Handout 2 for MATH 220 and MATH 323

Notes on Determinants and Inverses of Matrices

Laurence Barker, Mathematics Department, Bilkent University,
version: 20th January 2012.

Warning: These notes are intended as a reference for an introductory course on linear algebra or an introductory course on group theory. Their purpose is to supply some proofs of some important results: the multiplicative property of determinants, the vanishing of the determinant for singular matrices, and the role of determinants in a formula for the inverse of a square matrix. Illustrative numerical examples can be found in textbooks.

For the purposes of our discussion, it can be understood that, for all the matrices under consideration, the entries are complex numbers.

Let us begin with some preliminary comments on matrix multiplication. Recall that, given positive integers r, s, t and an $r \times s$ matrix A and an $s \times t$ matrix B, then the product AB is the $r \times t$ matrix such that, writing $a_{i,j}$ and $b_{j,k}$ and $c_{i,k}$, respectively, for the (i, j) entry of A and the (j, k) entry of B and the (i, k) entry of AB, we have

$$c_{i,k} = \sum_j a_{i,j}\, b_{j,k} \; .$$

Matrix multiplication is associative. We mean to say, given another positive integer u and a $t \times u$ matrix C, then $(AB)C = A(BC)$. So we can write ABC unambiguously.

We define the **transpose** of A, denoted A^T, to be the $s \times t$ matrix A^T such that the (j, i) entry of A^T is equal to the (i, j)-entry of A. It is easy to see that the transpose of a product is the product of the transposes,

$$(AB)^T = B^T A^T \; .$$

Now let A be a square matrix, we mean to say, an $n \times n$ matrix, where n is a positive integer. We say that A is **invertible** or **non-singular** if there exists an $n \times n$ matrix A^{-1} such that $A^{-1} A = I = A A^{-1}$, where I denotes the identity $n \times n$ matrix. In that case, we call A^{-1} the **inverse** of A. The inverse, if it exists, is unique. Indeed, given $n \times n$ matrices B and C such that $BA = I = AC$ then, using the associative property of matrix multiplication, we have $B = BI = BAC = IC = C$. A slightly weaker characterization of the inverse will appear in Corollary 12, below. When no inverse exists, we say that A is **non-invertible** or **singular**. The following two remarks are obvious.

Remark 1: (The inverse of the transpose is the transpose of the inverse.) *Given an invertible $n \times n$ matrix A, then the $n \times n$ matrix A^T is invertible, and $(A^T)^{-1} = (A^{-1})^T$.*

Remark 2: (The inverse of a product is the product of the inverses.) *Given invertible $n \times n$ matrices A and B, then AB is invertible and $(AB)^{-1} = B^{-1}A^{-1}$.*

Given a 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we define the **determinant** of A to be $\det(A) = ad - bc$. If $\det(A) \neq 0$, then A is invertible. Indeed, by direct calculation again, it is easy to check that

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \; .$$

Conversely, by the next exercise, if A is invertible then $\det(A^{-1})\det(A) = \det(A^{-1}A) = \det(I) = 1$, hence $\det(A) \neq 0$.

Exercise A: By direct calculation, show that

$$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) = \det\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \det\begin{bmatrix} e & f \\ g & h \end{bmatrix} .$$

Let us write out the definition of the determinant of a 2×2 matrix in a different way. As a briefer notation, we sometimes write the determinant of a 2×2 matrix A as $|A| = \det(A)$. The defining formula for the determinant is

$$\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1} .$$

Now let A be a 3×3 matrix. Write $a_{i,j}$ for the (i, j) entry of A. We define the **determinant** of A, denoted $\det(A)$ or $|A|$, to be

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = a_{1,1}\begin{vmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{vmatrix} - a_{1,2}\begin{vmatrix} a_{2,1} & a_{2,3} \\ a_{3,1} & a_{3,3} \end{vmatrix} + a_{1,3}\begin{vmatrix} a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \end{vmatrix}$$

$$= a_{1,1}\,a_{2,2}\,a_{3,3} - a_{1,1}\,a_{2,3}\,a_{3,2} - a_{1,2}\,a_{2,1}\,a_{3,3} + a_{1,2}\,a_{2,3}\,a_{3,1} + a_{1,3}\,a_{2,1}\,a_{3,2} - a_{1,3}\,a_{2,2}\,a_{3,1} .$$

Before defining the determinant of an $n \times n$ matrix for an arbitrary positive integer n, we need to introduce the notion of a permutation.

