Solutions to Artin's Algebra, First Ed.

Alec Mouri

This file contains solutions in Micheal Artin's Algebra (First Edition) from Chapter 1 to Chapter 3, Section 4.

These solutions are provided by Alec Mouri on `https://github.com/AMouri/artin-algebra`.

Contents

Chapter 1

Matrix Operations

Exercises

For some reason it is popular to write the solution of the system of equations $AX = B$ in this form, and it is often this form that is called *Cramer's Rule*. However, this expression does not simplify computation. The main thing to remember is expression (5.8) for the inverse of a matrix in terms of its adjoint; the other formulas follow from this expression.

As with the complete expansion of the determinant (4.10), formulas (5.8–5.11) have theoretical as well as practical significance, because the answers A^{-1} and X are exhibited explicitly as quotients of polynomials in the variables $\{a_{ij}, b_i\}$, with integer coefficients. If, for instance, a_{ij} and b_j are all continuous functions of t, so are the solutions x_i.

A general algebraical determinant in its developed form
may be likened to a mixture of liquids seemingly homogeneous,
but which, being of differing boiling points, admit of being separated
by the process of fractional distillation.

James Joseph Sylvester

EXERCISES

1. The Basic Operations

1. What are the entries a_{21} and a_{23} of the matrix $\begin{bmatrix} 1 & 2 & 5 \\ 2 & 7 & 8 \\ 0 & 9 & 4 \end{bmatrix}$?

2. Compute the products AB and BA for the following values of A and B.

   (a) $A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -8 & -4 \\ 9 & 5 \\ -3 & -2 \end{bmatrix}$

   (b) $A = \begin{bmatrix} 1 & 4 \\ 1 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 6 & -4 \\ -3 & 2 \end{bmatrix}$

   (c) $A = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$, $B = [1 \quad 2 \quad 1]$

3. Let $A = (a_1, \ldots, a_n)$ be a row vector, and let $B = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$ be a column vector. Compute the products AB and BA.

4. Verify the associative law for the matrix product

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix}.$$

Notice that this is a self-checking problem. You have to multiply correctly, or it won't come out. If you need more practice in matrix multiplication, use this problem as a model.

5. Compute the product $\begin{bmatrix} 1 & a \\ & 1 \end{bmatrix}\begin{bmatrix} 1 & b \\ & 1 \end{bmatrix}$.

6. Compute $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}^n$.

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

8. Compute the following matrix products by block multiplication:

$$\left[\begin{array}{cc|cc} 1 & 1 & 1 & 5 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right]\left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 3 \end{array}\right], \quad \left[\begin{array}{c|cc} 0 & 1 & 2 \\ \hline 0 & 1 & 0 \\ 3 & 0 & 1 \end{array}\right]\left[\begin{array}{c|cc} 1 & 2 & 3 \\ \hline 4 & 2 & 3 \\ 5 & 0 & 4 \end{array}\right].$$

9. Prove rule (1.20) for block multiplication.

10. Let A, B be square matrices.
    (a) When is $(A + B)(A - B) = A^2 - B^2$?
    (b) Expand $(A + B)^3$.

11. Let D be the diagonal matrix

$$\begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{bmatrix},$$

and let $A = (a_{ij})$ be any $n \times n$ matrix.
    (a) Compute the products DA and AD.
    (b) Compute the product of two diagonal matrices.
    (c) When is a diagonal matrix invertible?

12. An $n \times n$ matrix is called *upper triangular* if $a_{ij} = 0$ whenever $i > j$. Prove that the product of two upper triangular matrices is upper triangular.

13. In each case, find all real 2×2 matrices which commute with the given matrix.
    (a) $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ (c) $\begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}$ (d) $\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$ (e) $\begin{bmatrix} 2 & 3 \\ 0 & 6 \end{bmatrix}$

14. Prove the properties $0 + A = A$, $0A = 0$, and $A0 = 0$ of zero matrices.

15. Prove that a matrix which has a row of zeros is not invertible.

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.

17. (a) Find infinitely many matrices B such that $BA = I_2$ when

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \\ 2 & 5 \end{bmatrix}.$$

    (b) Prove that there is no matrix C such that $AC = I_3$.

18. Write out the proof of Proposition (1.18) carefully, using the associative law to expand the product $(AB)(B^{-1}A^{-1})$.
19. The *trace* of a square matrix is the sum of its diagonal entries:
$$\text{tr } A = a_{11} + a_{22} + \cdots + a_{nn}.$$
(a) Show that $\text{tr } (A + B) = \text{tr } A + \text{tr } B$, and that $\text{tr } AB = \text{tr } BA$.
(b) Show that if B is invertible, then $\text{tr } A = \text{tr } BAB^{-1}$.
20. Show that the equation $AB - BA = I$ has no solutions in $n \times n$ matrices with real entries.

2. Row Reduction

1. (a) For the reduction of the matrix M (2.10) given in the text, determine the elementary matrices corresponding to each operation.
(b) Compute the product P of these elementary matrices and verify that PM is indeed the end result.
2. Find all solutions of the system of equations $AX = B$ when
$$A = \begin{bmatrix} 1 & 2 & 1 & 1 \\ 3 & 0 & 0 & 4 \\ 1 & -4 & -2 & -2 \end{bmatrix}$$
and B has the following value:
$$\text{(a)} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{(b)} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \quad \text{(c)} \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}$$
3. Find all solutions of the equation $x_1 + x_2 + 2x_3 - x_4 = 3$.
4. Determine the elementary matrices which are used in the row reduction in Example (2.22) and verify that their product is A^{-1}.
5. Find inverses of the following matrices:
$$\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}.$$
6. Make a sketch showing the effect of multiplication by the matrix $A = \begin{bmatrix} 2 & -1 \\ 2 & 3 \end{bmatrix}$ on the plane $\mathbb{R}^2$.
7. How much can a matrix be simplified if both row and column operations are allowed?
8. (a) Compute the matrix product $e_{ij}e_{k\ell}$.
(b) Write the identity matrix as a sum of matrix units.
(c) Let A be any $n \times n$ matrix. Compute $e_{ii}Ae_{jj}$.
(d) Compute $e_{ij}A$ and Ae_{ij}.
9. Prove rules (2.7) for the operations of elementary matrices.
10. Let A be a square matrix. Prove that there is a set of elementary matrices $E_1, \ldots, E_k$ such that $E_k \cdots E_1 A$ either is the identity or has its bottom row zero.
11. Prove that every invertible 2×2 matrix is a product of at most four elementary matrices.
12. Prove that if a product AB of $n \times n$ matrices is invertible then so are the factors A, B.
13. A matrix A is called symmetric if $A = A^t$. Prove that for any matrix A, the matrix AA^t is symmetric and that if A is a square matrix then $A + A^t$ is symmetric.

14. **(a)** Prove that $(AB)^t = B^tA^t$ and that $A^{tt} = A$.
(b) Prove that if A is invertible then $(A^{-1})^t = (A^t)^{-1}$.

15. Prove that the inverse of an invertible symmetric matrix is also symmetric.

16. Let A and B be symmetric $n \times n$ matrices. Prove that the product AB is symmetric if and only if $AB = BA$.

17. Let A be an $n \times n$ matrix. Prove that the operator "left multiplication by A" determines A in the following sense: If $AX = BX$ for very column vector X, then $A = B$.

18. Consider an arbitrary system of linear equations $AX = B$ where A and B have real entries.
(a) Prove that if the system of equations $AX = B$ has more than one solution then it has infinitely many.
(b) Prove that if there is a solution in the complex numbers then there is also a real solution.

***19.** Prove that the reduced row echelon form obtained by row reduction of a matrix A is uniquely determined by A.

3. Determinants

1. Evaluate the following determinants:

(a) $\begin{bmatrix} 1 & i \\ 2-i & 3 \end{bmatrix}$ **(b)** $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ **(c)** $\begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$ **(d)** $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 8 & 6 & 3 & 0 \\ 0 & 9 & 7 & 4 \end{bmatrix}$

(e) $\begin{bmatrix} 1 & 4 & 1 & 3 \\ 2 & 3 & 5 & 0 \\ 4 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{bmatrix}$

2. Prove that $\det \begin{bmatrix} 1 & 2 & 5 & 6 \\ 3 & 1 & 7 & 7 \\ 0 & 0 & 2 & 3 \\ 4 & 2 & 1 & 5 \end{bmatrix} = -\det \begin{bmatrix} 2 & 1 & 5 & 1 \\ 1 & 3 & 7 & 0 \\ 0 & 0 & 2 & 1 \\ 2 & 4 & 1 & 4 \end{bmatrix}$.

3. Verify the rule $\det AB = (\det A)(\det B)$ for the matrices $A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 5 & -2 \end{bmatrix}$. Note that this is a self-checking problem. It can be used as a model for practice in computing determinants.

4. Compute the determinant of the following $n \times n$ matrices by induction on n.

(a) $\begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \cdot & & \\ & \cdot & & & \\ \cdot & & & & \\ 1 & & & & \\ 1 & & & & \end{bmatrix}$ **(b)** $\begin{bmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & \\ & -1 & 2 & -1 & \\ & & -1 & \cdot & \\ & & & & 2 \; -1 \\ & & & & -1 \; \; 2 \end{bmatrix}$

5. Evaluate $\det \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 2 & 3 & & \cdot \\ 3 & 3 & 3 & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & & \cdot & \cdot \\ n & \cdots & \cdots & & n \end{bmatrix}$

*6. Compute $\det \begin{bmatrix} 2 & 1 & & & & & & \\ 1 & 2 & 1 & & & & & \\ & 1 & 2 & 1 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix}$.

7. Prove that the determinant is linear in the rows of a matrix, as asserted in (3.6).
8. Let A be an $n \times n$ matrix. What is $\det(-A)$?
9. Prove that $\det A^t = \det A$.
10. Derive the formula $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$ from the properties (3.5, 3.6, 3.7, 3.9).
11. Let A and B be square matrices. Prove that $\det(AB) = \det(BA)$.
12. Prove that $\det \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} = (\det A)(\det D)$, if A and D are square blocks.

*13. Let a $2n \times 2n$ matrix be given in the form $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, where each block is an $n \times n$ matrix. Suppose that A is invertible and that $AC = CA$. Prove that $\det M = \det(AD - CB)$. Give an example to show that this formula need not hold when $AC \neq CA$.

4. Permutation Matrices

1. Consider the permutation p defined by $\mathbf{1} \rightsquigarrow \mathbf{3}$, $\mathbf{2} \rightsquigarrow \mathbf{1}$, $\mathbf{3} \rightsquigarrow \mathbf{4}$, $\mathbf{4} \rightsquigarrow \mathbf{2}$.
   (a) Find the associated permutation matrix P.
   (b) Write p as a product of transpositions and evaluate the corresponding matrix product.
   (c) Compute the sign of p.
2. Prove that every permutation matrix is a product of transpositions.
3. Prove that every matrix with a single 1 in each row and a single 1 in each column, the other entries being zero, is a permutation matrix.
4. Let p be a permutation. Prove that $\operatorname{sign} p = \operatorname{sign} p^{-1}$.
5. Prove that the transpose of a permutation matrix P is its inverse.
6. What is the permutation matrix associated to the permutation $\mathbf{i} \rightsquigarrow \mathbf{n-i}$?
7. (a) The complete expansion for the determinant of a 3×3 matrix consists of six triple products of matrix entries, with sign. Learn which they are.
   (b) Compute the determinant of the following matrices using the complete expansion, and check your work by another method:

$$\begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

8. Prove that the complete expansion (4.12) defines the determinant by verifying rules (3.5–3.7).
9. Prove that formulas (4.11) and (4.12) define the same number.

5. Cramer's Rule

1. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a matrix with determinant 1. What is A^{-1}?
2. (self-checking) Compute the adjoints of the matrices $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix}$, $\begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix}$, and $\begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$, and verify Theorem (5.7) for them.
3. Let A be an $n \times n$ matrix with integer entries a_{ij}. Prove that A^{-1} has integer entries if and only if $\det A = \pm 1$.
4. Prove that expansion by minors on a row of a matrix defines the determinant function.

Miscellaneous Problems

1. Write the matrix $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ as a product of elementary matrices, using as few as you can. Prove that your expression is as short as possible.
2. Find a representation of the complex numbers by real 2×2 matrices which is compatible with addition and multiplication. Begin by finding a nice solution to the matrix equation $A^2 = -I$.
3. (*Vandermonde determinant*) **(a)** Prove that $\det \begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{bmatrix} = (b - a)(c - a)(c - b)$.

   ***(b)** Prove an analogous formula for $n \times n$ matrices by using row operations to clear out the first column cleverly.

***4.** Consider a general system $AX = B$ of m linear equations in n unknowns. If the coefficient matrix A has a left inverse A', a matrix such that $A'A = I_n$, then we may try to solve the system as follows:

$$AX = B$$
$$A'AX = A'B$$
$$X = A'B.$$

But when we try to check our work by running the solution backward, we get into trouble:

$$X = A'B$$
$$AX = AA'B$$
$$AX \stackrel{?}{=} B.$$

We seem to want A' to be a right inverse: $AA' = I_m$, which isn't what was given. Explain. (Hint: Work out some examples.)

5. **(a)** Let A be a real 2×2 matrix, and let A_1, A_2 be the rows of A. Let P be the parallelogram whose vertices are $0, A_1, A_2, A_1 + A_2$. Prove that the area of P is the absolute value of the determinant $\det A$ by comparing the effect of an elementary row operation on the area and on $\det A$.

***(b)** Prove an analogous result for $n \times n$ matrices.

***6.** Most invertible matrices can be written as a product $A = LU$ of a lower triangular matrix L and an upper triangular matrix U, where in addition all diagonal entries of U are 1.

