}}=F_{\mathbf{I},\mathbf{b}}\circ F_{\mathbf{A},\mathbf{0}}$. ⌘

index

2-path, 13
3-path, 13
3-space, 72, 77, 106

A

adding a multiple of a row to another row, 44, 123
adjacency matrix, 2, 3
adjoint theorem, 117, 121
adjoint, 116
affine function, 167
affine transformations & conics, 167
affine transformations, 167
angle, 75
antipodal, 103
Appendix of Proofs, 117, 141, 162, 166
associativity, 5, 25
augmented matrix, 45
axis of rotation, 106

B

balanced block decomposition, 10
balanced block, 28
basis, 94, 95, 97, 101
belongs, 79
bijection, 107
block multiplication, 28
block upper triangular, 37, 38, 126
blocking, 26

C

cancellation, 25, 34
Cayley, 143
Cayley-Hamilton Theorem, 144, 149
characteristic polynomial, 128, 134, 140, 153
classical adjoint, 116
closure under addition, 91
collinear, 166
column and left null spaces, 99
column reducing, 124
column space, 79, 88, 98
column vectors, 1
columns by rows, 17
communication network, 2, 19
commutativity, 5, 25
complete graph, 21
complex numbers, 138
composition, 102
conics, 165
constant vector, 42
corner, 67
Cramer's Rule, 122
cryptography, 40
cycle, 14

D

deer population, 132
Descartes, 69
determinant of a product is the product of the determinants, 123
determinant of inverse, 123
determinant, 34, 35, 73, 74, 116, 135, 153
determinants and inverses, 122
diagonability, 144, 170
diagonable, 140
diagonal matrix, 9, 18, 22, 32, 39
diagonal, 30, 127
different eigenvalues, 145
dilatation, 103
dimension of the eigenspace, 146
dimension, 91, 92, 94, 148
direct sum, 8
direction, 69
distributivity, 6, 25
dot product, 11

E

edges, 2
eigenspace, 128, 147
eigenvalue, 128, 134, 153
eigenvalues and upper triangular form, 138
eigenvalues of a polynomial, 142
eigenvalues, 127
eigenvector, 128, 134
eigenvectors and independence, 145

ellipse, 172
entry-by-entry, 17
equations and inverses, 43
Example 1, 11
Example 2, 16, 20
Example 3, 13
Example 4, 23
Example 5 Revisited, 130
existence of solutions, 49, 85

F

Fermat, 69
Fibonacci Sequence, 127
Fibonacci, 130
five points, 166
free variables, 60
full column rank, 53, 57, 87, 93, 108
full rank, 53
full row rank, 53, 55, 85, 108

G

Gaussian elimination, 44, 46, 122
Gauss-Jordan, 53
geometry and eigenvectors, 138
Golden Ratio, 129
Gram-Schmidt, 157, 163

H

Hamilton, 143
Hamming distance, 160
homogeneous system, 59
hyperbola, 165, 172
hyperplane, 77

I

I matrix, 23
idempotent, 112
identity function, 103
identity matrix, 23, 25
identity, 135, 166
image, 102
incidence matrix, 4
induction, 30
influence network, 3
inverse of a 2-by-2, 34
inverse of a 3-by-3, 36
inverse of a product, 32
inverse of the transpose, 32
inverse, 31
inverses & polynomials, 37
invertible, 31, 39, 43, 47, 53, 93, 97, 108, 121, 128, 134, 136

J

J matrix, 21, 135

L

law of exponents, 16
least squares, 113
left null space, 89
length of a vector, 72
length, 69, 72
line in the direction, 70
linear combination, 17, 55, 71, 80, 85
linear independence, 92
linear systems, 60
linear transformation, 102
linearly independent, 93, 94, 95, 109, 145
lower triangular, 9, 30

M

main diagonal, 2
Markov chain, 130
Mathematical Manual, 62
matrices, 1
matrix of coefficients, 42
matrix, 4
maximum, 67
minimal, 92
minimum polynomial, 148, 151, 153
minimum, 66
mod 27, 41
multiples, 70
multiplicativity, 123
multiplicity, 146
multiplying a row by a nonzero number, 44, 123
mutually orthogonal, 154

N

nearest point, 113
nodes, 2
nonpivotal columns, 56, 81, 99
nonpivotal, 60

nonzero, 128
normal, 105
null space, 62, 86, 88, 129
nullity, 98
number of columns, 12
number of rows, 12

O

one-dimensional object, 71
one-to-one, 107, 108
onto, 107, 108
order of multiplication, 13
orientation, 74, 75
orthogonal basis, 159
orthogonal complement, 88, 89
orthogonal matrix, 156, 168
orthogonal sets, 154
orthogonal, 76, 154
orthogonality of eigenvectors, 162
orthogonality of rows, 156
orthonormal basis, 154
orthonormal, 154

P

parabola, 165, 172
parallelepiped, 74
parallelogram law, 70
parallelogram, 74
path, 13
permutation matrix, 32, 120
permutation, 133, 142
permuting rows, 44, 123
perpendicular, 76, 154
Petersen graph, 20, 28, 37, 142, 149
pivot, 48
pivotal column, 48
pivotal row, 48
pivoting, 46, 68
plane, 72
point, 69
polynomial in **A**, 24, 25
polynomial, 24, 37, 107
polynomials & eigenvalues, 141
powers of a matrix, 91
powers of a square matrix, 15
preserves distances, 155
preserves lengths, 155
projection on a plane, 106
projection, 104, 112, 153, 158
Pythagorean Theorem, 72

Q

quadratic, 165

R

rank & adjoints, 121
rank & equations, 55
rank of a product, 100
rank of transpose, 100
rank, 53, 109
ray, 70
real eigenvalues, 162
recursive, 11
reduce, 45
reduced form, 48, 53
reducing by hand, 52
reduction, 45
reflection on a plane, 105
reflection, 104, 105, 114, 138, 153
root, 135
rotation, 104, 106, 153
row and null spaces, 97
row echelon form, 48
row equivalent, 53
row expansion, 118
row of zeroes, 118
row reduced echelon form, 48
row reduced form, 48
row reduction, 42, 45
row space, 89
row times column, 17

S

scalar matrix, 148
scalar multiplication, 5, 70
scalar, 1, 128, 134
Schur's Lemma, 163
shear, 104
similar, 140
similarity, 140, 153
size of a matrix, 1
skew-symmetric, 91
spaces and matrices, 101
span, 72, 79, 80
spanning set, 92
Spectral Theorem, 163, 168
Spectrum of Inverse, 136
spectrum, 135, 141, 143
square of **A**, 13
square of the length, 72
square, 1, 37

stable, 132
stacking, 7, 26
standard basis, 95
subdeterminant, 35, 116, 119
subspace, 79, 91, 94, 96, 129
swap, 33
symmetric idempotents, 112
symmetric matrix, 23, 162
symmetric, 142, 165
symmetric, 8, 33, 91, 96, 112

T

tensor products, 8
trace, 135, 140, 153
transition matrix, 4, 130
translation, 167
translations, 167
transparent, 81, 89, 93
transpose of a sum, 8
transpose, 7, 22, 118, 120
trasformation, 102
triangular matrices, 30
triangularizable, 140
two identical rows, 118

U

uniqueness of solutions, 57, 87
uniqueness of the row echelon form, 50
unit circle, 168
unit vector, 73, 75, 76
upper triangular matrices, 29,119, 136, 143
upper triangular, 9, 38, 136, 143

V

vector subspace, 79
vector, 1, 69
vertices, 2

Z

zero function, 103
zero matrix, 2, 141