Consider a set X. We define a **permutation** of X to be a bijection from X to X, we mean to say, an invertible function from X to X. Given permutations ρ and σ of X, we write $\rho\sigma$ to denote the composite of ρ and σ. Thus, $\rho\sigma$ is the permutation of X such that $(\rho\sigma)(x) = \rho(\sigma(x))$ for $x \in X$. We write $\mathrm{Sym}(X)$ to denote the set of permutations on X. Usually, we call $\rho\sigma$ the **product** of ρ and σ. We think of $\mathrm{Sym}(X)$ as a set equipped with an operation, called **multiplication**, which sends a pair of elements ρ and σ of $\mathrm{Sym}(X)$ to the element $\rho\sigma$ of X.

Our concern will be with the case where X is replaced by the set $\mathbb{Z}_n^+ = \{1, 2, ..., n-1, n\}$ of positive integers less than or equal to n. We write $S_n = \mathrm{Sym}(\mathbb{Z}_n^+)$. Note that $|S_n| = n!$. Let us introduce a convenient notation for representing elements of S_n. Given mutually distinct elements i_1, i_2, ..., i_{r-1}, i_r of $\mathbb{Z}_n^+$, we write $(i_1, i_2, ..., i_r)$ to denote the element of S_n such that, given $k \in \mathbb{Z}_n^r$, then

$$(i_1, ..., i_n)(k) = \begin{cases} i_{t+1} & \text{if } k = i_t \text{ for some } 1 \leq t < r, \\ i_1 & \text{if } k = i_r, \\ k & \text{otherwise.} \end{cases}$$

The permutation $(i_1, ..., i_r)$ is called an r**-cycle**. As an example, putting $n = 2$, we have

$$S_2 = \{1, (1, 2)\}$$

where 1 denotes the identity function on the set $\mathbb{Z}_2^\times = \{1, 2\}$. Putting $n = 3$, we have

$$S_3 = \{1, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\} .$$

The 2-cycles in S_n, called the **transpositions** in S_n, play an especially important role in the theory. These are the elements $(i, j) = (j, i)$ where i and j are distinct elements of $\mathbb{Z}_n^+$. We have $(i,j)(i) = j$ and $(i,j)(j) = (i)$ and $(i,j)(k) = k$ for all the other elements k of $\mathbb{Z}_n^+$. Note that, given a transposition τ in S_n, then $\tau^2 = 1$, in other words, $\tau^{-1} = \tau$.

Two integers are said to have the **same parity** provided they are both even or both odd. They are said to have **opposite parity** provided one of them is even and one of them is odd.

Lemma 3: (Well-definedness of the signature of a permutation.) *For all $n \geq 2$, any element σ of S_n is a product of transpositions. Writing $\sigma = \tau_r ... \tau_1 = \tau'_{r'} ... \tau'_1$ as products of transpositions τ_i and τ'_i, then the integers r and r' have the same parity.*

Proof: For the first part, we argue by induction on n. The case $n = 2$ is clear. Now suppose that $n \geq 3$ and assume that the assertion holds for S_{n-1}. Let $\sigma \in S_{n-1}$. If $\sigma(n) = n$, then we can regard σ as an element of S_{n-1}, hence σ is a product of transpositions. On the other hand, if $\sigma(n) \neq n$ then, introducing the transposition $\tau = (\sigma(n), n)$. and letting $\rho = \tau\sigma$, we have $\rho(n) = n$, hence ρ is a product of transpositions. But $\sigma = \tau\rho$, so σ is a product of transpositions. The first part is established.