(a) Prove uniqueness, that is, prove that there is at most one way to write A as a product.

(b) Explain how to compute L and U when the matrix A is given.

(c) Show that every invertible matrix can be written as a product LPU, where L, U are as above and P is a permutation matrix.

7. Consider a system of n linear equations in n unknowns: $AX = B$, where A and B have *integer* entries. Prove or disprove the following.

(a) The system has a rational solution if $\det A \neq 0$.

(b) If the system has a rational solution, then it also has an integer solution.

***8.** Let A, B be $m \times n$ and $n \times m$ matrices. Prove that $I_m - AB$ is invertible if and only if $I_n - BA$ is invertible.

1.1 The Basic Operations

(1) $a_{21} = 2, s_{23} = 8$

(2) (a)

$$AB = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} -8 & -4 \\ 9 & 5 \\ -3 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$BA = \begin{bmatrix} -8 & -4 \\ 9 & 5 \\ -3 & -2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{bmatrix} = \begin{bmatrix} -20 & -28 & -28 \\ 24 & 33 & 33 \\ -9 & -12 & -11 \end{bmatrix}$$

(b)

$$AB = \begin{bmatrix} 1 & 4 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 6 & -4 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} -6 & -4 \\ 0 & 0 \end{bmatrix}$$

$$BA = \begin{bmatrix} 6 & -4 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 16 \\ -1 & -8 \end{bmatrix}$$

(c)

$$AB = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ -1 & -2 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \end{bmatrix}$$

(3)

$$AB = \begin{bmatrix} a_1 & \dots & a_n \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 b_1 + ... + a_n b_n \end{bmatrix}$$

$$BA = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \begin{bmatrix} a_1 & \dots & a_n \end{bmatrix} = \begin{bmatrix} a_1 b_1 & a_2 b_1 & \dots & a_n b_1 \\ a_1 b_2 & a_2 b_2 & \dots & a_n b_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1 b_n & a_2 b_n & \dots & a_n b_n \end{bmatrix}$$

(4)

$$\left(\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix} \right) \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 8 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 38 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix} \right) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 10 \\ 14 \end{bmatrix} = \begin{bmatrix} 38 \\ 14 \end{bmatrix}$$

(5)
$$\begin{bmatrix} 1 & a \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ & 1 \end{bmatrix}$$

(6) I claim that
$$\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ & 1 \end{bmatrix}$$

Let $n = 1$. Then
$$\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$$

So the statement is trivially true for $n = 1$. Suppose the statement is true for $n = k - 1$. Then
$$\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}^{k-1} \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & k-1 \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & k \\ & 1 \end{bmatrix}$$

(7) I claim that
$$\begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n & T_n \\ & 1 & n \\ & & 1 \end{bmatrix}$$

Where $T_n = \sum_{i=1}^{n} i$

Suppose $n = 1$. Then
$$\begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}$$

Since $T_1 = 1$, then the statement is true. Suppose the statement is true for $n = k - 1$. Then
$$\begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}^{k-1} \begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & k-1 & T_{k-1} \\ & 1 & k-1 \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & k-1+1 & T_{k-1}+k-1+1 \\ & 1 & k-1+1 \\ & & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & k & T_k \\ & 1 & k \\ & & 1 \end{bmatrix}$$

(8)
$$\left[\begin{array}{cc|cc} 1 & 1 & 1 & 5 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right] \left[\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 3 \end{array}\right]$$

$$= \left[\begin{array}{c|c} \begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&2\\0&1\end{bmatrix}+\begin{bmatrix}1&5\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&1\end{bmatrix} & \begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&1\end{bmatrix}+\begin{bmatrix}1&5\\0&1\end{bmatrix}\begin{bmatrix}0&1\\1&3\end{bmatrix} \\ \hline \begin{bmatrix}1&0\\0&1\end{bmatrix}\begin{bmatrix}1&2\\0&1\end{bmatrix}+\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1&0\\0&1\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&1\end{bmatrix}+\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}0&1\\1&3\end{bmatrix} \end{array}\right]$$

$$= \left[\begin{array}{c|c} \begin{bmatrix}1&3\\0&1\end{bmatrix}+\begin{bmatrix}1&5\\0&1\end{bmatrix} & \begin{bmatrix}1&1\\0&1\end{bmatrix}+\begin{bmatrix}5&16\\1&3\end{bmatrix} \\ \hline \begin{bmatrix}1&2\\0&1\end{bmatrix}+\begin{bmatrix}0&1\\1&0\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix}+\begin{bmatrix}1&3\\0&1\end{bmatrix} \end{array}\right] = \begin{bmatrix}2&8&6&17\\0&2&1&4\\1&3&2&3\\1&1&0&1\end{bmatrix}$$

$$\left[\begin{array}{c|cc} 0&1&2\\ \hline 0&1&0\\3&0&1\end{array}\right]\left[\begin{array}{c|cc} 1&2&3\\ \hline 4&2&3\\5&0&4\end{array}\right]$$

$$= \left[\begin{array}{c|c} [0]\begin{bmatrix}1\end{bmatrix}+\begin{bmatrix}1&2\end{bmatrix}\begin{bmatrix}4\\5\end{bmatrix} & [0]\begin{bmatrix}2&3\end{bmatrix}+\begin{bmatrix}1&2\end{bmatrix}\begin{bmatrix}2&3\\0&4\end{bmatrix} \\ \hline \begin{bmatrix}0\\3\end{bmatrix}\begin{bmatrix}1\end{bmatrix}+\begin{bmatrix}1&0\\0&1\end{bmatrix}\begin{bmatrix}4\\5\end{bmatrix} & \begin{bmatrix}0\\3\end{bmatrix}\begin{bmatrix}2&3\end{bmatrix}+\begin{bmatrix}1&0\\0&1\end{bmatrix}\begin{bmatrix}2&3\\0&4\end{bmatrix} \end{array}\right]$$

$$= \left[\begin{array}{c|c} \begin{bmatrix}0\end{bmatrix}+\begin{bmatrix}14\end{bmatrix} & \begin{bmatrix}0&0\end{bmatrix}+\begin{bmatrix}2&11\end{bmatrix} \\ \hline \begin{bmatrix}0\\3\end{bmatrix}+\begin{bmatrix}4\\5\end{bmatrix} & \begin{bmatrix}0&0\\6&9\end{bmatrix}+\begin{bmatrix}2&3\\0&4\end{bmatrix} \end{array}\right] = \begin{bmatrix}14&2&11\\4&2&3\\8&6&13\end{bmatrix}$$

(9) Let M be a $m \times n$ matrix and M' be a $n \times p$ matrix where

$$M = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{cccc|cccc} a_{11} & a_{12} & \dots & a_{1i} & b_{11} & b_{12} & \dots & b_{1n-i} \\ a_{21} & a_{22} & \dots & a_{2i} & b_{21} & b_{22} & \dots & b_{2n-i} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{ji} & b_{j1} & b_{j2} & \dots & b_{jn-i} \\ \hline c_{11} & c_{12} & \dots & c_{1i} & d_{11} & d_{12} & \dots & d_{1n-i} \\ c_{21} & c_{22} & \dots & c_{2i} & d_{21} & d_{22} & \dots & d_{2n-i} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m-j1} & c_{m-j2} & \dots & c_{m-ji} & d_{m-j1} & d_{m-j2} & \dots & d_{m-jn-i} \end{array}\right]$$

$$M' = \left[\begin{array}{c|c} A' & B' \\ \hline C' & D' \end{array}\right] = \left[\begin{array}{cccc|cccc} a'_{11} & a'_{12} & \dots & a'_{1x} & b'_{11} & b'_{12} & \dots & b'_{1p-x} \\ a'_{21} & a'_{22} & \dots & a'_{2x} & b'_{21} & b'_{22} & \dots & b'_{2p-x} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a'_{i1} & a'_{i2} & \dots & a'_{ix} & b'_{i1} & b'_{i2} & \dots & b'_{ip-x} \\ \hline c'_{11} & c'_{12} & \dots & c'_{1x} & d'_{11} & d'_{12} & \dots & d'_{1p-x} \\ c'_{21} & c'_{22} & \dots & c'_{2x} & d'_{21} & d'_{22} & \dots & d'_{2p-x} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ c'_{n-i1} & c'_{n-i2} & \dots & c'_{n-ix} & d'_{n-i1} & d'_{n-i2} & \dots & d'_{n-ip-x} \end{array}\right]$$

Then

$$MM' = \begin{bmatrix} \sum_{k=1}^{i} a_{1k}a'_{k1} + \sum_{k=1}^{n-i} b_{1k}c'_{k1} & \dots & \sum_{k=1}^{i} a_{1k}b'_{kp-x} + \sum_{k=1}^{n-i} b_{1k}d'_{kp-x} \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^{i} c_{1k}a'_{k1} + \sum_{k=1}^{n-i} d_{1k}c'_{k1} & \dots & \sum_{k=1}^{i} c_{1k}b'_{kp-x} + \sum_{k=1}^{n-i} d_{1k}d'_{kp-x} \end{bmatrix}$$

$$= \left[\begin{array}{c|c} AA' + AC' & A'B + BD' \\ \hline CA' + DC' & CB' + DD' \end{array}\right]$$

(10) (a)

$$A^2 - B^2 = (A+B)(A-B) = A^2 + BA - AB - B^2 \rightarrow BA = AB$$

(b)

$$(A+B)^3 = (A+B)(A^2 + AB + BA + B^2)$$
$$= A^3 + A^2B + ABA + AB^2 + BA^2 + BAB + B^2A + B^3$$

(11) (a)

$$DA = \begin{bmatrix} d_1a_{11} & d_1a_{12} & \dots & d_1a_{1n} \\ d_2a_{21} & d_2a_{22} & \dots & d_2a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ d_na_{n1} & d_na_{n2} & \vdots & d_na_{nn} \end{bmatrix}$$

$$AD = \begin{bmatrix} d_1a_{11} & d_2a_{12} & \dots & d_na_{1n} \\ d_1a_{21} & d_2a_{22} & \dots & d_na_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ d_1a_{n1} & d_2a_{n2} & \dots & d_na_{nn} \end{bmatrix}$$

(b) Let D, D' be $n \times n$ diagonal matrices with entries d_{ii} and d'_{ii} respectively. Then

$$DD' = \begin{bmatrix} d_{11}d'_{11} & & & \\ & d_{22}d'_{22} & & \\ & & \ddots & \\ & & & d_{nn}d'_{nn} \end{bmatrix}$$

(c) From part (a), each diagonal entry i of either product DA or AD equals d_ia_{ii}. If A is an inverse of D, then each $d_ia_{ii} = 1$, implying each diagonal entry of D must be nonzero.

(12) Let A, B be $n \times n$ upper triangular matrices. Then

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=i}^{j} a_{ik}b_{kj}$$

Since $i > j$, then $(AB)_{ij} = 0$. Therefore, AB is upper triangular.

(13) (a)

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$
$$\rightarrow \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}$$

Thus, a matrix that commutes has the form

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$$

(b)

$$\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix}=\begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}$$

$$\rightarrow \begin{bmatrix}c & d\\0 & 0\end{bmatrix}=\begin{bmatrix}0 & a\\0 & c\end{bmatrix}$$

Thus, a matrix that commutes has the form

$$\begin{bmatrix}0 & a\\0 & 0\end{bmatrix}$$

(c)

$$\begin{bmatrix}2 & 0\\0 & 6\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix}=\begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}2 & 0\\0 & 6\end{bmatrix}$$

$$\rightarrow \begin{bmatrix}2a & 2b\\6c & 6d\end{bmatrix}=\begin{bmatrix}2a & 6b\\2c & 6d\end{bmatrix}$$

Thus, a matrix that commutes has the form

$$\begin{bmatrix}a & 0\\0 & d\end{bmatrix}$$

(d)

$$\begin{bmatrix}1 & 3\\0 & 1\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix}=\begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}1 & 3\\0 & 1\end{bmatrix}$$

$$\rightarrow \begin{bmatrix}a+3c & b+3d\\c & d\end{bmatrix}=\begin{bmatrix}a & 3a+b\\c & 3c+d\end{bmatrix}$$

Thus, a matrix that commutes has the form

$$\begin{bmatrix}a & b\\0 & a\end{bmatrix}$$

(e)

$$\begin{bmatrix}2 & 3\\0 & 6\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix}=\begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}2 & 3\\0 & 6\end{bmatrix}$$

$$\rightarrow \begin{bmatrix}2a+3c & 2b+3d\\6c & 6d\end{bmatrix}=\begin{bmatrix}2a & 3a+6b\\2c & 3c+6d\end{bmatrix}$$

Thus, a matrix that commutes has the form

$$\begin{bmatrix}a & \frac{3}{4}(d-a)\\0 & d\end{bmatrix}$$

(14) Let $A = (a_{ij})$ be an $n \times n$ matrix. Then

$$0 + A = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix} + \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} 0 + a_{11} & \dots & 0 + a_{1n} \\ \vdots & \ddots & \vdots \\ 0 + a_{n1} & \dots & 0 + a_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} = A$$

$$0A = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} 0a_{11} + \ldots + 0a_{n1} & \dots & 0a_{1n} + \ldots + 0a_{nn} \\ \vdots & \ddots & \vdots \\ 0a_{11} + \ldots + 0a_{n1} & \dots & 0a_{1n} + \ldots + 0a_{nn} \end{bmatrix} = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix} = 0$$

$$A0 = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0a_{11} + \ldots + 0a_{1n} & \dots & 0a_{11} + \ldots + 0a_{1n} \\ \vdots & \ddots & \vdots \\ 0a_{n1} + \ldots + 0a_{nn} & \dots & 0a_{n1} + \ldots + 0a_{nn} \end{bmatrix} = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix} = 0$$

(15) Suppose an $n \times n$ A matrix has a row i of zeros. Then for any $n \times n$ matrix B,

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki} = 0$$

So B cannot be an inverse of A, so A is not invertible.

