3.1 Invertible matrices.

0. *Assumed background.*

   - What has been covered in Topics 1-2, especially:—
     - ∗ 1.2 *Matrix multiplication.*
     - ∗ 1.3 *Transpose, symmetry and skew-symmetry.*
     - ∗ 2.1 *Systems of linear equations.*

   Abstract. We introduce:—

   - the notion of left inverse and right inverse for a matrix,
   - the concept of invertibility for square matrices, and the notion of inverse for a square matrix,
   - the basic algebraic properties of invertible.

1. **Definition. (Left inverse and right inverse.)**

   Let A be an $(p \times q)$-matrix. (Here we do not assume p, q are equal.)

   (1) *Suppose H is a $(q \times p)$-matrix. Then we say H is a* **left inverse** *of A if and only if the equality $HA = I_q$ holds.*

   (2) *Suppose G is a $(q \times p)$-matrix. Then we say G is a* **right inverse** *of A if and only if the equality $AG = I_p$ holds.*

   Remark.

   (a) H is a left-inverse of A exactly when multiplication to A from the left by H results in I_q.

   (b) G is a right-inverse of A exactly when multiplication to A from the right by G results in I_p.

2. **Example (1). (Left inverse and right inverse.)**

   Suppose $A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix}$, and $B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 1/3 & 0 & 0 \\ 0 & 0 & 0 & 1/4 & 0 \\ 0 & 0 & 0 & 0 & 1/5 \end{bmatrix}$.

   (a) *We want to verify the statement (†):*

   (†) *A has a common left inverse and right inverse, namely B.*

   Just perform the computations: $BA = \cdots = I_5$, $AB = \cdots = I_5$.

   (b) *We want to verify the statement (‡):*

   (‡) *B is the unique left inverse of A, and the unique right inverse of A.*

   i. We want to verify the statement: '*if H is a left inverse of A, then $H = B$.*'
   Suppose H is a left inverse of A. [Ask: Is it true that $H = B$?]
   By assumption, $HA = I_5$.
   We already know that B is a right inverse of A. Then $AB = I_5$.
   We now obtain this chain of equalities (using associativity of matrix multiplication):

   $$H = HI_5 = H(AB) = (HA)B = I_5B = B.$$

   ii. With a similar argument, we also verify this statement: '*If G is a right inverse of A, then $G = B$.*'

3. **Example (2). (Questions of existence and uniqueness for left inverse and right inverse.)**

   Let $A = \begin{bmatrix} 1 & 1 \\ 4 & 3 \\ 3 & 4 \\ 0 & 0 \end{bmatrix}$.

   (a) *For any numbers a, b, define* $X_{a,b} = \begin{bmatrix} -3 & 1 & 0 & a \\ -3 & 0 & 1 & b \end{bmatrix}$.

   We want to verify the statement (♯):

   (♯) *For any numbers a, b, the matrix $H_{a,b}$ is a left inverse of A.*

For any number a, b, we have

$$H_{a,b}A = \begin{bmatrix} -3 & 1 & 0 & a \\ -3 & 0 & 1 & b \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 4 & 3 \\ 3 & 4 \\ 0 & 0 \end{bmatrix} = \cdots\cdots = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2.$$

Hence, by definition, $H_{a,b}$ is a left inverse of A.

Remark. It also follows that there are many left inverses of A: distinct choices of the values of a, b give rise to distinct left inverses of A.

(b) We want to verify the statement ($\flat$):

($\flat$) *A has no right inverse.*

We give a proof-by-contradiction argument:—

Suppose G is a right inverse of A. Then G is a (2×4)-matrix, and $AG = I_4$.

In particular the $(4, 4)$-th entry of AG is 1.

However, since the 4-th row of A is $[\ 0 \quad 0\ ]$, the $(4, 4)$-th entry of AG is 0. So $1 = 0$, which is impossible.

4. **Comments on Example (2).**

Existence and uniqueness of inverse is guaranteed for matrix addition. There is a 'Law of Existence and Uniqueness of additive inverse for matrix addition', which reads:—

'*Suppose A is a $(p \times q)$-matrix.*

Then there is some unique $(p \times q)$ matrix Z, namely $Z = \mathcal{O}_{p\times q}$, such that $A + Z = A$ and $Z + A = A$.'