Let $\Pi(\sigma) = \{\{u,v\} \subseteq \mathbb{Z}_n^+ : u < v,\ \sigma(u) > \sigma(v)\}$. Let τ be a transposition in S_n, and write $\tau = (i,j)$ with $i < j$. Consider the sets $\{u,v\}$ that belong to exactly one of the sets $\Pi(\sigma)$ or $\Pi(\tau\sigma)$. These are precisely the sets such that

$$\{\{\sigma(u), \sigma(v)\} \in \{(\{i,j\},\ \{i,k\},\ \{k,j\} : i < k < j\}\ .$$

The number of such sets is $2j - 2i - 1$, which is odd. Therefore $|\Pi(\sigma)|$ and $|\Pi(\tau\sigma)|$ have opposite parity. But $|\Pi(1)| = 0$. An inductive argument now shows that if σ is a product of r transpositions, then $|\Pi(\sigma)|$ and r have the same parity. The rider follows. $\square$

For any positive integer n and any element $\sigma \in S_n$, we define

$$\mathrm{sgn}(\sigma) = (-1)^r = \begin{cases} 1 & \text{if } r \text{ is even,} \\ -1 & \text{if } r \text{ is odd.} \end{cases}$$

In the trivial case $n = 1$, the only permutation is the identity function 1, and we understand that $\mathrm{sgn}(1) = 1$. We call $\mathrm{sgn}(\sigma)$ the **signature** of σ. Note that, given elements $\rho, \sigma \in S_n$, then

$$\mathrm{sgn}(\rho\sigma) = \mathrm{sgn}(\rho)\mathrm{sgn}(\sigma)\ .$$

Now let A be an $n \times n$ matrix with (i,j)-entry $a_{i,j}$ for $i, j \in \mathbb{Z}_n^+$. We define the **determinant** of A, denoted $\det(A)$ or $|A|$, to be

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma)\, a_{\sigma(1),1} ... a_{\sigma_n, n}\ .$$

Proposition 4: *With the notation above, suppose that two rows of A are the same, or that two columns of A are the same. That is to say, for some i and j with $i \neq j$, we have $a_{i,k} = a_{j,k}$ for all k, or we have $a_{k,i} = a_{k,j}$ for all k. Then* $\det(A) = 0$.

Proof: Suppose that row i and row j are the same, with $i \neq j$. Consider the transposition $\tau = (i,j)$. We can arrange the elements of S_n in pairs, where elements σ and σ' of S_n are partners provided $\sigma' = \tau\sigma$, or equivalently, $\sigma = \tau\sigma'$. When σ and σ' are partners, we have $\mathrm{sgn}(\sigma) + \mathrm{sgn}(\sigma') = 0$ and

$$a_{\sigma(1),1} ... a_{\sigma(n),n} = a_{\sigma'(1),1} ... a_{\sigma'(n),n}\ .$$

So $\det(A) = 0$. The case where two columns are the same can be dealt with similarly, by pairing σ with $\sigma\tau$, or alternatively, it can be deduced by considering the transpose of A. $\square$

Theorem 5: (Multiplicative property of determinants.) *Let n be a positive integer and let A and B be $n \times n$ matrices. Then* $\det(AB) = \det(A)\det(B)$.

