# Subfiles package example

Overleaf

## 1 Introduction

## Chapter 1

Notation: I use $\mathbf{a}_i$ to denote the $i$th column of matrix $A$, and $\mathbf{a}_j$ to denote the $j$th row.

1.7 Find a formula for $\begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}^n$, and prove it by induction.

**Discussion.** Call this matrix $A$, and consider what $A$ does to $B$ in the product $BA$: $A$ places $B$'s first column in the product's first column, $B$'s column 1 + $B$'s column 2 in the product's second column, and the sum of $B$'s 3 columns in the product's third column.

$$BA = \begin{bmatrix} | & | & | \\ \mathbf{b}_1 & \mathbf{b}_1 + \mathbf{b}_2 & \mathbf{b}_1 + \mathbf{b}_2 + \mathbf{b}_3 \\ | & | & | \end{bmatrix}$$

$$A^2 = AA = \begin{bmatrix} | & | & | \\ \mathbf{a}_1 & \mathbf{a}_1 + \mathbf{a}_2 & \mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3 \\ | & | & | \end{bmatrix}$$

If the left matrix is itself $A$, we can guess that repeated application of $A$ on the right will leave column 1 unchanged, so we suppose the first column of $A^n = (1, 0, 0)$. If this is correct, each right-multiplication by $A$ adds $(1, 0, 0)$ to $(1, 1, 0)$, making column 2 of $A^n = (n, 1, 0)$. For column 3 of $A^2$ we add $(1, 0, 0) + (1, 1, 0) + (1, 1, 1) = (3, 2, 1)$. For column 3 of $A^3$ we add $(1, 0, 0) + (2, 1, 0) + (3, 2, 1)$, and we suspect that in $A^n$'s 3rd column, the first entry is the sum $1 + 2 + \ldots + n$. So we guess the third column is $(\sum_{k=1}^{n} k, n, 1)$. The sum of the first k natural numbers has a well-known closed form, $n(n + 1)/2$, so we can now claim:

$$A^n = \begin{bmatrix} 1 & n & \frac{n(n+1)}{2} \\ & 1 & n \\ & & 1 \end{bmatrix}$$

**Proof by induction.**

For the base case we may use $n = 1$. Then $\frac{n(n+1)}{2} = 1(2)/2 = 1$ and the base case holds. Assuming this holds for some $n$, for the inductive step we would have:

$$\begin{aligned} A^{n+1} &= A^n A && \text{associativity} \\ &= \begin{bmatrix} 1 & n & \frac{n(n+1)}{2} \\ & 1 & n \\ & & 1 \end{bmatrix} A \\ &= \begin{bmatrix} 1 & n+1 & \frac{n(n+1)}{2} + n + 1 \\ & 1 & n+1 \\ & & 1 \end{bmatrix} \end{aligned}$$

The diagonal and superdiagonal are as we claimed. The top-right entry can be rewritten as:

$$\frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2n + 2}{2} = \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2}$$

which is also as claimed. Thus the proof is complete.

1.14 Find infinitely many matrices $B$ such that $BA = I_2$ when

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \\ 1 & 1 \end{bmatrix}$$

and prove there is no matrix $C$ such that $AC = I_3$.

**Discussion.** To find infinitely many solutions, we can find a vector that when added to $B$ doesn't change the product $BA$. By the row picture of matrix multiplication, the rows of $B$ specify linear combinations $A$ rows to make the product $BA$. So we'll look for a linear combination of $A$ rows that sum to $\mathbf{0}$. Then any multiple of this linear combination will also be $\mathbf{0}$, and can be added to $B$ without changing $BA$. Technically, we seek a vector in $A$'s left null space.