(16) Suppose $k = 1$. Then $A = 0$, so trivially $I + A = I$ is invertible: its inverse is I.
Suppose $k > 1$. Consider $B = I + \sum_{i=1}^{k-1} (-1)^i A^i$. Then

$$(I + A)B = I + \sum_{i=1}^{k-1} \left((-1)^i A^i + (-1)^i A^{i+1} \right)$$

$$= I + (-1)^k A^k + \sum_{i=1}^{k-1} \left((-1)^{i-1} A^i + (-1)^i A^i \right) = I$$

Furthermore,

$$B(I + A) = I + \sum_{i=1}^{k-1} \left((-1)^i A^i + (-1)^i A^{i+1} \right)$$

$$= I + (-1)^k A^k + \sum_{i=1}^{k-1} \left((-1)^{i-1} A^i + (-1)^i A^i\right) = I$$

Thus, $(I + A)^{-1} = B$

(17) (a) Consider the 2×3 matrix B that is a left inverse of A, where

$$B = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$$

Then

$$BA = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 1 & 2 \\ 2 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 2a + b + 2c & 3a + 2b + 5c \\ 2d + e + 2f & 3d + 2e + 5f \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Thus

$$B = \begin{bmatrix} 2 + c & -3 - 4c & c \\ f - 1 & 2 - 4f & f \end{bmatrix}$$

(b) Consider the 2×3 matrix C, where

$$C = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$$

Suppose C is a right inverse of A. Then

$$AC = \begin{bmatrix} 2 & 3 \\ 1 & 2 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$$

$$= \begin{bmatrix} 2a + 3d & 2b + 3e & 2c + 3f \\ a + 2d & b + 2e & c + 2f \\ 2a + 5d & 2a + 5e & 2a + 5f \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

In particular, $a+2d = 2a+5d = 0$ implies that $a = 0$ and $d = 0$. But then $0 = 2a+3d = 1$, a contradiction. Thus C cannot be a right inverse of A.

(18) Assume A, B are invertible. We can then check if $B^{-1}A^{-1}$ is the inverse of AB:

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = A(I)A^{-1} = AA^{-1} = I$$

Similarly,

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

(19) (a) Let $C = A + B$. Then $c_{ij} = a_{ij} + b_{ij}$. So

$$\text{tr } C = \sum_{i=1}^{n} c_{ii} = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = \text{tr } A + \text{tr } B$$

Let $D = AB$ and $E = BA$. Then $d_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$, and $e_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}$. So

$$\text{tr } D = \sum_{i=1}^{n} d_{ii} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki} = \sum_{k=1}^{n}\sum_{i=1}^{n} b_{ki}a_{ik} = \sum_{k=1}^{n} e_{kk} = \text{tr } E$$

(b) Let $C = BA$. Then

$$\text{tr } BAB^{-1} = \text{tr } CB^{-1}\text{tr } B^{-1}C = \text{tr } B^{-1}BA = \text{tr } A$$

(20) Note that tr $I = n$. Furthermore, for any matrix A and a constant c,

$$\text{tr } cA = ca_{11} + ca_{22} + ... + ca_{nn} = c(a_{11} + a_{22} + ... + a_{nn}) = c \cdot \text{tr } A$$

But

$$\text{tr } (AB - BA) = \text{tr } AB + \text{tr } (-1)BA = \text{tr } AB - \text{tr } BA = 0$$

Therefore, $AB - BA \neq I$.

1.2 Row Reduction

(1) (a)

$$E_1 = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, E_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}, E_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix}$$

$$E_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}, E_5 = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

(b)

$$P = E_5E_4E_3E_2E_1$$

$$= \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ -2 & 3 & -1 \\ 1 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 & -1 \\ -2 & 3 & -1 \\ 1 & -2 & 1 \end{bmatrix}$$

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

(2) (a)

$$\left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 3 & 0 & 0 & 4 & 0 \\ 1 & -4 & -2 & -2 & 0 \end{array}\right] \to\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & -6 & -3 & 1 & 0 \\ 0 & -6 & -3 & -3 & 0 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1/2 & -1/6 & 0 \\ 0 & -6 & -3 & -3 & 0 \end{array}\right] \to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1/2 & -1/6 & 0 \\ 0 & 0 & 0 & -4 & 0 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1/2 & -1/6 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \to\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

For arbitrary x_3, then $x_4 = 0, x_2 = -x_3/2, x_1 = 0$.

(b)

$$\left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 3 & 0 & 0 & 4 & 1 \\ 1 & -4 & -2 & -2 & 0 \end{array}\right] \to\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & -6 & -3 & 1 & -2 \\ 0 & -6 & -3 & -3 & -1 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & 1 & 1/2 & -1/6 & 1/3 \\ 0 & -6 & -3 & -3 & -1 \end{array}\right] \to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & 1 & 1/2 & -1/6 & 1/3 \\ 0 & 0 & 0 & -4 & 1 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & 1 & 1/2 & -1/6 & 1/3 \\ 0 & 0 & 0 & 1 & -1/4 \end{array}\right] \to\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 5/4 \\ 0 & 1 & 1/2 & 0 & 7/24 \\ 0 & 0 & 0 & 1 & -1/4 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & 1/2 & 0 & 7/24 \\ 0 & 0 & 0 & 1 & -1/4 \end{array}\right]$$

For arbitrary x_3, $x_4 = -1/4$, $x_2 = 7/24 - x_3/2, x_1 = 2/3$.

(c)

$$\left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 3 & 0 & 0 & 4 & 2 \\ 1 & -4 & -2 & -2 & 2 \end{array}\right] \to\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & -6 & -3 & 1 & 2 \\ 0 & -6 & -3 & -3 & 2 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1/2 & -1/6 & -1/3 \\ 0 & -6 & -3 & -3 & 2 \end{array}\right] \to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1/2 & -1/6 & -1/3 \\ 0 & 0 & 0 & -4 & 0 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 0 \\ 0 & 1 & 1/2 & -1/6 & -1/3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \to\to \left[\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1/2 & 0 & -1/3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

$$\to \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 2/3 \\ 0 & 1 & 1/2 & 0 & -1/3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

For arbitrary x_3, $x_4 = 0$, $x_2 = -1/3 - x_3/2, x_1 = 2/3$.

(3) For arbitrary x_2, x_3, x_4, $x_1 = 3 - x_2 - 2x_3 + x_4$

(4)

$$E_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}, E_2 = \begin{bmatrix} 1 & -4 \\ 0 & 1 \end{bmatrix}, E_3 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

$$A^{-1} = E_3E_2E_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 5 & -4 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & -4 \\ -6 & 5 \end{bmatrix}$$

(5)

$$A = \begin{bmatrix} 1 & \\ & 2 \end{bmatrix} \to \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \Rightarrow A^{-1} = \begin{bmatrix} 1 & \\ & 1/2 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \to \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \Rightarrow B^{-1} = \begin{bmatrix} 1 & -1 \\ & 1 \end{bmatrix}$$

$$C = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \to \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \Rightarrow C^{-1} = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$$

$$D = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 5/3 \\ 1 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 5/3 \\ & 1/3 \end{bmatrix} \to \begin{bmatrix} 1 & 5/3 \\ & 1 \end{bmatrix} \to \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

$$D^{-1} = \begin{bmatrix} 1 & -5/3 \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & 3 \end{bmatrix} \begin{bmatrix} 1 & \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1/3 & \\ & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -5/3 \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & 3 \end{bmatrix} \begin{bmatrix} 1/3 & \\ -1/3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -5/3 \\ & 1 \end{bmatrix} \begin{bmatrix} 1/3 & \\ -1 & 3 \end{bmatrix}$$

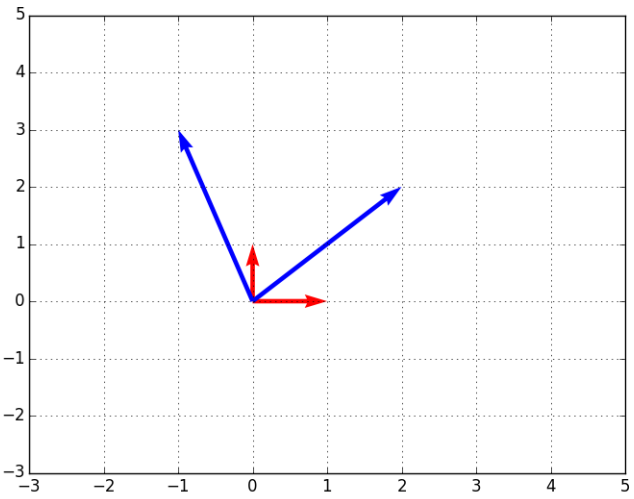
$$= \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}$$

$$E = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = BCD$$

$$(BCD)^{-1} = D^{-1}C^{-1}B^{-1} = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \begin{bmatrix} 1 & -1 \\ & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \begin{bmatrix} & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -5 & 7 \\ 3 & -4 \end{bmatrix}$$

(6) $Ae_1 = \begin{bmatrix} 2 & 2 \end{bmatrix}^\top, Ae_2 = \begin{bmatrix} -1 & 3 \end{bmatrix}^\top$



(7) Suppose we have a matrix A in row reduced echelon form:

$$A = \left[\begin{array}{c|c} & 1 \\ \hline & \end{array}\begin{array}{c|c} B & \\ \hline D & \end{array}\right]$$

Suppose we can inductively reduce the submatrix D with column operations such that all pivots are denoted with a 1, and all other values are 0. Then we use column operations to negate out all values in B. Thus, A can be reduced to a matrix which only has 1's in the locations of the pivots, and all other values are 0.

(8) (a) Let $A = e_{ij}$, $B = e_{k\ell}$, $E = AB$. Then

$$E_{xy} = \sum_{z=1}^{n} A_{xz} B_{zy}$$

Note that if $j = k$, then

$$E_{i\ell} = \sum_{z=1}^{n} A_{iz} B_{z\ell} = A_{ij} B_{k\ell} = 1$$

If $j \neq k$, then $E_{i\ell} = 0$. For all other x, y, then $E_{xy} = 0$.

(b)

$$I = e_{11} + e_{22} + ... + e_{nn} = \sum_{i=1}^{n} e_{ii}$$

(c) Denote $A^{(k)}$ the $n \times n$ matrix where for each i, $A^{(k)}_{ik} = A_{ik}$, and $A^{(k)}_{ij} = A_{ij}$ for $j \neq k$. Then

$$e_{ii} A e_{jj} = e_{ii} A^{(j)} = A_{ij} e_{ii}$$

(d) Denote $B = e_{ij}A$. If $a = i$, then for all b, $B_{ab} = A_{jb}$. Otherwise, $B_{ab} = 0$.
Denote $C = Ae_{ij}$. If $b = j$, then for all a, $C_{ab} = A_{ai}$. Otherwise, $C_{ab} = 0$.

(9) Let X be an arbitrary matrix. Let $E_1 = I + ae_{ij}$ be a type (i) matrix. Then

$$E_1X = (I + ae_{ij}X) = X + ae_{ij}X$$

Then, if $x = i$, then for all y, $(E_1X)_{xy} = X_{iy} + aX_{jy}$, ie. scaling row j by a and adding it to row i. If $x \neq i$, then for all y, $(E_1X)_{xy} = X_{xy}$.

Let $E_2 = I + e_{ij} + e_{ji} - e_{ii} - e_{jj}$ be a type (ii) matrix. Then

$$E_2X = (I + e_{ij} + e_{ji} - e_{ii} - e_{jj})X = X + e_{ij}X + e_{ji}X - e_{ii}X - e_{jj}X$$

Then, if $x = i$, then for all y, $(E_2X)_{xy} = X_{iy} + X_{jy} - X_{iy} = X_{jy}$. If $x = j$, then for all y, $(E_2X)_{xy} = X_{jy} + X_{iy} - X_{jy} = X_{iy}$. Otherwise, $(E_2X)_{xy} = X_{xy}$. Ie. rows i and j are interchanged.

Let $E_3 = I + (c-1)e_{ii}$ be a type (iii) matrix. Then

$$E_3X = (I + (c-1)e_{ii})X = X + (c-1)e_{ii}X$$

Then, if $x = i$, then for all y, $(E_3X)_{xy} = X_{iy} + (c-1)X_{iy} = cX_{iy}$. Otherwise, $(E_3X)_{xy} = X_{xy}$. Ie. row i is multiplied by c.

(10) Let A' be the row reduced echelon form of A. Then there exists a set of elementary matrices $E_1, ..., E_K$ such that $E_k...E_1A = A'$. If every row of A' contains a pivot, then each $A'_{ii} = 1$, and for $i \neq j$, $A'_{ij} = 0$, ie. A' is the identity. Suppose some row i of A' does not contain a pivot. Then every row $\geq i$ also does not contain a pivot, and in particular each such row is a row of zeros. Therefore, A' has its bottom row zero.

(11) Consider the 2×2 matrix A, where

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Note that if $a = c = 0$, then A is not invertible. If $c = 0$, note that $d \neq 0$ (otherwise A is not invertible). Then

$$\begin{bmatrix} a & b \\ & d \end{bmatrix} \to \begin{bmatrix} 1 & b/a \\ & d \end{bmatrix} \to \begin{bmatrix} 1 & b/a \\ & 1 \end{bmatrix} \to \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

If $a = 0$, then $b \neq 0$. Then we can swap rows 1 and 2, and proceed as above (so that 4 operations total are used). If $a \neq 0$ and $c \neq 0$, then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to \begin{bmatrix} 1 & b/a \\ c & d \end{bmatrix} \to \begin{bmatrix} 1 & b/a \\ & d - bc/a \end{bmatrix} \to \begin{bmatrix} 1 & b/a \\ & 1 \end{bmatrix} \to \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

Note with respect to the above operations that if $ad - bc = 0$, then A is not invertible. So, A can be reduced to the identity in 4 operations E_1, E_2, E_3, E_4, where some E_i may be the identity operation. Then $A^{-1} = E_4E_3E_2E_1$, so A^{-1} is a product of at most 4 elementary matrices.