But the respective questions of existence, uniqueness are highly nontrivial for matrix multiplication. In fact, none of the statements below is true:

(a) *Suppose A is a $(p \times q)$-matrix. Then A has a left inverse.*

(b) *Suppose A is a $(p \times q)$-matrix. Then A has a right inverse.*

(c) *Suppose A is a $(p \times q)$-matrix. Then A has at most one left inverse.*

(d) *Suppose A is a $(p \times q)$-matrix. Then A has at most one right inverse.*

Example (2) has provided a counter-example against Statement (b) and Statement (c).

5. From now on we will be interested only in square matrices when we talk about left inverse and right inverse.

It will transpire (after some work we are about to do) that:—

($\star$) any given square matrix has both left and right inverses, or neither; furthermore,

($\star\star$) given any square matrix, if it has both left and right inverses, these two latter matrices will be the same square matrix, and the only such matrix that will serve as both left and right inverses of the given square matrix.

6. With this in mind, it makes sense to introduce the definition below.

Definition. (Invertibility for square matrix, and matrix inverse.)

Suppose A is a $(p \times p)$-square matrix.

Then we say that A is **invertible** *if and only if there is some $(p \times p)$-square matrix B such that B is both a left inverse and a right inverse of A.*

Such a matrix B is called a **matrix inverse** *of A.*

Remark on terminology.

In the literature, people also use the word '**non-singular**' (or '**nonsingular**') in place of the word '*invertible*', and use the word '**singular**' in place of the phrase '*not invertible*'.

7. We are going to handle ($\star\star$) immediately, and to deduce some basic algebraic properties for the notion of matrix inverse.

The work on ($\star$) will involve the notion of row-operations and row-operation matrices, and will be postponed.

Theorem (1). (Uniqueness of matrix inverse.)

Let A, B, C be $(p \times p)$-square matrices.

(a) *Suppose that B is a left inverse of A, and C is a right inverse of A. Then $B = C$.*

(b) *Suppose that B, C are both matrix inverses of A. Then $B = C$.*

8. **Proof of Theorem (1).**

   Let A, B, C be $(p \times p)$-square matrices.

   (a) Suppose that B is a left inverse of A, and C is a right inverse of A.
   By assumption, $BA = I_p$ and $AC = I_p$ respectively.
   Therefore (by the associativity of matrix multiplication), $B = BI_p = B(AC) = (BA)C = I_pC = C$.

   (b) Suppose both of B, C are matrix inverses of A.
   Then B is a left inverse of A, and C is a right inverse of A.
   By the result in (a), it follows that $B = C$.

   Remarks on terminologies and notations.

   (a) From now on there is no problem using the article *the* in writing the words *the matrix inverse of the invertible matrix blah-blah-blah*.

   (b) For the same reason, it makes sense to label the matrix inverse of an invertible matrix, say, A, with something which involves the symbol 'A'.
   From now on, we denote by A^{-1} the matrix inverse of such an invertible matrix A.

9. **Example (3).**

   (a) The identity matrix I_p is invertible, and a matrix inverse of I_p is the matrix I_p itself.

   (b) The zero $(p \times p)$-square matrix is not invertible.

10. **Example (4). (Diagonal matrices.)**

   Suppose $\alpha_1, \alpha_2, \cdots, \alpha_p$ are numbers, and

$$\mathrm{diag}(\alpha_1, \alpha_2, \cdots, \alpha_p) = \begin{bmatrix} \alpha_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \alpha_3 & \ddots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & \alpha_{p-2} & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \alpha_{p-1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \alpha_p \end{bmatrix}.$$

   Then the $(p \times p)$-square matrix $\mathrm{diag}(\alpha_1, \alpha_2, \cdots, \alpha_p)$ is called the **diagonal matrix with (respective) diagonal entries** $\alpha_1, \alpha_2, \cdots, \alpha_p$.

   We can verify the statements below:—

   (a) *Suppose all of $\alpha_1, \alpha_2, \cdots, \alpha_p$ are non-zero.*
   Then $\mathrm{diag}(\alpha_1, \alpha_2, \cdots, \alpha_p)$ is invertible, with a matrix inverse given by $\mathrm{diag}({\alpha_1}^{-1}, {\alpha_2}^{-1}, \cdots, {\alpha_p}^{-1})$.