Consider the row space of $A$: there are three vectors in a 2-dimensional space so they must be linearly dependent. In fact we might see that the first row is the sum of the other two, and so $\mathbf{a}_1 - \mathbf{a}_2 - \mathbf{a}_3 = \mathbf{0}$. Therefore the row vector $[1 \ -1 \ -1]$ is in $A$'s left null space:

$$\lambda \begin{bmatrix} 1 & -1 & -1 \end{bmatrix} A = \mathbf{0}$$

Let $N = \begin{bmatrix} 1 & -1 & -1 \\ 1 & -1 & -1 \end{bmatrix}$, stacking this vector. Then:

$$NA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \text{ and } (B + \lambda N)A = BA + \lambda NA = BA + 0 = BA$$

Next we seek a matrix $\tilde{B}$ such that $\tilde{B}A = I_2$. We could ignore $A$'s third row and invert the 2-by-2 matrix $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$, its inverse is $\begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$. To make it the right size we append a column of zeros to get:

$$\tilde{B} = \begin{bmatrix} 2 & -3 & 0 \\ -1 & 2 & 0 \end{bmatrix}, \quad \tilde{B}A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$

Now we can let $B = \tilde{B} + \lambda N$ for any choice of scalar $\lambda$, and we'll have:

$$BA = (\tilde{B} + \lambda N)A = \tilde{B}A = I_2$$

To prove that there $A$ has no right-inverse $C$, observe that $A$ has 2 linearly independent columns and a 3-dimensional codomain. By rank-nullity, $A$ is not full-rank and cannot produce $I_3$.

1.15 With $A$ arbitrary, determine the products $e_{ij}A, Ae_{ij}, e_jAe_k, e_{ii}Ae_{jj}$, and $e_{ij}Ae_{k\ell}$

**Discussion.** Note that Artin defines $e_{ij}$ as a 'unit matrix', a matrix with a 1 at the $(i, j)$ coordinate and 0 elsewhere.

- $e_{ij}A$: since $e_{ij}$ is multiplying $A$ on the left, it is making linear combinations of $A$'s rows. Since it only has a 1 in column $j$ it extracts the $j$th row of $A$ and puts in in the $i$th row of the product, which is 0 everywhere else.

$$e_{ij}A = \begin{array}{cc} & j \\ i & \begin{bmatrix} & & \\ & 1 & \\ & & \end{bmatrix} \end{array} \begin{bmatrix} — & \mathbf{a}_1 & — \\ & \vdots & \\ — & \mathbf{a}_j & — \\ & \vdots & \\ — & \mathbf{a}_n & — \end{bmatrix} = \begin{array}{cc} i & \begin{bmatrix} & & \\ — & \mathbf{a}_j & — \\ & & \end{bmatrix} \end{array}$$

- $Ae_{ij}$: Note that the $j$th column of $e_{ij}$ is also the $i$th basis vector $e_i$. Multiplying $A$ by a basis vector $e_i$ simply extracts the $i$th column from $A$: $Ae_i = \mathbf{a}_i$. Next, consider that in $e_{ij}$ there are $j-1$ columns of $\mathbf{0}$ before the $\mathbf{e}_j$ column. So $Ae_{ij}$ is a matrix with $\mathbf{a}_i$ in the $j$th column and 0's everywhere else.

$$Ae_j = \begin{array}{cc} & \begin{bmatrix} | \\ e_i \\ | \end{bmatrix} \\ \begin{bmatrix} | & & | \\ \mathbf{a}_1 & \dots & \mathbf{a}_n \\ | & & | \end{bmatrix} & \begin{bmatrix} | \\ \mathbf{a}_i \\ | \end{bmatrix} \end{array}$$

$$Ae_{ij} = \begin{array}{cc} & \begin{array}{ccccc} & & j & & \end{array} \\ & \begin{bmatrix} & | & | & | & \\ \dots & \mathbf{0} & e_i & \mathbf{0} & \dots \\ & | & | & | & \end{bmatrix} \\ \begin{bmatrix} | & & | \\ \mathbf{a}_1 & \dots & \mathbf{a}_n \\ | & & | \end{bmatrix} & \begin{bmatrix} & | & | & | & \\ \dots & \mathbf{0} & \mathbf{a}_i & \mathbf{0} & \dots \\ & | & | & | & \end{bmatrix} \end{array}$$