(12) Suppose A is not invertible. Then for some elementary row operations $E_p, E_{p-1}, ..., E_1$, A has reduced echelon form A' such that $E_p...E_1A = A'$, and A' has a bottom row of 0s. Then $AB = (E_p...E_1)^{-1}A'B$, and furthermore $A'B$ also has a bottom row of zeros. Therefore, AB is cannot row reduce to the identity matrix, and therefore AB is not invertible.

Thus, if AB is invertible, then A is invertible. Therefore, for some set of elementary matrices, $A = E_1...E_p$. Thus, $AB = E_1...E_pB \to (AB)E_p^{-1}...E_1^{-1} = B$. Since

$$BE_1...E_p(AB)^{-1} = (AB)E_p^{-1}...E_1^{-1}E_1...E_p(AB)^{-1} = I$$

Then $B^{-1} = E_1...E_p(AB)^{-1}$, so B is invertible.

(13) Let A be a $n \times m$ matrix. Then $A^\top$ is a $m \times n$ matrix, $AA^\top$ is a $n \times n$ matrix, and

$$(AA^\top)_{ij} = \sum_{k=1}^{n} A_{ki}A_{jk}^\top = \sum_{k=1}^{n} A_{ki}A_{kj}$$

Since $(AA^\top)_{ij} = (AA^\top)_{ji}$, then $AA^\top$ is symmetric.

$$(A + A^\top)_{ij} = A_{ij} + A_{ii}^\top = A_{ij} + A_{ji}$$

Since $(A + A^\top)_{ij} = (A + A^\top)_{ji}$, then $A + A^\top$ is symmetric.

(14) (a) Let A be a $n \times m$ matrix and B be a $m \times n$ matrix. Then

$$(B^\top A^\top)_{ij} = \sum_{k=1}^{n} B_{ik}^\top A_{kj}^\top = \sum_{k=1}^{n} B_{ki}A_{jk} = (AB)_{ji} = ((AB)^\top)_{ij}$$

And, $((A^\top)^\top)_{ij} = (A^\top)_{ji} = A_{ij}$.

(b)

$$A^\top(A^{-1})^\top = (A^{-1}A)^\top = I^\top = I$$

Thus, $(A^{-1})^\top = (A^\top)^{-1}$.

(15) If A is symmetric and invertible, then

$$(A^{-1})^\top = (A^\top)^{-1} = A^{-1}$$

Thus A^{-1} is symmetric.

(16) Suppose AB is symmetric. Then

$$AB = (AB)^\top = B^\top A^\top = BA$$

Suppose $AB = BA$. Then

$$(AB)^\top = (BA)^\top = A^\top B^\top = AB$$

Thus AB is symmetric.

(17) Suppose $AX = BX$ for arbitrary X. Then $(A - B)X = 0$. Consider the standard column vectors $e_1, ..., e_n$, where e_i has a 1 in the ith position as its only nonzero entry. For e_i, then for all j, $0 = ((A - B)e_i)_j = (A - B)_{ji} = A_{ji} - B_{ji} \to A_{ji} = B_{ji}$. Thus, $A = B$.

(18) (a) Suppose $AX = B$ has two distinct solutions X_1, X_2. Then $A(X_1 - X_2) = AX_1 - AX_2 = 0$, and for all $c \in \mathbb{R}$, $A(cX_1 - cX_2) = 0$. Thus, $A(X_1 + cX_1 - cX_2) = B \to X_1 + cX_1 - cX_2$ is also a solution. Therefore, $AX = B$ has infinitely many solutions.

(b) Suppose $A = m \times n$ matrix, and let

$$X = \begin{bmatrix} x_1 + y_1 i \\ \vdots \\ x_n + y_n i \end{bmatrix}$$

where at least one $y_i \neq 0$. Then

$$B_j = \sum_{k=1}^{n} A_{jk} X_k = \sum_{k=1}^{n} A_{jk}(x_k + y_k i)$$

Since B_j is real, then

$$\sum_{k=1}^{n} A_{jk} y_k = 0$$

The above equation is satisfied when each $y_k = 0$. Therefore,

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

is also a solution for $AX = B$.

(19) Suppose A is a $m \times 1$ matrix. Then trivially the row reduced echelon form A' of A solely of zeros (if $A = 0$), otherwise A' has a pivot in the first row. Suppose for all $m \times n - 1$ matrices that its corresponding row reduced echelon form is uniquely determined. Suppose now that A is a $m \times n$ matrix, with distinct row reduced echelon forms B and C. Note that $A = [A'|A"], B = [B'|B"]$ and $C = [C'|C"]$, where A', B', C' are $m \times n - 1$ matrices, and $A", B", C"$ are $m \times 1$ matrices. Thus, B', C' are row reduced echelon forms of A', and in particular $B' = C'$. So, $B" \neq C"$: in particular for some i, $B"_i \neq C"_i$. Consider $AX = 0$. Then $BX = CX = 0$. So, we have

$$0 = \sum_{k=1}^{n} B_{ik} X_k = \sum_{k=1}^{n} C_{ik} X_k$$

Since for $1 \leq k \leq n - 1$, $B_{ik} = C_{ik}$, then

$$0 = B_{in} X_n = C_{in} X_n \to (B_{in} - C_{in}) X_n = 0$$

Since $B_{in} \neq C_{in}$, then $X_n = 0$. Therefore, $B"$ and $C"$ must contain a pivot, and since $B' = C'$ the pivot must be in the same location. But then all other entries of $B"$ and $C"$ must be 0. Thus, $B" = C"$, and by contradiction $B = C$.

1.3 Determinants

(1) (a)

$$\det \begin{bmatrix} 1 & i \\ 2-i & 3 \end{bmatrix} = (1)(3) - (i)(2-i) = 3 - 2i + i^2 = 2 - 2i$$

(b)

$$\det \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = (1)(-1) - (1)(1) = -1 - 1 = -2$$

(c)

$$\det \begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix} = 2 \det \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} - 0 \det \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} + 1 \det \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= 2((1)(2) - (0)(0)) + 1((0)(0) - (1)(1)) = 4 - 1 = 3$$

(d)

$$\det \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 8 & 6 & 3 & 0 \\ 0 & 9 & 7 & 4 \end{bmatrix} = \det \begin{bmatrix} 1 & 5 & 8 & 0 \\ 0 & 2 & 6 & 9 \\ 0 & 0 & 3 & 7 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

$$= 1 \det \begin{bmatrix} 2 & 6 & 9 \\ 0 & 3 & 7 \\ 0 & 0 & 4 \end{bmatrix} = 2 \det \begin{bmatrix} 3 & 7 \\ 0 & 4 \end{bmatrix} = 2((3)(4) - (7)(0)) = 24$$

(e)

$$\det \begin{bmatrix} 1 & 4 & 1 & 3 \\ 2 & 3 & 5 & 0 \\ 4 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{bmatrix} = - \det \begin{bmatrix} 3 & 4 & 1 & 1 \\ 0 & 3 & 5 & 2 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 0 & 2 \end{bmatrix} = \det \begin{bmatrix} 3 & 1 & 4 & 1 \\ 0 & 5 & 3 & 2 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

$$= 3 \det \begin{bmatrix} 5 & 3 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 2 \end{bmatrix} = 15 \begin{bmatrix} 1 & 4 \\ 0 & 2 \end{bmatrix} = 15(2 - 0) = 30$$

(2)

$$\det \begin{bmatrix} 1 & 2 & 5 & 6 \\ 3 & 1 & 7 & 7 \\ 0 & 0 & 2 & 3 \\ 4 & 2 & 1 & 5 \end{bmatrix} = - \det \begin{bmatrix} 2 & 1 & 5 & 6 \\ 1 & 3 & 7 & 7 \\ 0 & 0 & 2 & 3 \\ 2 & 4 & 1 & 5 \end{bmatrix}$$

$$= - \det \begin{bmatrix} 2 & 1 & 5 & 6-5 \\ 1 & 3 & 7 & 7-7 \\ 0 & 0 & 2 & 3-2 \\ 2 & 4 & 1 & 5-1 \end{bmatrix} = - \det \begin{bmatrix} 2 & 1 & 5 & 1 \\ 1 & 3 & 7 & 0 \\ 0 & 0 & 2 & 1 \\ 2 & 4 & 1 & 4 \end{bmatrix}$$

(3)

$$\det A = (2)(4) - (1)(3) = 5$$

$$\det B = (1)(-2) - (5)(1) = -7$$

$$\det AB = \det \begin{bmatrix} 17 & -4 \\ 21 & -7 \end{bmatrix} = (17)(-7) - (21)(-4) = -119 + 84 = -35$$

$$\det AB = -35 = (5)(-7) = (\det A)(\det B)$$

(4) (a) Let A be an $n \times n$ matrix, where

$$A = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \end{bmatrix}$$

I claim that $\det A = 1$.

Suppose $n = 1$. Then clearly $\det A = 1$. Suppose for $n = k - 1$, that $\det A = 1$. Then, if $n = k$,

$$A = \left[\begin{array}{c|c} & A' \\ \hline 1 & \end{array}\right]$$

Where A' has dimensions $k - 1 \times k - 1$. Note that $\det A' = 1$, from the inductive hypothesis. Then

$$\det A = 1 \det A' = 1$$

(b) Let A be an $n \times n$ matrix, where

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

I claim that $\det A = n + 1$.

Suppose $n = 1$. Then clearly $\det A = 2$. Suppose for $n = i$, where $i < k$, that $\det A = i + 1$. Then, if $n = k$,

$$A = \left[\begin{array}{c|ccc} 2 & -1 & 0 & \cdots \\ \hline -1 & & & \\ 0 & & A' & \\ \vdots & & & \end{array}\right]$$

Where A' has dimensions $k-1 \times k-1$. In particular,

$$A' = \left[\begin{array}{c|ccc} 2 & -1 & 0 & \cdots \\ \hline -1 & & & \\ 0 & & A\text{"} & \\ \vdots & & & \end{array}\right]$$

Where A" has dimensions $k-2 \times k-2$. Note that $\det A' = k$, and $\det A\text{"} = k-1$, from the inductive hypothesis. Then

$$\det A = 2 \det A' - (-1) \det \left[\begin{array}{c|ccc} -1 & 0 & \cdots & \\ \hline -1 & & & \\ 0 & & A\text{"} & \\ \vdots & & & \end{array}\right]$$

$$= 2k + \det \left[\begin{array}{c|ccc} -1 & -1 & 0 & \cdots \\ \hline 0 & & & \\ 0 & & A\text{"}^\top & \\ \vdots & & & \end{array}\right] = 2k - \det A\text{"}^\top$$

$$= 2k - \det A\text{"} = 2k - (k-1) = k+1$$

(5) Lemma: Let A be a $n \times n$ upper triangular matrix. Then $\det A = a_{11}a_{22}...a_{nn}$. Proof: If A is a 1×1 matrix, then trivially $\det A = a_{11}$. Suppose the statement is true for all $k-1 \times k-1$ matrices. Suppose A is a $k \times k$ matrix, ie.

$$A = \left[\begin{array}{c|c} a_{11} & * \\ \hline & A' \end{array}\right]$$

where A' is a $k-1 \times k-1$ matrix, and $*$ is a $1 \times k-1$ matrix. Then $\det A = a_{11} \det A' = a_{11}a_{22}...a_{nn}$.

Thus, via the Lemma,

$$\det \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 2 & 3 & & \vdots \\ 3 & 3 & 3 & & \vdots \\ \vdots & & & \ddots & \vdots \\ n & \cdots & \cdots & \cdots & n \end{bmatrix} = \det \begin{bmatrix} -1 & 2 & 3 & \cdots & n \\ 0 & 2 & 3 & & \vdots \\ 0 & 3 & 3 & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & n & \cdots & \cdots & n \end{bmatrix}$$

$$= ... = \det \begin{bmatrix} -1 & -1 & -1 & \cdots & -1 & n \\ 0 & -1 & -1 & \cdots & -1 & n \\ 0 & 0 & -1 & \cdots & -1 & n \\ \vdots & & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 & n \end{bmatrix} = (-1)^{n-1} n$$

(6)

$$\det\begin{bmatrix} 2 & 1 & & & & & & \\ 1 & 2 & 1 & & & & & \\ & 1 & 2 & 1 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix} = \frac{1}{2}\det\begin{bmatrix} 2 & 1 & & & & & & \\ 2 & 4 & 2 & & & & & \\ & 1 & 2 & 1 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix}$$

$$= \frac{1}{2}\det\begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & 1 & 2 & 1 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix} = \frac{1}{6}\det\begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & 3 & 6 & 3 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix}$$

$$= \frac{1}{6}\det\begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix} = \frac{1}{24}\det\begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & 4 & 8 & 4 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix}$$

$$= \frac{1}{24}\det\begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & 1 & 2 & 1 & & 1 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix} = \frac{1}{120}\det\begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & 5 & 10 & 5 & & 5 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix}$$

$$= \frac{1}{120}\det\begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & & 6 & 5 & & 5 \\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2 \end{bmatrix}$$

$$= \frac{1}{4320} \det \begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & & 6 & 5 & & 5 \\ & & & & 6 & 12 & 6 & \\ & & & & & 1 & 2 & \\ & & & & 6 & & & 12 \end{bmatrix} = \frac{1}{4320} \det \begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & & 6 & 5 & & 5 \\ & & & & & 7 & 6 & -5 \\ & & & & & 1 & 2 & \\ & & & & & -5 & & 7 \end{bmatrix}$$

$$= \frac{1}{5292000} \det \begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & & 6 & 5 & & 5 \\ & & & & & 35 & 30 & -25 \\ & & & & & 35 & 70 & \\ & & & & & -35 & & 49 \end{bmatrix}$$

$$= \frac{1}{5292000} \det \begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & & 6 & 5 & & 5 \\ & & & & & 35 & 30 & -25 \\ & & & & & & 40 & 25 \\ & & & & & & 30 & 24 \end{bmatrix}$$

$$= \frac{1}{63504000} \det \begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & & 6 & 5 & & 5 \\ & & & & & 35 & 30 & -25 \\ & & & & & & 120 & 75 \\ & & & & & & 120 & 96 \end{bmatrix}$$

$$= \frac{1}{63504000} \det \begin{bmatrix} 2 & 1 & & & & & & \\ & 3 & 2 & & & & & \\ & & 4 & 3 & & & & \\ & & & 5 & 4 & & & \\ & & & & 6 & 5 & & 5 \\ & & & & & 35 & 30 & -25 \\ & & & & & & 120 & 75 \\ & & & & & & & 21 \end{bmatrix}$$

From the Lemma of the previous exercise, then we have

$$\frac{1}{63504000}(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 35 \cdot 120 \cdot 21) = 1$$

(7) Suppose A is a 1×1 matrix. Then for an arbitrary 1×1 matrix B, $\det(A+B) = a_{11}+b_{11} = \det A + \det B$. Furthermore, if $C = [ca_{11}]$, then $\det C = ca_{11} = c\det A$.