Proof: Let $C = AB$ and let $a_{i,j}$ and $b_{j,k}$ and $c_{i,k}$ denote, respectively, the (i,j) entry of A, the (j,k) entry of B, the (i,k) entry of C. Since $c_{i,k} = \sum_j a_{i,j} b_{j,k}$, we have

$$\det(C) = \sum_{\pi} \operatorname{sgn}(\pi)\, c_{\pi(1),1} ... c_{\pi(n),n} = \sum_{\pi} \operatorname{sgn}(\pi) \big(\sum_{j_1,...,j_n} a_{\pi(1),j_1}\, b_{j_1,1} ... a_{\pi(n),j_n}\, b_{j_n,n} \big)$$

summed over all the elements $\pi \in S_n$ and $j_1, ..., j_n \in \mathbb{Z}_n^+$. Defining

$$\gamma(j_1, ..., j_n) = \sum_{\pi} \operatorname{sgn}(\pi) a_{\pi(1),j_1}\, b_{j_1,1} ... a_{\pi(n),j_n}\, b_{j_n,n}$$

and changing the order of the summation, we have

$$\det(C) = \sum_{j_1,...,j_n} \gamma(j_1, ..., j_n) \ .$$

On the other hand,

$$\det(A)\det(B) = \big(\sum_{\sigma} \operatorname{sgn}(\sigma) a_{\sigma(1),1} ... a_{\sigma(n),n} \big) \big(\sum_{\rho} \operatorname{sgn}(\rho) b_{\rho(1),1} ... b_{\rho(n),n} \big)$$

$$= \sum_{\sigma,\rho} \operatorname{sgn}(\rho\sigma) a_{\sigma(1),1} ... a_{\sigma(n),n}\, b_{\rho(1),1} ... b_{\rho(n),n}$$

summed over all the elements $\sigma, \rho \in S_n$. Changing the order of the multiplication,

$$b_{\rho(1),1} ... b_{\rho(n),n} = b_{\rho\sigma(1),\sigma(1)} ... b_{\rho\sigma(n),\sigma(n)} \ .$$

For each σ, the product $\pi = \rho\sigma$ runs over the elements of S_n as ρ runs over the elements of S_n. Therefore

$$\det(A)\det(B) = \sum_{\sigma,\pi} \operatorname{sgn}(\pi) a_{\pi(1),\sigma(1)}\, b_{\sigma(1),1)} ... a_{\pi(n),\sigma(n)}\, b_{\sigma(n),n)} = \sum_{\sigma} \gamma(\sigma(1), ..., \sigma(n)) \ .$$

It suffices to show that $\gamma(j_1, ..., j_n) = 0$ when the integers j_1, ..., j_n are not mutually distinct. Suppose that $j_u = j_v$ with $u \neq v$. Of course, the assumption implies that $n \geq 2$. Consider the transposition $\tau = (u, v)$. Much as in the previous argument, we can arrange the elements of S_n in pairs, partnering elements π and π' of S_n when $\pi' = \tau\pi$, whence $\operatorname{sgn}(\pi) + \operatorname{sgn}(\pi') = 0$ and $a_{\pi(1),j_1}\, b_{j_1,1} ... a_{\pi(n),j_n}\, b_{j_n,n} = a_{\pi'(1),j_1}\, b_{j_1,1} ... a_{\pi'(n),j_n}\, b_{j_n,n}$. We deduce that $\gamma(j_1, ..., j_n) = 0$, as required. □

Corollary 6: (The determinant of the inverse is the inverse of the determinant.) *Given an invertible $n \times n$ matrix A, then* $\det(A) \neq 0$ *and* $\det(A^{-1}) = (\det(A))^{-1}$.

Proof: We have $\det(A^{-1})\det(A) = \det(A^{-1}A) = \det(I) = 1$. □

Exercise B, for the mathematically inclined: The quaternions are an extension of the complex numbers. They have the form $q = t + ix + jz + ky$ where t, x, y, z are real numbers which uniquely determine q. We define a multiplication operation on the quaternions such that $i^2 = j^2 = k^2 = ijk = -1$ and $qr = rq$ for all real numbers r. Let $\mathbb{H}$ denote the set of quaternions, let $\mathrm{Mat}_2(\mathbb{C})$ denote the set of 2×2 matrices and let ρ be the function $\mathbb{H} \to \mathrm{Mat}_2(\mathbb{C})$ such that

$$\rho(q) = t \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + x \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + y \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + z \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} .$$

(a) Show that $\rho(qq') = \rho(q)\rho(q')$. Deduce that multiplication of quaternions is associative.