  Alternatively, we can write $Ae_{ij} = (e_{ij}^\top A^\top)^\top = (e_{ji}A^\top)^\top$ and use the previous result: $e_{ji}A^\top$ places the $i$th row of $A^\top$ in the $j$th row of the product, then the transpose $(e_{ji}A^\top)^\top$ has the $i$th *row* of $A$ in the $j$th *column* (and zeros everywhere else).
- $e_jAe_k$: the product $e_jA$ is not defined for an arbitrary $A$. Suppose $e_j$ is $m \times 1$, then for $e_jA$ to be defined $A$ must have the shape $1 \times n$. Then $e_k$ must be $n \times 1$ for the product $e_jAe_k$ to be defined. It would be very unconventional for $e_j$ and $e_k$ to have different shapes, but nevertheless $Ae_k$ would be the single entry matrix $[a_{1k}]$, which then multiplies $e_j$ like a scalar to produce $a_{1k}e_j$. In case Artin intended the product to read $e_j^\top Ae_k$, the answer would be that $e_j^\top A$ extracts the $j$th row of $A$, then multiplying by $e_k$ extracts the $k$th component of that row: $e_j^\top Ae_k = a_{jk}$
- $e_{ii}Ae_{jj}$: using previous results, $Ae_{jj}$ has the effect of zeroing out $A$ except for the $j$th column. Multiplying this by $e_{ii}$ on the left zeros out everything but the $i$th row, which leaves only $a_{ij}$ and zeros everywhere else: $e_{ii}Ae_{jj} = a_{ij}e_{ij}$ .
- $e_{ij}Ae_{k\ell}$: the product $Ae_{k\ell}$ is a matrix with $\mathbf{a}_k$ in the $\ell$th column and zeros everywhere else. Multiplying this by $e_{ij}$ on the left takes the $j$th component of this column, $a_{jk}$, and places it in the $i$th row of the product, with zeros everywhere else. Therefore we have only $a_{jk}$ in the $(i, \ell)$ entry, or $a_{jk}e_{i\ell}$.

## Exercises from 1st edition

**1.1.16** A square matrix $A$ is called *nilpotent* if $A^k = 0$ for some $k > 0$. Prove that if $A$ is nilpotent then $I + A$ is invertible.

### Discussion

If $I + A$ is invertible then its inverse is some matrix $(I + A)^{-1}$. If we consider this a function of $A$ then we find that it is infinitely differentiable and we might attempt to evaluate its Maclaurin series. Note the resemblance to a geometric series:

$$f(A) = (I + A)^{-1} = I - A + A^2 - A^3 + \dots$$

Since $A$ is nilpotent all powers of $A$ from $k$ onwards are 0, so this is really a finite sum:

$$(I + A)^{-1} = I - A + A^2 - \dots (-1)^{k-1}A^{k-1}$$

We'll assume Artin meant that $k$ is the *lowest* integer such that $A^k = \mathbf{0}$.

**Proof**

We check if it inverts $I + A$, and indeed it does:

$$\begin{aligned}
&(I + A)(I - A + A^2 - \dots (-1)^{k-1}A^{k-1}) \\
&= \left(I(I - A + A^2 - \dots (-1)^{k-1}A^{k-1})\right) + \left(A(I - A + A^2 - \dots (-1)^{k-1}A^{k-1})\right). \\
&= I + A - A + A^2 - A^2 + \dots (-1)^{k-1}A^{k-1} + (-1)^{k-2}A^{k-1} + 0 \\
&= I
\end{aligned}$$

which confirms that $I + A - A^2 + \dots (-1)^{k-1}A^{k-1}$ is indeed the inverse of $I + A$.

# Chapter 2

## 2 Section 1

1. Let $S$ be a set. Prove that the law of composition defined by $ab = a$ for all $a, b$ in $S$ is associative.

   **Solution: use algebra to demonstrate order of groupings doesn't matter** We'll show that $a \circ (b \circ c) = (a \circ b) \circ c$. For any $a, b, c \in S$, the composition $a \circ (b \circ c) = a \circ b = a$. Also $(a \circ b) \circ c = a \circ c = a$. Therefore this composition is associative.

   Takeaway: projection is associative.

2. . Prove the properties of inverses that are listed near the end of the section.