Suppose for all $n-1\times n-1$ matrices, the determinant operates linearly on rows. Consider the $n\times n$ matrices A, B, C, where for some k, $c_{kj} = a_{kj}+b_{kj}$. Otherwise, if $i\neq k$, $a_{ij} = b_{ij} = c_{ij}$. In particular, $A_{i1} = B_{i1} = C_{i1}$, and by the inductive hypothesis $\det C_{k1} = \det A_{k1} + \det B_{k1}$. Then

$$\det C = \sum_{i=1}^{n}(-1)^{i+1}c_{i1}\det C_{i1}$$

$$= (-1)^{k+1}(a_{k1}+b_{k1})\det A_{k1} + \sum_{i\neq k}(-1)^{i+1}a_{i1}(\det A_{i1} + \det B_{i1})$$

$$= \sum_{i=1}^{n}(-1)^{i+1}a_{i1}\det A_{i1} + \sum_{i=1}^{n}(-1)^{i+1}b_{i1}\det B_{i1} = \det A + \det B$$

Now consider the $n\times n$ matrices A', B', where for some k, $b_{kj} = ca_{kj}$, Otherwise, if $i\neq k$, $a_{ij} = b_{ij}$. In particular, $A_{i1} = B_{i1}$, and by the inductive hypothesis $\det B_{k1} = c\det A_{k1}$. Then

$$\det B = \sum_{i=1}^{n}(-1)^{i+1}b_{i1}\det B_{i1}$$

$$= (-1)^{k+1}ca_{kj}\det A_{k1} + \sum_{i\neq k}(-1)^{i+1}a_{i1}(c\det A_{k1})$$

$$= c\sum_{i=1}^{n}(-1)^{k+1}a_{i1}\det A_{i1} = c\det A$$

(8)

$$\det(-A) = \det\begin{bmatrix}-A_1\\ -A_2\\ \vdots\\ -A_n\end{bmatrix} = (-1)^n\det\begin{bmatrix}A_1\\ A_2\\ \vdots\\ A_n\end{bmatrix} = (-1)^n\det A$$

(9) Lemma: Let E be an elementary matrix. Then $\det E = \det E^\top$. Proof: If $E = I + ae_{ij}$ is an elementary matrix of the first kind, then $E^\top = I + ae_{ji}$. Clearly, $E^\top$ is also an elementary matrix of the first kind, so $\det E = \det E^\top = 1$. If $E = I + e_{ij} + e_{ji} - e_{ii} - e_{jj}$ is an elementary matrix of the second kinda, then $E^\top = I + e_{ji} + e_{ij} - e_{ii} - e_{jj} = E$, so $\det E = \det E^\top$. If $E = I + (c-1)e_{ii}$ is an elementary matrix of the third kind, then $E^\top = I + (c-1)e_{ii} = E$, so $\det E = \det E^\top$.

Suppose A is not invertible. Then $A^\top$ is also not invertible, and therefore $\det A = \det A^\top = 0$.

Suppose A is invertible. Then $A^\top$ is also invertible, and for some elementary matrices $E_1, ..., E_p$, $\det E_p ... \det E_1 \det A = \det A^\top \det E_1^\top ... \det E_p^\top = \det I = 1$. Note that from the Lemma, $\det E_i = \det E_i^\top$. Therefore, $\det A = \det A^\top$.

(10)
$$\det\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \det\begin{bmatrix} a & 0 \\ c & d \end{bmatrix} + \det\begin{bmatrix} 0 & b \\ c & d \end{bmatrix}$$
$$ad\det\begin{bmatrix} 1 & 0 \\ c/d & 1 \end{bmatrix} - \det\begin{bmatrix} c & d \\ 0 & b \end{bmatrix} = ad\det\begin{bmatrix} 1 & 0 \\ c/d & 1 \end{bmatrix} - cb\det\begin{bmatrix} 1 & d/c \\ 0 & 1 \end{bmatrix}$$
$$= ad\left(\det\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \det\begin{bmatrix} 1 & 0 \\ c/d & 0 \end{bmatrix}\right) - bc\left(\det\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \det\begin{bmatrix} 0 & d/c \\ 0 & 1 \end{bmatrix}\right)$$
$$= ad\left(1 + \frac{c}{d}\det\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\right) - bc\left(1 + \frac{d}{c}\det\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\right) = ad - bc$$

(11)
$$\det(AB) = (\det A)(\det B) = (\det B)(\det A) = \det(BA)$$

(12) Suppose A is a 1×1 submatrix. Then trivially
$$\det\begin{bmatrix} A & B \\ 0 & D \end{bmatrix} = (\det A)(\det D)$$
Suppose the statement is true for all $k-1 \times k-1$ submatrices A. Let A' be a $k \times k$ submatrix. Let
$$X = \begin{bmatrix} A' & B' \\ 0 & D' \end{bmatrix}$$
Then
$$\det X = \sum_{i=1}^{k}(-1)^{i+1}a'_{i1}\det X_{i1} = \sum_{i=1}^{k}(-1)^{i+1}a'_{i1}(\det A'_{i1})(\det D)$$
$$= (\det D)\sum_{i=1}^{k}(-1)^{i+1}a'_{i1}(\det A'_{i1}) = (\det D)(\det A')$$

(13) Let
$$X = \begin{bmatrix} I_n & \\ -C & A \end{bmatrix}, Y = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$
Then
$$XY = \begin{bmatrix} A & B \\ -CA + AC & -CB + AD \end{bmatrix} = \begin{bmatrix} A & B \\ & AD - CB \end{bmatrix}$$
Note that $\det X = \det X^\top = \det A$ and $(\det X)(\det Y) = \det XY = (\det A)(\det(AD - CB))$. Thus $\det Y = \det(AD - CB)$.

Let
$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, D = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$
Note that $BC \neq CB$.
$$AD - CB = \begin{bmatrix} 2 & 0 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$
Note that $\det Y = 0$, but $\det(AD - CB) = 1$. Thus the formula does not hold.

1.4 Permutation Matrices

(1) (a)

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

(b) Define the transpositions

$$a : 1 \to 3, 3 \to 1$$

$$b : 2 \to 1, 1 \to 2$$

$$c : 2 \to 4, 4 \to 2$$

Then $cba = 1 \to 3, 2 \to 1, 3 \to 4, 4 \to 2 = p$. Let A, B, C be the matrices corresponding to a, b, c respectively. Then

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Then

$$CBA = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = P$$

(c)

$$\text{sign } p = \det P = (\det C)(\det B)(\det A) = (-1)^3 = -1$$

(2) Consider the $n \times n$ permutation matrix P. P has the form of

$$P = \left[\begin{array}{c|c} I_{n-m} & \\ \hline & P_m \end{array}\right]$$

where P_m is a $m \times m$ permutation matrix. Let $m = 1$. Then $P = I_n$, so P is a product of transpositions (namely, the trivial transposition). Suppose for $m = k-1$, that P is a product of transpositions. Now let $m = k$ and that $P_{kk} = 0$. So for some $i > k$, then $P_{ki} = 1$. Let E be the elementary matrix of the second kind corresponding to interchanging rows i and k. Then

$$P = \left[\begin{array}{c|c} I_{n-k} & \\ \hline & P_k \end{array}\right] = E \left[\begin{array}{c|c} I_{n-k+1} & \\ \hline & P_{k-1} \end{array}\right]$$

By the inductive hypothesis, then P is a product of transpositions.

(3) Let P be a $n \times n$ matrix with a single 1 in each row and column. Suppose for each $i \leq n$, α_i is the location of the 1 in row i in P. Ie. $P_{i,\alpha_i} = 1$, and for all $j \neq \alpha_i$, $P_{i,j} = 0$. Note that $\alpha_1 \neq ... \neq \alpha_n$. Then for some matrix X with rows $X_1, ..., X_n$, then

$$(PX)_{i,j} = \sum_{k=1}^{n} P_{i,k} X_{k,i} = X_{\alpha_i,i} \to PX = \begin{bmatrix} X_{\alpha_1} \\ \vdots \\ X_{\alpha_n} \end{bmatrix}$$

So P permutes the rows of X, thus P is a permutation matrix.

(4) Let P be a permutation matrix. Then $P = E_m...E_1$, where $E_1, ..., E_m$ are transpositions. Note that for each i, $\det E_i = -1$, and therefore $\det E_i^{-1} = -1$. Therefore,

$$\text{sign } p = \det P = \det(E_m...E_1) = (\det E_m)...(\det E_1)$$

$$= (\det E_m^{-1})...(\det E_1^{-1}) = \det(E_1^{-1}...E_m^{-1}) = \det P^{-1} = \text{sign } p^{-1}$$

(5) Lemma: Let E be an elementary matrix of the second kind. Then $E = E^\top = E^{-1}$. Proof: suppose E transposes rows i and j. We can then write $E = I + e_{ij} + e_{ji} - e_{ii} - e_{jj}$. Furthermore, $E^\top = I + e_{ji} + e_{ij} - e_{ii} - e_{jj} = E$, and $E^{-1} = I + e_{ij} + e_{ji} - e_{ii} - e_{jj} = E$.

Suppose P is a permutation matrix. We can write P as a product of transpositions $E_1, ..., E_m$. Ie. $P = E_m...E_1$. Then

$$P^\top = (E_m...E_1)^\top = E_1^\top...E_m^\top = E_1^{-1}...E_m^{-1} = (E_m...E_1)^{-1} = P^{-1}$$

(6)

$$P = \begin{bmatrix} & & & & 1 \\ & & & 1 & \\ & & \iddots & & \\ & 1 & & & \\ 1 & & & & \\ & & & & 1 \end{bmatrix}$$

Let x be a column matrix. Then

$$Px = \begin{bmatrix} & & & 1 & \\ & & 1 & & \\ & \iddots & & & \\ 1 & & & & \\ & & & & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-2} \\ x_{n-1} \\ x_n \end{bmatrix} = \begin{bmatrix} x_{n-1} \\ x_{n-2} \\ \vdots \\ x_2 \\ x_1 \\ x_n \end{bmatrix}$$

(7) (a)