(b) Let $N(q) = t^2 + x^2 + y^2 + z^2$. Show that $N(q) = \det(\rho(q))$ and $N(qq') = N(q)N(q')$.

(c) A natural number n is said to be a **sum of four squares** provided $n = t^2 + x^2 + y^2 + z^2$ for some integers t, x, y, z. Using part (b), show that, if natural numbers n and m are sums of four squares, then nm is a sum of four squares. (This conclusion is due to Euler. Subsequently, in 1771, Lagrange made use of this to prove that every natural number is a sum of four squares.)

We define the **permutation matrix** associated with an element $\sigma \in S_n$ to be the $n \times n$ matrix $A(\sigma)$ whose (i, j) entry is 1 when $i = \sigma(j)$ and whose (i, j) entry is zero otherwise. The next two remarks are obvious.

Remark 7: *Given an elements $\rho, \sigma \in S_n$, then $A(\rho)A(\sigma) = A(\rho\sigma)$.*

Remark 8: *Given an element $\sigma \in S_n$, then $\det(A(\sigma)) = \mathrm{sgn}(\sigma)$.*

We shall also need the following technical lemma.

Lemma 9: *Let $\sigma \in \S_n$ and $i, j \in \mathbb{Z}_n^+$ such that $i = \sigma(j)$. Let M be the matrix obtained from $A(\sigma)$ by deleting the i-th row and the j-th column. Then $(-1)^{i+j}\det(M) = \mathrm{sgn}(\sigma)$.*

Proof: As permutations, let $\alpha = (n, n-1, ..., i+1, i)$ and $\beta = (j, j+1, ..., n-1, n)$ and $\pi = \alpha\sigma\beta$. We have $\pi(n) = n$, and the matrix M is obtained from $A(\pi)$ by deleting the n-th row and the n-th column, so we can regard π as an element of S_n with permutation matrix M. Using the latest two remarks and the multiplicative property of determinants

$$\det(M) = \det(A(\pi)) = \det(A(\alpha)A(\beta)A(\gamma))$$

$$= \det(A(\alpha)) \det(A(\sigma) \det(A(\beta)) = \mathrm{sgn}(\alpha) \, \mathrm{sgn}(\sigma) \, \mathrm{sgn}(\beta) \; .$$

But $\alpha = (n, n-1)(n-1, n-2)...(i+1, i)$ as a product of $n-i$ transpositions, so $\det(\alpha) = n-i$. Similarly, $\det(\beta) = n - j$. The required conclusion follows. □

The next result characterizes determinants in a recursive way that is sometimes useful for practical calculation. Let A be an $n \times n$ matrix. Again, we write $a_{i,j}$ for the (i, j) entry of A. Of course, in the case $n = 1$, we have $\det(A) = a_{1,1}$. For $n \geq 2$, we can express $\det(A)$ in terms of the determinants of some $(n-1) \times (n-1)$ matrices. Let $M_{i,j}$ be the $(n-1) \times (n-1)$ matrix obtained from A by deleting the i-th row and the j-th column. Let $A_{i,j} = (-1)^{i+j}\det(M_{i,j})$.

Theorem 10: *With the notation above, let C be the $n \times n$ matrix with (i, j) entry $A_{i,j}$. Then $AC = \det(A)I = CA$. In other words, for all $k \in \mathbb{Z}_n^+$, we have*

$$a_{k,1} \, A_{1,k} + a_{k,2} \, A_{2,k} + ... + a_{k,n} \, A_{n,k} = A_{k,1} \, a_{1,k} + A_{k,2} \, a_{2,k} ... + A_{k,n} \, a_{n,k} = \det(A)$$

and for all $i, j \in \mathbb{Z}_n^+$ with $i \neq j$, we have

$$a_{i,1} \, A_{1,j} + a_{i,2} \, A_{2,j} + ... + a_{i,n} \, A_{n,j} = A_{i,1} \, a_{1,j} + A_{i,2} \, a_{2,j} ... + A_{i,n} \, a_{n,j} = 0 \; .$$