   (b) *Suppose some amongst $\alpha_1, \alpha_2, \cdots, \alpha_p$ is zero.*
   Then $\mathrm{diag}(\alpha_1, \alpha_2, \cdots, \alpha_p)$ is not invertible.
   Remark. Work needs to be done for this to be seen. Imitate what has been done in Example (2).

   Hence overall:—

   $\mathrm{diag}(\alpha_1, \alpha_2, \cdots, \alpha_p)$ *is invertible if and only if all of* $\alpha_1, \alpha_2, \cdots, \alpha_p$ *are non-zero.*

11. Example (4) hints at the result below:—

   Theorem (2). (Invertibility of matrix inverse.)

   Let A be a $(p \times p)$-square matrix.

   Suppose A is invertible.

   Then its matrix inverse A^{-1} is invertible, and the matrix inverse of A^{-1} is given by

$$(A^{-1})^{-1} = A.$$

12. **Proof of Theorem (2).**

    Let A be a $(p \times p)$-square matrix.

    Suppose A is invertible.

    [Ask: Is A^{-1} is invertible?]

    By assumption, we have $A^{-1}A = I_p$ and $AA^{-1} = I_p$.

    Then A is respectively a right inverse of A^{-1} and a left inverse of A^{-1}.

    So by definition of invertibility, A^{-1} is invertible, with a matrix inverse given by $(A^{-1})^{-1} = A$.

13. **Theorem (3). (Invertibility of products of invertible matrices.)**

    Let A, B be $(p \times p)$-square matrices.

    Suppose A, B are invertible.

    Then the product AB is invertible with matrix inverse given by

    $$(AB)^{-1} = B^{-1}A^{-1}.$$

14. **Proof of Theorem (3).**

    Let A, B be $(p \times p)$-square matrices.

    Suppose A, B are invertible.

    [Ask: Is AB invertible?]

    By assumption, $A^{-1}A = I_p$ and $AA^{-1} = I_p$. Also„ $B^{-1}B = I_p$ and $BB^{-1} = I_p$.

    Write $C = B^{-1}A^{-1}$.
    We have

    $$C(AB) = (B^{-1}A^{-1})(AB) = B^{-1}[A^{-1}(AB)] = B^{-1}[(A^{-1}A)B] = B^{-1}(I_pB) = B^{-1}B = I_p.$$

    We also have

    $$(AB)C = (AB)(B^{-1}A^{-1}) = \cdots\cdots\cdots = I_p.$$

    Therefore, by the definition of matrix inverse and invertibility, AB is invertible with matrix inverse

    $$C = B^{-1}A^{-1}.$$

15. Applying mathematical induction, we can prove this generalization of Theorem (3):

    Theorem (4). (Corollary to Theorem (3).)

    Let $A_1, A_2, \cdots, A_n$ be $(p \times p)$-square matrices.

    Suppose $A_1, A_2, \cdots, A_n$ are invertible.

    Then the product $A_1A_2 \cdots A_n$ is invertible with matrix inverse given by

    $$(A_1A_2 \cdots A_n)^{-1} = {A_n}^{-1} \cdots {A_2}^{-1}{A_1}^{-1}.$$

16. A special case of Theorem (4) is the result below.

    Theorem (5). (Corollary (2) to Theorem (3).)

    Let A be a $(p \times p)$-square matrix.

    Suppose A is invertible.

    Then, for each positive integer n, the matrix A^n is invertible with matrix inverse given by $(A^n)^{-1} = (A^{-1})^n$.

17. **Notations and conventions on integral powers of invertible square matrices.**

    Because of the validity of Theorem (5), it makes sense to extend the notations for positive integral powers of square matrices to negative integral powers for those square matrices which are invertible.

    Definition. (Non-positive integral powers of invertible square matrices.)

    Suppose A is an invertible $(p \times p)$-square matrix, and m is a non-positive integer.

Then the m**-th power of** A*, which is denoted by* A^m*, is defined to be the square matrix given by:—*

$$A^m = \begin{cases} I_p & \text{if} \quad m = 0 \\ \\ (A^{-1})^{-m} & \text{if} \quad m < 0 \end{cases}$$

18. **Example (5). (Illustrations on integral powers of invertible square matrices.)**

(a) Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$.

It happens that A is invertible, with matrix inverse given by $A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/3 \end{bmatrix}$.