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$$

(b) Complete Expansion:

$$\det \begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix}$$

$$= (1)(4)(1) + (1)(2)(0) + (2)(2)(2)$$

$$-(1)(2)(2) - (1)(2)(1) - (2)(4)(0) = 6$$

$$\det \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix}$$

$$= (4)(1)(1) + (-1)(-2)(1) + (1)(1)(-1)$$

$$-(4)(-2)(-1) - (-1)(1)(1) - (1)(1)(1) = -3$$

$$\det \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = (a)(0)(1) + (b)(1)(1) + (c)(1)(1)$$

$$-(a)(1)(1) - (b)(1)(1) - (c)(0)(1) = c - a$$

Other methods:

$$\det \begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix} = 1((4)(1) - (2)(2)) - 2((1)(1) - (2)(2)) = 6$$

$$\det \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix} = 4((1)(1) - (-1)(-2)) - 1((-1)(1) - (1)(-1))$$

$$+1((-1)(-2) - (1)(1)) = -3$$

$$\det \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = a((0)(1) - (1)(1)) - (1)((b)(1) - (c)(1))$$

$$+(1)((b)(1) - (c)(0)) = -a - b + c + b = c - a$$

(8) Denote

$$D(A) = \sum_{\text{perm } p} (\text{sign } p) a_{1p(1)} ... a_{np(n)}$$

to be the complete expansion of A. Then

$$D(I)(1)...(1) = 1$$

Let A, B, C be $n \times n$ matrices with rows $\alpha_i, \beta_i, \gamma_i$. For some k, $\gamma_k = \alpha_k + \beta_k$, and for all $i \neq k$, $\alpha_i = \beta_i = \gamma_i$. Then

$$D(C) = \sum_{\text{perm } p} (\text{sign } p) c_{1p(1)} ... c_{np(n)}$$

$$= \sum_{\text{perm } p} (\text{sign } p) c_{1p(1)} ... c_{(k-1)p(k-1)} c_{kp(k)} c_{(k+1)p(k+1)} ... c_{np(n)}$$

$$= \sum_{\text{perm } p} (\text{sign } p) c_{1p(1)} ... c_{(k-1)p(k-1)} (a_{kp(k)} + b_{kp(k)}) c_{(k+1)p(k+1)} ... c_{np(n)}$$

$$= \sum_{\text{perm } p} (\text{sign } p) a_{1p(1)} ... a_{np(n)} + \sum_{\text{perm } p} (\text{sign } p) b_{1p(1)} ... b_{np(n)}$$

$$= D(A) + D(B)$$

Now suppose A and B are $n \times n$ matrices with rows α_i, β_i. For some k, $\beta_k = c\alpha_k$, and for all $i \neq k$, $\alpha_i = \beta_i$. Then

$$D(B) = \sum_{\text{perm } p} (\text{sign } p) b_{1p(1)} ... b_{np(n)}$$

$$= \sum_{\text{perm } p} (\text{sign } p) b_{1p(1)} ... b_{(k-1)p(k-1)} b_{kp(k)} b_{(k+1)p(k+1)} ... b_{np(n)}$$

$$= \sum_{\text{perm } p} (\text{sign } p) b_{1p(1)} ... b_{(k-1)p(k-1)} c a_{kp(k)} b_{(k+1)p(k+1)} ... b_{np(n)}$$

$$= c \sum_{\text{perm } p} (\text{sign } p) a_{1p(1)} ... a_{np(n)} = cD(A)$$

Now suppose we have a $n \times n$ matrix where rows k and $k+1$ are equivalent. Let P be the set of all permutations, and let $P_<$ be the set of permutations such that $p(k) < p(k+1)$, and let $P_>$ be the set of permutations such that $p(k) > p(k+1)$. Note that $P = P_< \cup P_>$, and that $P_<$ and $P_>$ are disjoint. Furthermore, for some $p \in P_<$ and $p' \in P_>$ where $p(k) = p'(k+1), p(k+1) = p'(k)$, and for all $i \neq k$, $p(i) = p'(i+1)$, then sign $p = -$sign p'. Then

$$D(A) = \sum_{\text{perm } p} (\text{sign } p) a_{1p(1)} ... a_{np(n)}$$

$$= \sum_{\text{perm } p} (\text{sign } p) a_{1p(1)} ... a_{kp(k)} a_{(k+1)p(k+1)} ... a_{np(n)}$$

$$= \sum_{p \in P_<} (\text{sign } p) a_{1p(1)} ... a_{kp(k)} a_{(k+1)p(k+1)} ... a_{np(n)}$$

$$+ \sum_{p \in P_>} (\text{sign } p) a_{1p(1)} ... a_{kp(k)} a_{(k+1)p(k+1)} ... a_{np(n)}$$

$$= \sum_{p \in P_<} ((\text{sign } p) a_{1p(1)} ... a_{kp(k)} a_{(k+1)p(k+1)} ... a_{np(n)}$$

$$-(\text{sign } p) a_{1p(1)} ... a_{kp(k+1)} a_{(k+1)p(k)} ... a_{np(n)}) = 0$$

(9) Note that sign p = sign p^{-1}. Then

$$\det A = \sum_{\text{perm } p} (\text{sign } p) a_{p(1)1} ... a_{p(n)n}$$

$$= \sum_{\text{perm } p} (\text{sign } p) a_{1p^{-1}(1)} ... a_{np^{-1}(n)} = \sum_{\text{perm } q} (\text{sign } q) a_{1q(1)} ... a_{nq(n)}$$

1.5 Cramer's Rule

(1)

$$A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & d \end{bmatrix}$$

(2)

$$\text{adj } \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix}$$

$$\det \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = (1)(4) - (2)(3) = -2$$

$$\begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}$$

$$\text{adj } \begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix} = \begin{bmatrix} \det \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix} & -\det \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} & \det \begin{bmatrix} 1 & 2 \\ 4 & 2 \end{bmatrix} \\ -\det \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix} & \det \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} & -\det \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} \\ \det \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} & -\det \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} & \det \begin{bmatrix} 1 & 1 \\ 2 & 4 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 3 & -6 \\ -2 & 1 & 2 \\ 4 & -2 & 2 \end{bmatrix}$$

$$\det \begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix} = 1(4-4) - 2(1-4) = 6$$

$$\begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix}\begin{bmatrix} 0 & 3 & -6 \\ -2 & 1 & 2 \\ 4 & -2 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 3 & -6 \\ -2 & 1 & 2 \\ 4 & -2 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{bmatrix}$$

$$\text{adj } \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \det \begin{bmatrix} 1 & -2 \\ -1 & 1 \end{bmatrix} & -\det \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} & \det \begin{bmatrix} -1 & 1 \\ 1 & -2 \end{bmatrix} \\ -\det \begin{bmatrix} 1 & -2 \\ 1 & 1 \end{bmatrix} & \det \begin{bmatrix} 4 & 1 \\ 1 & 1 \end{bmatrix} & -\det \begin{bmatrix} 4 & 1 \\ 1 & -2 \end{bmatrix} \\ \det \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & -\det \begin{bmatrix} 4 & -1 \\ 1 & -1 \end{bmatrix} & \det \begin{bmatrix} 4 & -1 \\ 1 & 1 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 0 & 1 \\ -3 & 3 & 9 \\ -2 & 3 & 5 \end{bmatrix}$$

$$\det \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix} = 4 \det \begin{bmatrix} 1 & -2 \\ -1 & 1 \end{bmatrix} - \det \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} + \det \begin{bmatrix} -1 & 1 \\ 1 & -2 \end{bmatrix}$$

$$= 4(1-2) - (-1+1) + (2-1) = -3$$

$$\begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 \\ -3 & 3 & 9 \\ -2 & 3 & 5 \end{bmatrix} = \begin{bmatrix} -3 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -3 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 0 & 1 \\ -3 & 3 & 9 \\ -2 & 3 & 5 \end{bmatrix} \begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} -3 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -3 \end{bmatrix}$$

$$\text{adj} \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} \det \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} & -\det \begin{bmatrix} b & c \\ 1 & 1 \end{bmatrix} & \det \begin{bmatrix} b & c \\ 0 & 1 \end{bmatrix} \\ -\det \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} & \det \begin{bmatrix} a & c \\ 1 & 1 \end{bmatrix} & -\det \begin{bmatrix} a & c \\ 1 & 1 \end{bmatrix} \\ \det \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} & -\det \begin{bmatrix} a & b \\ 1 & 1 \end{bmatrix} & \det \begin{bmatrix} a & b \\ 1 & 0 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} -1 & c-b & b \\ 0 & a-c & c-a \\ 1 & b-a & -b \end{bmatrix}$$

$$\det \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = a \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} - \begin{bmatrix} b & c \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} b & c \\ 0 & 1 \end{bmatrix}$$

$$= a(0-1) - (b-c) + (b-0) = c-a$$

$$\begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} -1 & c-b & b \\ 0 & a-c & c-a \\ 1 & b-a & -b \end{bmatrix}$$

$$= \begin{bmatrix} c-a & ac-ab+ab-bc+bc-ac & ab+bc-ab-bc \\ -1+1 & c-b+b-a & b-b \\ -1+1 & c-b+a-c+b-a & b+c-a-b \end{bmatrix}$$

$$= \begin{bmatrix} c-a & 0 & 0 \\ 0 & c-a & 0 \\ 0 & 0 & c-a \end{bmatrix}$$

$$\begin{bmatrix} -1 & c-b & b \\ 0 & a-c & c-a \\ 1 & b-a & -b \end{bmatrix} \begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -a+c-b+b & -b+b & -c+c-b+b \\ a-c+c-a & c-a & a-c+c-a \\ a+b-a-b & b-b & c+b-a-b \end{bmatrix} = \begin{bmatrix} c-a & 0 & 0 \\ 0 & c-a & 0 \\ 0 & 0 & c-a \end{bmatrix}$$

(3) Suppose A^{-1} has integer entries. we have that

$$\det(A^{-1}A) = \det I = 1$$

and

$$\det(A^{-1}A) = \det A^{-1} \det A$$

Since A has integer entries, then $\det A$ and $\det A^{-1}$ are also integers. So, we have $\det A = \frac{1}{\det A^{-1}}$, and therefore $\det A^{-1} = \pm 1$.

Suppose $\det A = \pm 1$. Then $A^{-1} = \frac{1}{\det A}\text{adj } A = \pm\text{adj } A$. Since $\pm\text{adj}_{ij} = \pm(-1)^{ij} \det A_{ji}$ is composed from the multiplication and addition of integers, then $\pm$adj A has entirely integer entries. Therefore, A^{-1} has entirely integer entries.

(4)

$$\det A = \det A^{\top} = \sum_{i=1}^{n} a_{1i} \det A_{1i}^{\top} = \sum_{i=1}^{n} a_{1i} \det A_{1i}$$

1.6 Miscellaneous Problems

(1)

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \to \begin{bmatrix} 1 & 2 \\ 0 & -2 \end{bmatrix} \to \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\to A = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

We must now show that there does not exist a pair of elementary matrices E_1, E_2 such that $A = E_1E_2$, or equivalently $E_1^{-1}A = E_2$. Let E be the set of all elementary matrices. We will proceed by brute force: suppose

$$E_1 = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \to E_1^{-1} = \begin{bmatrix} 1 & -c \\ 0 & 1 \end{bmatrix}$$

where $c \neq 0$. Then

$$E_1^{-1}A = \begin{bmatrix} 1 & -c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1-3c & 2-4c \\ 3 & 4 \end{bmatrix} \notin E$$

Suppose

$$E_1 = \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \to E_1^{-1} = \begin{bmatrix} 1 & 0 \\ -c & 1 \end{bmatrix}$$

where $c \neq 0$. Then

$$E_1^{-1}A = \begin{bmatrix} 1 & 0 \\ -c & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3-c & 4-2c \end{bmatrix} \notin E$$

Suppose

$$E_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \to E_1^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Then

$$E_1^{-1}A = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}3 & 4\\ 1 & 2\end{bmatrix} \notin E$$

Suppose

$$E_1 = \begin{bmatrix}c & 0\\ 0 & 1\end{bmatrix} \to E_1^{-1} = \begin{bmatrix}1/c & 0\\ 0 & 1\end{bmatrix}$$

where $c \neq 0, 1$. Then

$$E_1^{-1}A = \begin{bmatrix}1/c & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}1/c & 2/c\\ 3 & 4\end{bmatrix} \notin E$$

Suppose

$$E_1 = \begin{bmatrix}1 & 0\\ 0 & c\end{bmatrix} \to E_1^{-1} = \begin{bmatrix}c & 0\\ 0 & 1/c\end{bmatrix}$$

where $c \neq 0, 1$. Then

$$E_1^{-1}A = \begin{bmatrix}1 & 0\\ 0 & 1/c\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} = \begin{bmatrix}1 & 2\\ 3/c & 4/c\end{bmatrix} \notin E$$

(2) Let

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

Then

$$A^2 = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} = -I$$

So, the complex number $a + bi$ can be represented by the matrix

$$\begin{bmatrix}a & -b\\ b & a\end{bmatrix}$$

Then, we can add two complex numbers $(a + bi) + (c + di) = (a + c) + (b + d)i$:

$$\begin{bmatrix}a & -b\\ b & a\end{bmatrix} + \begin{bmatrix}c & -d\\ d & c\end{bmatrix} = \begin{bmatrix}a + c & -(b + d)\\ b + d & a + c\end{bmatrix}$$

And we can multiply two complex numbers $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$:

$$\begin{bmatrix}a & -b\\ b & a\end{bmatrix}\begin{bmatrix}c & -d\\ d & c\end{bmatrix} = \begin{bmatrix}ac - bd & -(ad + bc)\\ ad + bc & ac - bd\end{bmatrix}$$

(3) (a)

$$\det\begin{bmatrix}1 & 1 & 1\\ a & b & c\\ a^2 & b^2 & c^2\end{bmatrix} = \det\begin{bmatrix}b & c\\ b^2 & c^2\end{bmatrix} - \det\begin{bmatrix}a & c\\ a^2 & c^2\end{bmatrix} + \det\begin{bmatrix}a & b\\ a^2 & b^2\end{bmatrix}$$

$$= (bc^2 - b^2c) - (ac^2 - a^2c) + (ab^2 - a^2b) = c(bc - b^2 + a^2 - ac) + ab(b - a)$$

$$= c((a - b)(a + b) + c(b - a)) + ab(b - a) = -c(b - a)(a + b - c) + ab(b - a)$$

$$= (b - a)(ab - ac - bc + c^2) = (b - a)(a(b - c) - c(b - c)$$

$$= (b - a)(b - c)(a - c) = (b - a)(c - a)(c - b)$$

(b) Let

$$A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_k \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_k^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & a_3^{k-1} & \cdots & a_k^{k-1} \end{bmatrix}$$