Proof: We have

$$a_{k,1}\,A_{1,k} + a_{k,2}\,A_{2,k} + ... + a_{k,n}\,A_{n,k} = (-1)^{k+1}a_{k,1}\det(M_{k,1}) + ... + (-1)^{k+n}a_{k,n}\det(M_{k,n})$$
$$= \sum_{\sigma} s_k(\sigma)\,a_{1,\sigma(1)}...a_{n,\sigma(n)}$$

where $s_k(\sigma) = \pm 1$ and $s_k(\sigma)$ depends on σ and possibly on k, but not on A. To show that $s_k(\sigma) = \text{sgn}(\sigma)$, we may assume that $A = A(\sigma)$. Writing $k = \sigma(j)$ then, by the latest lemma,

$$s_k(\sigma) = (-1)^{k+j}\det(M_{k,j}) = \text{sgn}(\sigma)\ .$$

We have have now established that

$$a_{k,1}\,A_{1,k} + a_{k,2}\,A_{2,k} + ... + a_{k,n}\,A_{n,k} = \det(A)\ .$$

The other asserted equality for $\det(A)$ holds by a similar argument or, alternatively, it can be deduced by considering the transpose of A.

For all i and j in $\mathbb{Z}_n^+$, we have

$$a_{i,1}\,A_{1,j} + a_{i,2}\,A_{2,j} + ... + a_{i,n}\,A_{n,j} = (-1)^{j+1}a_{i,1}\det(M_{j,1}) + ... + (-1)^{j+n}a_{i,n}\det(M_{j,n})$$

Supposing now that $i \neq j$ then, since each of the matrices appearing in the right-hand expression has been obtained by deleting row j from A, the value of the right-hard expression will not change if we replace row j of A with row i of A. But then, by the previous paragraph, the right-hand expression is the determinant of a matrix whose i-th row and j-th row are the same. Hence, via Proposition 4, $a_{i,1}\,A_{1,j} + ... + a_{i,n}\,A_{n,j} = 0$. The remaining asserted equality can be demonstrated by a similar argument or, alternatively, by considering transposes. □

Corollary 11: *Given a square matrix A, then A is invertible if and only if $\det(A) = 0$. In that case, the (i, j) entry of A^{-1} is, in the notation above, $A_{i,j}/\det(A)$.*

Proof: This follows immediately from Corollary 6 and the latest theorem. □

Corollary 12: *Let A and B be $n \times n$ matrices. Suppose that $AB = I$ or $BA = I$. Then A and B are invertible and $A^{-1} = B$.*

Proof: The hypothesis, combined with the multiplicative property of determinants, implies that $\det(A)\det(B) = \det(I) = 1$. Hence $\det(A) \neq 0$ and A is invertible. The uniqueness property of the inverse now implies that $A^{-1} = B$. □

Recall that the three elementary row operations are: multiplying a row by a non-zero scalar factor, interchanging two rows, adding one row to another row.

Exercise C: Find a method for calculating the determinant of a square matrix based on using elementary row operations to convert the matrix to upper triangular form. (Hint: the determinant of an upper triangular matrix is easy to calculate. Consider the determinants of the matrices representing the three kinds of row operation. Alternative hint: the method can be found in textbooks.)

Comment for mathematics students: All of the above material holds for matrices over an arbitrary field. The set S_n, equipped with the multiplication we imposed, is a group called the **symmetric group of degree** n. The function $\text{sgn} : S_n \to \{\pm 1\}$ is a group homomorphism. The kernel $A_n = \{\sigma \in S_n : \text{sgn}(\sigma) = 1\}$ is called the **alternating group of degree** n**.** The groups S_n and A_n crop up in many different contexts of application.