   The properties are:

   - If an element $a$ has both a left inverse $\ell$ and a right inverse $r$, then the left inverse and the right inverse are equal.

     **Solution: use algebra to show equality**. We'll use algebra to show that $\ell = r$. Given $a\ell = 1$, multiply both sides by $r$. This gives $\ell ar = 1r = r$. Using associativity we have $\ell(ar) = r$. But since $ar = 1$, as $r$ is a right inverse, this simplifies to $\ell = r$.

   - If $a$ is invertible, its inverse is unique. **Solution: assume there are multiple inverses and show they are equal.**

     Suppose $a$ is invertible. This means there exists at least one inverse $a^{-1}$. Let $b, c$ be other, possibly different inverses for $a$. Then

     $$ca = ba \implies caa^{-1} = baa^{-1} \implies c = b$$

     showing that $b = c$.

   - Inverses multiply in the opposite order: $(ab)^{-1} = b^{-1}a^{-1}$.

     **Solution: use algebra to demonstrate the property holds.**

     This requires that $a$ and $b$ individually have inverses. Using associativity:

     $$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$$

   - An element $a$ may have a left inverse or a right inverse, though it is not invertible.

     **Solution: show an example**

- Let $\mathbb{N}$ denote the set $\{1, 2, 3, \ldots\}$, and let $s : \mathbb{N} \to \mathbb{N}$ be the *shift* map function defined by $s(n) = n + 1$. Prove that $s$ has no right inverse, but that it has infinitely many left inverses. **Solution: explore the function's properties and form a proof.**

  Suppose $s$ has a right inverse $t$. Then $t$ must be a function from $\mathbb{N}$ to $\mathbb{N}$ such that $s(t(n)) = n$. We can also write this as $t(n) + 1 = n$. This clearly works if $t(n) = n - 1$. However if $n = 1$ then $n - 1$ is not in the target set $\mathbb{N}$. In this sense $s$ cannot have a right inverse.

  If $s$ has a left inverse then $t(s(n)) = n$ for all $n$. I.e. $t(n + 1) = n$. We can define $t(n) = n - 1$ and since $t$ can never receive a number lower than 2 as input, we don't have the problem before of $t(n)$ mapping out of $\mathbb{N}$. However, $t$ must still be *defined* on the entire set $\mathbb{N}$, so we can map 1 to any natural number we like. For example we could have $t_1$ which maps 1 to 1, $t_{29}$ which maps 1 to 29, etc. In this sense each $t_k$ is a left inverse of $s$ and there are infinitely many different ones, one for each natural number.

# 3 Section 2

2.1 First

2.2 Second

2.3 third

2.4 fourth

2.5 In the definition of a subgroup, the identity element in $H$ is required to be the identity of $G$. One might require only that $H$ have an identity element, not that it need be the same as the identity of $G$. Show that if $H$ has an identity at all, then it is the identity of $G$. Show the analagous statement is true for inverses.

**Solution: isolate the essential difference between the objects then show they must be equal.** Suppose $H \leq G$ and $e$ is the identity of $H$. Then for any $h \in H, eh = he = h$. Now take some $g \in G$ that is not in $H$ (if there is no such $g$ then $H = G$ and $e$ is the identity in $G$, as the group identity is unique). Let $eg = g'$. Perhaps $g \neq g'$ and $e$ is not the identity in $G$. However, using associativity:

$$\begin{tikzcd} & (eh)g \; = & hg \arrow[dd, equal] \\ ehg \arrow[ur, equal] \arrow[dr, equal] & & \\ & (eh)g = (he)g = h(eg) = & hg' \end{tikzcd}$$

shows $hg = hg'$. We apply the cancellation law to get $g = g'$. That means $eg = g$ for any $g \in G$ not in $H$ and $e$ is already the identity for $H$. Therefore $e$ behaves as the identity in $G$ as well, and since group identities are unique, $e$ must be the identity of $G$.

For inverses, suppose $h \in H$ has an inverse $h^{-1}$ in $H$ but a possibly different inverse $j \in G$. Then in $G$, $hh^{-1} = hj$ and by the cancellation law $h^{-1} = j$.