I claim that $\det A = \prod_{i<j}(a_j - a_i)$. Suppose $n = 2$. Then $\det A = (a_2 - a_1)$, so the statement is valid for $n = 2$. Suppose the statement is true for $n = k - 1$. Then for $n = k$,

$$\det A = \det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_k \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_k^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & a_3^{k-1} & \cdots & a_k^{k-1} \end{bmatrix}$$

$$= \det \begin{bmatrix} 0 & 1 - a_2/a_1 & 1 - a_3/a_1 & \cdots & 1 - a_k/a_1 \\ 0 & a_2 - a_2^2/a_1 & a_3 - a_3^2/a_1 & \cdots & a_k - a_k^2/a_1 \\ 0 & a_2^2 - a_2^3/a_1 & a_3^2 - a_3^3/a_1 & \cdots & a_k^2 - a_k^3/a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_2^{k-2} - a_2^{k-1}/a_1 & a_3^{k-2} - a_3^{k-1}/a_1 & \cdots & a_k^{k-2} - a_k^{k-1}/a_1 \\ a_1^{k-1} & a_2^{k-1} & a_3^{k-1} & \cdots & a_k^{k-1} \end{bmatrix}$$

$$= \frac{1}{a_1^{k-1}} \det \begin{bmatrix} 0 & a_1 - a_2 & a_1 - a_3 & \cdots & a_1 - a_k \\ 0 & a_2(a_1 - a_2) & a_3(a_1 - a_3) & \cdots & a_k(a_1 - a_k) \\ 0 & a_2^2(a_1 - a_2) & a_3^2(a_1 - a_3) & \cdots & a_k^2(a_1 - a_k) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_2^{k-2}(a_1 - a_2) & a_3^{k-2}(a_1 - a_3) & \cdots & a_k^{k-2}(a_1 - a_k) \\ a_1^{k-1} & a_2^{k-1} & a_3^{k-1} & \cdots & {}_{k-1} \end{bmatrix}$$

$$= \frac{(a_1 - a_2)(a_1 - a_3)...(a_1 - a_k)}{a_1^{k-1}} \det \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 \\ 0 & a_2 & a_3 & \cdots & a_k \\ 0 & a_2^2 & a_3^2 & \cdots & a_k^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_2^{k-2} & a_3^{k-2} & \cdots & a_k^{k-2} \\ a_1^{k-1} & a_2^{k-1} & a_3^{k-1} & \cdots & a_k^{k-1} \end{bmatrix}$$

$$= (-1)^{k-1}(a_1 - a_2)(a_1 - a_3)...(a_1 - a_k) \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_2 & a_3 & \cdots & a_k \\ a_2^2 & a_3^2 & \cdots & a_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_2^{k-2} & a_3^{k-2} & \cdots & a_k^{k-2} \\ a_2^{k-1} & a_3^{k-1} & \cdots & a_k^{k-1} \end{bmatrix}$$

$$= \prod_{i<j}(a_j - a_i)$$

(4) X need not exist if $m > n$. For instance, let

$$A = \begin{bmatrix} 3 \\ 0 \end{bmatrix}, B = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$$

Then A has a left inverse

$$A' = \begin{bmatrix} \frac{1}{3} & 0 \end{bmatrix}$$

Then

$$X = \begin{bmatrix} \frac{1}{3} & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = [1]$$

But clearly

$$AX = \begin{bmatrix} 3 \\ 0 \end{bmatrix} [1] = \begin{bmatrix} 3 \\ 0 \end{bmatrix} \neq B$$

Note that if $m = n$ and A has a left inverse, then A also has a right inverse, and so the procedure is valid.

(5) (a) Consider $A_1 = (1, 0)$ and $A_2 = (0, 1)$. Then

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

Clearly, $\det A = \text{area } P = 1$. Now consider arbitrary A_1, A_2.

Suppose without loss of generality that $A_1 \mapsto A_1 + cA_2$ for some $c \neq 0$. Since A_1 is translated parallel to $\overline{A_2}$, then the area of the parallelogram remains constant. Accordingly, the operation corresponds to an elementary operation of the first kind, so the determinant remains unchanged.

Suppose $A_1 \mapsto A_2$ and $A_2 \mapsto A_1$. Clearly, the area remains unchanged. Accordingly, the operation corresponds to an elementary operation of the second kind, so the determinant changes by a factor of -1.

Suppose without loss of generality that $A_1 \mapsto cA_1$ for some $c \neq 0$. Let θ be the angle between $\overline{A_1}$ and $\overline{A_2}$. Since $|\sin\theta|$ remains constant, then the area changes by a factor of $|c|$. Accordingly, the operation corresponds to an elementary operation of the third kind, so the determinant changes by a factor of c.

Since we can arrive at any A_1, A_2 by applying a series of these operations to $(1, 0)$ and $(0, 1)$, then $|\det A| = \text{area } P$.

(b) Consider $A_1 = (1, 0, ..., 0)$, $A_2 = (0, 1, 0, ..., 0)$, ..., $A_n = (0, ..., 0, 1)$. Then $A = I_n$. Clearly, $\det A = \text{vol } P = 1$. Now consider arbitrary $A_1, A_2, ..., A_n$.

Suppose without loss of generality that $A_1 \mapsto A_1 + cA_2$ for some $c \neq 0$. Since A_1 is translated parallel to $\overline{A_2}$, then the volume of the parallelepiped remains constant. Accordingly, the operation corresponds to an elementary operation of the first kind, so the determinant remains unchanged.

Suppose withou loss of generality that $A_1 \mapsto A_2$ and $A_2 \mapsto A_1$. Clearly, the area remains unchanged. Accordingly, the operation corresponds to an elementary operation of the second kind, so the determinant changes by a factor of -1.

Suppose without loss of generality that $A_1 \mapsto cA_1$ for some $c \neq 0$. Let θ_i be the angle between $\overline{A_1}$ and $\overline{A_i}$, for $i \neq 1$. Since $|\sin\theta_i|$ remains constant, then the volume changes

by a factor of $|c|$. Accordingly, the operation corresponds to an elementary operation of the third kind, so the determinant changes by a factor of c.

Since we can arrive at any $A_1, A_2, ..., A_n$ by applying a series of these operations to $(1, 0, ..., 0)$, ..., $(0, ..., 0, 1)$, then $|\det A| = \text{vol } P$.

(6) (a) We will proceed by means of induction: suppose A is a 1×1 matrix. Then clearly $A = LU$, where $L = A$ and $U = I_1$, and also L and U are unique. Suppose for all $k-1 \times k-1$ matrices A', there exists unique L' and U' such that $A' = L'U'$. Now consider the $k \times k$ matrix A. We can express A as

$$A = \left[\begin{array}{c|c} A' & a \\ \hline b & c \end{array}\right]$$

where A' has dimensions $k-1 \times k-1$, a has dimensions $k-1 \times 1$, b has dimensions $1 \times k-1$, and c has dimensions 1×1. I claim that if $A = LU$, then L and U are unique. Decomposing L and U into submatrices with the same dimensions as the submatrices of A, we can write

$$A = LU = \left[\begin{array}{c|c} L' & d \\ \hline e & f \end{array}\right]\left[\begin{array}{c|c} U' & g \\ \hline h & i \end{array}\right] = \left[\begin{array}{c|c} L'U' + dh & L'g + di \\ \hline eU' + fh & eg + fi \end{array}\right]$$

$$\left[\begin{array}{c|c} L'U' & L'g \\ \hline eU' & eg + fi \end{array}\right] = \left[\begin{array}{c|c} A' & a \\ \hline b & c \end{array}\right]$$

Note that L' is lower triangular and U' is upper triangular only 1s on its diagonal. Thus by the inductive hypothesis, L' and U' are unique. It now suffices to show that g, e, f, i are unique.

Consider $L'g = a$. Consider the 1st row of a: $a_1 = L'_1 g = L'_{11} g_1 \to g_1 = \frac{a_1}{L'_{11}}$. Suppose we can uniquely determine g_i for $i < k$. For $i = k$, then $a_k = L'_k g = \sum_{j=1}^{k} L'_{kj} g_j \to g_k = \frac{1}{L'_{kk}}(a_k - \sum_{j=1}^{k-1} L'_{kj} g_j)$

Consider $eU' = b$. Consider the 1st column of b: $b_1 = eU'_1 = e_1 U'_{11} \to e_1 = b_1$. Suppose we can uniquely determine e_i, for $i < k$. For $i = k$, then $b_k = eU'_k = \sum_{j=1}^{k} e_j U'_{jk} \to e_k = b_k - \sum_{j=1}^{k-1} e_j U'_{jk}$.

Consider $eg + fi = c$. Since $U_x = 1$ for all x, then $i = 1$. So, $f = c - eg = c - \sum_{i=1}^{k-1} e_1 g_1$. By the uniqueness of e and g above, f is then unique.

Since we have found unique g, e, f, i, then L and U are unique.

(b) From part (a), then for i, j where $i > j$ we have the following recursive formulae:

$$\ell_{11} = a_{11}$$

$$u_{ii} = 1$$

$$\ell_{ji} = u_{ij} = 0$$

$$\ell_{ij} = a_{ij} - \sum_{k=1}^{j-1} \ell_{ik} u_{kj}$$

$$u_{ji} = \frac{1}{\ell_{jj}} \left(a_{ji} - \sum_{k=1}^{j-1} \ell_{jk} u_{ki} \right)$$

$$\ell_{ii} = a_{ii} - \sum_{k=1}^{i-1} \ell_{ik} u_{ki}$$

Solving these formulae allows us to compute L and U.

(c) Consider the $m \times n$ matrix A. Define A' to be the row-permuted form of A, where there eixsts a series of permutations such that we can transform A' into A" holding these properties:

1. The first nonzero entry in every row is 1. This is a pivot
2. The first nonzero entry of row $i+1$ is to the right of the first nonzero entry of i.

We can use the following procedure to row reduce A into a matrix A':

If $n = 1$, then normalize the matrix using a Type 3 operation.

If $m = 1$, then find the first row containing a nonzero entry, normalize the entry using a Type 3 operation, and clear out the entries below that row using Type 1 operations

Find the first column that contains a nonzero entry. Find the first row in that column that contains a nonzero entry: denote this entry a_{ij}. Normalize this entry using a Type 3 operation. Then clear out the entries in column j below row i using Type 1 operations. Now inductively row reduce A_{ij} to A'_{ij}: ie. row reduce the matrix A without all columns $\leq j$, and row i.

Each Type 1 operation is a lower triangular matrix, and each Type 3 operation is a diagonal matrix. Therefore, letting L be the sequence of Type 1 and Type 3 operations we have performed, we have $LA = A'$. Since $U = A$" $= PA'$ for some permutations P, then we have $PLA = U \to A = L^{-1}P^{-1}U$. It is easy to see that L^{-1} is also a lower triangular matrix (since the inverse of a Type 1 operation that is lower triangular is also lower triangular and the inverse of a Type 3 operation is also diagonal), and the inverse of a permutation matrix is also a permutation matrix. Furthermore, since A is invertible, then every column of A" has a pivot, and we can transform A" into the identity using a series of upper triangular Type 3 operations. Therefore, we have $A = LPU$ for a lower triangular L, a permutation P, and an upper triangular U.

(7) (a) If $\det A \neq 0$, then A is invertible. So, we have

$$X = A^{-1}B$$

Since by Cramer's Rule $A^{-1} = \frac{1}{\det A} \text{adj } A$, and since adj A has integer entries (since each $\det A_{ij}$ is an integer), then A^{-1} has rational entries. Since B also has integer entries, then X has rational entries.

(b) Consider

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

Then necessarily

$$X = \begin{bmatrix} \frac{1}{2} \\ 1 \end{bmatrix}$$

X is a rational solution, but there are no additional solutions, so there is not an additional integer solution.

(8) Suppose $C = I_m - AB$ is invertible. Let $D = I_n - BA$. Consider $E = (I_n + BC^{-1}A)$. Then

$$DE = (I_n - BA)(I_n + BC^{-1}A) = I_n - BA + BC^{-1}A - BABC^{-1}A$$

$$= I_n - BA + B(C^{-1} - ABC^{-1})A = I_n - BA + B((I_m - AB)C^{-1})A$$

$$= I_n - BA + B(CC^{-1})A = I_n - BA + BA = I_n$$

Similarly,

$$ED = (I_n + BC^{-1}A)(I_n - BA) = I_n + BC^{-1}A - BA - BC^{-1}ABA$$

$$= I_n - BA + B(C^{-1} - C^{-1}AB)A = I_n - BA + B(C^{-1}(I_m - AB))A$$

$$= I_n - BA + B(C^{-1}C)A = I_n - BA + BA = I_n$$

Therefore, D is invertible. We can similarly show that if D is invertible, then C is also invertible.

Chapter 2

Groups

Exercises

map $\overline{\varphi}$ which sends the coset $\overline{a} = aN$ to $\varphi(a)$:

$$\overline{\varphi}(\overline{a}) = \varphi(a).$$

This is our fundamental method of identifying quotient groups. For example, the absolute value map $\mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ maps the nonzero complex numbers to the positive real numbers, and its kernel is the unit circle U. So the quotient group $\mathbb{C}^\times/U$ is isomorphic to the multiplicative group of positive real numbers. Or, the determinant is a surjective homomorphism $GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$, whose kernel is the special linear group $SL_n(\mathbb{R})$. So the quotient $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ is isomorphic to $\mathbb{R}^\times$.

Proof of the First Isomorphism Theorem. According to Proposition (5.13), the nonempty fibres of φ are the cosets aN. So we can think of $\overline{G}$ in either way, as the set of cosets or as the set of nonempty fibres of φ. Therefore the map we are looking for is the one defined in (5.10) for any map of sets. It maps $\overline{G}$ bijectively onto the image of φ, which is equal to G' because φ is surjective. By construction it is compatible with multiplication: $\overline{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. □

Es giebt alſo ſehr viel verſchiedene Arten von Größen,
welche ſich nicht wohl herzehlen laßen;
und daher entſtehen die verſchiedene Theile der Mathematic,
deren eine jegliche mit einer beſondern Art von Größen beſchäftiget iſt.

Leonhard Euler

EXERCISES

1. The Definition of a Group

1. **(a)** Verify (1.17) and (1.18) by explicit computation.
(b) Make a multiplication table for S_3.

2. **(a)** Prove that $GL_n(\mathbb{R})$ is a group.
(b) Prove that S_n is a group.

3. Let S be a set with an associative law of composition and with an identity element. Prove that the subset of S consisting of invertible elements is a group.