For any integer n, we have $A^n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 3^n \end{bmatrix}$.

(b) Let θ be a real number, and $A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$.

It happens that A is invertible, and with matrix inverse given by $A^{-1} = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix}$.

For any integer n, we have $A^n = \begin{bmatrix} \cos(n\theta) & -\sin(n\theta) \\ \sin(n\theta) & \cos(n\theta) \end{bmatrix}$.

19. **Theorem (6). (Invertibility of transpose of invertible matrix.)**

Let A *be a* $(p \times p)$*-square matrix.*

Suppose A *is invertible.*

Then its transpose A^t *is invertible, and the matrix inverse of* A^t *is given by*

$$(A^t)^{-1} = (A^{-1})^t.$$

20. **Proof of Theorem (6).**

Let A be a $(p \times p)$-square matrix.

Suppose A is invertible.

[Ask: Is A^t is invertible?]

By assumption, we have $A^{-1}A = I_p$ and $AA^{-1} = I_p$.

Since $A^{-1}A = I_p$, we have $A^t(A^{-1})^t = (A^{-1}A)^t = {I_p}^t = I_p$.

Similarly, since $AA^{-1} = I_p$, we have $(A^{-1})^tA^t = \cdots = I_p$.

Then $(A^{-1})^t$ is respectively a right inverse of A^t and a left inverse of A^t.

So by definition of invertibility, A^t is invertible, with a matrix inverse given by $(A^t)^{-1} = (A^{-1})^t$.

21. One reason why we are interested in invertibility and matrix inverse is the result below, about existence and uniqueness questions for systems of linear equations.

Theorem (7).

Let A *be a* $(p \times p)$*-square matrix.*

Suppose A *is invertible.*

Then, for any column vector $\mathbf{b}$ *with* p *entries, the system* $\mathcal{LS}(A, \mathbf{b})$ *has a unique solution, namely* $A^{-1}\mathbf{b}$*.*

In particular, the homogeneous system $\mathcal{LS}(A, \mathbf{0}_p)$ *has a unique solution, namely* $\mathbf{0}_p$*.*

22. **Proof of Theorem (7).**

Let A be a $(p \times p)$-square matrix.

Suppose A is invertible. Then A^{-1} is well-defined as a $(p \times p)$-matrix.

Pick any column vector $\mathbf{b}$ with p entries.

Define $\mathbf{t} = A^{-1}\mathbf{b}$.

- By definition, $\mathbf{t}$ is a column vector with p entries.
  We have $A\mathbf{t} = A(A^{-1}\mathbf{b}) = (AA^{-1})\mathbf{b} = I_p\mathbf{b} = \mathbf{b}$.
  Then $\mathbf{t}$ is a solution of $\mathcal{LS}(A, \mathbf{b})$.
- Suppose $\mathbf{s}$ is also a solution of $\mathcal{LS}(A, \mathbf{b})$. Then $A\mathbf{s} = \mathbf{b}$.
  Then $\mathbf{s} = I_p\mathbf{s} = (A^{-1}A)\mathbf{s} = A^{-1}(A\mathbf{s}) = A^{-1}\mathbf{b} = \mathbf{t}$.
  Therefore $\mathbf{t}$ is the only solution of $\mathcal{LS}(A, \mathbf{b})$.

Note that $\mathbf{0}_p$ is a solution of $\mathcal{LS}(A, \mathbf{0}_p)$. Hence it is the unique solution of $\mathcal{LS}(A, \mathbf{0}_p)$.

23. Various portions of the argument for Theorem (7) can be adapted slight to provide the arguments for the results below (Theorem (8), Theorem (9)), about left inverse and right inverse. Their proofs are left as exercises.

Theorem (8).

Let A be a $(p \times q)$-matrix.

Suppose A has a left inverse.

Then:—

(a) *For any column vector $\mathbf{b}$ with p entries, the system $\mathcal{LS}(A, \mathbf{b})$ has at most one solution.*

(b) *The homogeneous system $\mathcal{LS}(A, \mathbf{0}_p)$ has no non-trivial solution; its only solution is $\mathbf{0}_q$.*

Theorem (9).

Let A be a $(p \times q)$-matrix.

Suppose A has a right inverse.

Then, for any column vector $\mathbf{b}$ with p entries, the system $\mathcal{LS}(A, \mathbf{b})$ is consistent.