4. Solve for y, given that $xyz^{-1}w = 1$ in a group.

5. Assume that the equation $xyz = 1$ holds in a group G. Does it follow that $yzx = 1$? That $yxz = 1$?

6. Write out all ways in which one can form a product of four elements a, b, c, d in the given order.

7. Let S be any set. Prove that the law of composition defined by $ab = a$ is associative.

8. Give an example of 2×2 matrices such that $A^{-1}B \neq BA^{-1}$.

9. Show that if $ab = a$ in a group, then $b = 1$, and if $ab = 1$, then $b = a^{-1}$.

10. Let a, b be elements of a group G. Show that the equation $ax = b$ has a unique solution in G.

11. Let G be a group, with multiplicative notation. We define an *opposite group* G^0 with law of composition $a \circ b$ as follows: The underlying set is the same as G, but the law of composition is the opposite; that is, we define $a \circ b = ba$. Prove that this defines a group.

2. Subgroups

1. Determine the elements of the cyclic group generated by the matrix $\begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ explicitly.
2. Let a, b be elements of a group G. Assume that a has order 5 and that $a^3b = ba^3$. Prove that $ab = ba$.
3. Which of the following are subgroups?
   (a) $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$.
   (b) $\{1, -1\} \subset \mathbb{R}^\times$.
   (c) The set of positive integers in $\mathbb{Z}^+$.
   (d) The set of positive reals in $\mathbb{R}^\times$.
   (e) The set of all matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$, in $GL_2(\mathbb{R})$.
4. Prove that a nonempty subset H of a group G is a subgroup if for all $x, y \in H$ the element xy^{-1} is also in H.
5. An nth root of unity is a complex number z such that $z^n = 1$. Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.
6. (a) Find generators and relations analogous to (2.13) for the Klein four group.
   (b) Find all subgroups of the Klein four group.
7. Let a and b be integers.
   (a) Prove that the subset $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$.
   (b) Prove that a and $b + 7a$ generate the subgroup $a\mathbb{Z} + b\mathbb{Z}$.
8. Make a multiplication table for the quaternion group H.
9. Let H be the subgroup generated by two elements a,b of a group G. Prove that if $ab = ba$, then H is an abelian group.
10. (a) Assume that an element x of a group has order rs. Find the order of x^r.
    (b) Assuming that x has arbitrary order n, what is the order of x^r?
11. Prove that in any group the orders of ab and of ba are equal.
12. Describe all groups G which contain no proper subgroup.
13. Prove that every subgroup of a cyclic group is cyclic.
14. Let G be a cyclic group of order n, and let r be an integer dividing n. Prove that G contains exactly one subgroup of order r.
15. (a) In the definition of 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 is the same as the identity in G. Show that if H has an identity at all, then it is the identity in G, so this definition would be equivalent to the one given.
    (b) Show the analogous thing for inverses.
16. (a) Let G be a cyclic group of order 6. How many of its elements generate G?
    (b) Answer the same question for cyclic groups of order 5, 8, and 10.
    (c) How many elements of a cyclic group of order n are generators for that group?
17. Prove that a group in which every element except the identity has order 2 is abelian.
18. According to Chapter 1 (2.18), the elementary matrices generate $GL_n(\mathbb{R})$.
    (a) Prove that the elementary matrices of the first and third types suffice to generate this group.
    (b) The *special linear group* $SL_n(\mathbb{R})$ is the set of real $n \times n$ matrices whose determinant is 1. Show that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

*(c) Use row reduction to prove that the elementary matrices of the first type generate $SL_n(\mathbb{R})$. Do the 2×2 case first.

19. Determine the number of elements of order 2 in the symmetric group S_4.

20. (a) Let a, b be elements of an abelian group of orders m, n respectively. What can you say about the order of their product ab?

*(b) Show by example that the product of elements of finite order in a nonabelian group need not have finite order.

21. Prove that the set of elements of finite order in an abelian group is a subgroup.

22. Prove that the greatest common divisor of a and b, as defined in the text, can be obtained by factoring a and b into primes and collecting the common factors.

3. Isomorphisms

1. Prove that the additive group $\mathbb{R}^+$ of real numbers is isomorphic to the multiplicative group P of positive reals.

2. Prove that the products ab and ba are conjugate elements in a group.

3. Let a, b be elements of a group G, and let $a' = bab^{-1}$. Prove that $a = a'$ if and only if a and b commute.

4. (a) Let $b' = aba^{-1}$. Prove that $b'^n = ab^n a^{-1}$.

(b) Prove that if $aba^{-1} = b^2$, then $a^3ba^{-3} = b^8$.

5. Let $\varphi\colon G \longrightarrow G'$ be an isomorphism of groups. Prove that the inverse function φ^{-1} is also an isomorphism.

6. Let $\varphi\colon G \longrightarrow G'$ be an isomorphism of groups, let $x, y \in G$, and let $x' = \varphi(x)$ and $y' = \varphi(y)$.

(a) Prove that the orders of x and of x' are equal.

(b) Prove that if $xyx = yxy$, then $x'y'x' = y'x'y'$.

(c) Prove that $\varphi(x^{-1}) = x'^{-1}$.

7. Prove that the matrices $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$ are conjugate elements in the group $GL_2(\mathbb{R})$ but that they are not conjugate when regarded as elements of $SL_2(\mathbb{R})$.

8. Prove that the matrices $\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ & 2 \end{bmatrix}$ are conjugate in $GL_2(\mathbb{R})$.

9. Find an isomorphism from a group G to its opposite group G^0 (Section 2, exercise 12).

10. Prove that the map $A \rightsquigarrow (A^t)^{-1}$ is an automorphism of $GL_n(\mathbb{R})$.

11. Prove that the set Aut G of automorphisms of a group G forms a group, the law of composition being composition of functions.

12. Let G be a group, and let $\varphi\colon G \longrightarrow G$ be the map $\varphi(x) = x^{-1}$.

(a) Prove that φ is bijective.

(b) Prove that φ is an automorphism if and only if G is abelian.

13. (a) Let G be a group of order 4. Prove that every element of G has order 1, 2, or 4.

(b) Classify groups of order 4 by considering the following two cases:

(i) G contains an element of order 4.

(ii) Every element of G has order < 4.

14. Determine the group of automorphisms of the following groups.

(a) $\mathbb{Z}^+$, (b) a cyclic group of order 10, (c) S_3.

15. Show that the functions $f = 1/x$, $g = (x - 1)/x$ generate a group of functions, the law of composition being composition of functions, which is isomorphic to the symmetric group S_3.
16. Give an example of two isomorphic groups such that there is more than one isomorphism between them.

4. Homomorphisms

1. Let G be a group, with law of composition written $x \# y$. Let H be a group with law of composition $u \circ v$. What is the condition for a map $\varphi\colon G \longrightarrow H'$ to be a homomorphism?
2. Let $\varphi\colon G \longrightarrow G'$ be a group homomorphism. Prove that for any elements $a_1, \ldots, a_k$ of G, $\varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k)$.
3. Prove that the kernel and image of a homomorphism are subgroups.
4. Describe all homomorphisms $\varphi\colon \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$, and determine which are injective, which are surjective, and which are isomorphisms.
5. Let G be an abelian group. Prove that the nth power map $\varphi\colon G \longrightarrow G$ defined by $\varphi(x) = x^n$ is a homomorphism from G to itself.
6. Let $f\colon \mathbb{R}^+ \longrightarrow \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism, and determine its kernel and image.
7. Prove that the absolute value map $|\ |\colon \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ sending $\alpha \rightsquigarrow |\alpha|$ is a homomorphism, and determine its kernel and image.
8. **(a)** Find all subgroups of S_3, and determine which are normal.
   (b) Find all subgroups of the quaternion group, and determine which are normal.
9. **(a)** Prove that the composition $\varphi \circ \psi$ of two homomorphisms φ, ψ is a homomorphism.
   (b) Describe the kernel of $\varphi \circ \psi$.
10. Let $\varphi\colon G \longrightarrow G'$ be a group homomorphism. Prove that $\varphi(x) = \varphi(y)$ if and only if $xy^{-1} \in \ker \varphi$.
11. Let G, H be cyclic groups, generated by elements x, y. Determine the condition on the orders m, n of x and y so that the map sending $x^i \rightsquigarrow y^i$ is a group homomorphism.
12. Prove that the $n \times n$ matrices M which have the block form $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ with $A \in GL_r(\mathbb{R})$ and $D \in GL_{n-r}(\mathbb{R})$ form a subgroup P of $GL_n(\mathbb{R})$, and that the map $P \longrightarrow GL_r(\mathbb{R})$ sending $M \rightsquigarrow A$ is a homomorphism. What is its kernel?
13. **(a)** Let H be a subgroup of G, and let $g \in G$. The *conjugate subgroup* gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, where $h \in H$. Prove that gHg^{-1} is a subgroup of G.
    (b) Prove that a subgroup H of a group G is normal if and only if $gHg^{-1} = H$ for all $g \in G$.
14. Let N be a normal subgroup of G, and let $g \in G$, $n \in N$. Prove that $g^{-1}ng \in N$.
15. Let φ and ψ be two homomorphisms from a group G to another group G', and let $H \subset G$ be the subset $\{x \in G \mid \varphi(x) = \psi(x)\}$. Prove or disprove: H is a subgroup of G.
16. Let $\varphi\colon G \longrightarrow G'$ be a group homomorphism, and let $x \in G$ be an element of order r. What can you say about the order of $\varphi(x)$?
17. Prove that the center of a group is a normal subgroup.

18. Prove that the center of $GL_n(\mathbb{R})$ is the subgroup $Z = \{cI \mid c \in \mathbb{R}, c \neq 0\}$.

19. Prove that if a group contains exactly one element of order 2, then that element is in the center of the group.

20. Consider the set U of real 3×3 matrices of the form

$$\begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix}.$$

(a) Prove that U is a subgroup of $SL_n(\mathbb{R})$.
(b) Prove or disprove: U is normal.
***(c)** Determine the center of U.

21. Prove by giving an explicit example that $GL_2(\mathbb{R})$ is not a normal subgroup of $GL_2(\mathbb{C})$.

22. Let $\varphi\colon G \longrightarrow G'$ be a surjective homomorphism.
(a) Assume that G is cyclic. Prove that G' is cyclic.
(b) Assume that G is abelian. Prove that G' is abelian.

23. Let $\varphi\colon G \longrightarrow G'$ be a surjective homomorphism, and let N be a normal subgroup of G. Prove that $\varphi(N)$ is a normal subgroup of G'.

5. Equivalence Relations and Partitions

1. Prove that the nonempty fibres of a map form a partition of the domain.

2. Let S be a set of groups. Prove that the relation $G \sim H$ if G is isomorphic to H is an equivalence relation on S.

3. Determine the number of equivalence relations on a set of five elements.

4. Is the intersection $R \cap R'$ of two equivalence relations $R, R' \subset S \times S$ an equivalence relation? Is the union?

5. Let H be a subgroup of a group G. Prove that the relation defined by the rule $a \sim b$ if $b^{-1}a \in H$ is an equivalence relation on G.

6. **(a)** Prove that the relation x conjugate to y in a group G is an equivalence relation on G.
(b) Describe the elements a whose conjugacy class (= equivalence class) consists of the element a alone.

7. Let R be a relation on the set $\mathbb{R}$ of real numbers. We may view R as a subset of the (x, y)-plane. Explain the geometric meaning of the reflexive and symmetric properties.

8. With each of the following subsets R of the (x, y)-plane, determine which of the axioms (5.2) are satisfied and whether or not R is an equivalence relation on the set $\mathbb{R}$ of real numbers.
(a) $R = \{(s,s) \mid s \in \mathbb{R}\}$.
(b) $R =$ empty set.
(c) $R =$ locus $\{y = 0\}$.
(d) $R =$ locus $\{xy + 1 = 0\}$.
(e) $R =$ locus $\{x^2y - xy^2 - x + y = 0\}$.
(f) $R =$ locus $\{x^2 - xy + 2x - 2y = 0\}$.

9. Describe the smallest equivalence relation on the set of real numbers which contains the line $x - y = 1$ in the (x, y)-plane, and sketch it.

10. Draw the fibres of the map from the (x,z)-plane to the y-axis defined by the map $y = zx$.

11. Work out rules, obtained from the rules on the integers, for addition and multiplication on the set (5.8).
12. Prove that the cosets (5.14) are the fibres of the map φ.

6. Cosets

1. Determine the index $[\mathbb{Z} : n\mathbb{Z}]$.
2. Prove directly that distinct cosets do not overlap.
3. Prove that every group whose order is a power of a prime p contains an element of order p.
4. Give an example showing that left cosets and right cosets of $GL_2(\mathbb{R})$ in $GL_2(\mathbb{C})$ are not always equal.
5. Let H, K be subgroups of a group G of orders $3, 5$ respectively. Prove that $H \cap K = \{1\}$.
6. *Justify (6.15) carefully.*
7. **(a)** Let G be an abelian group of odd order. Prove that the map $\varphi: G \longrightarrow G$ defined by $\varphi(x) = x^2$ is an automorphism.
   (b) Generalize the result of (a).
8. Let W be the additive subgroup of $\mathbb{R}^m$ of solutions of a system of homogeneous linear equations $AX = 0$. Show that the solutions of an inhomogeneous system $AX = B$ form a coset of W.
9. Let H be a subgroup of a group G. Prove that the number of left cosets is equal to the number of right cosets **(a)** if G is finite and **(b)** in general.
10. **(a)** Prove that every subgroup of index 2 is normal.
    (b) Give an example of a subgroup of index 3 which is not normal.
11. Classify groups of order 6 by analyzing the following three cases.
    (a) G contains an element of order 6.
    (b) G contains an element of order 3 but none of order 6.
    (c) All elements of G have order 1 or 2.
12. Let G, H be the following subgroups of $GL_2(\mathbb{R})$:

$$G = \left\{\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}\right\}, \quad H = \left\{\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}\right\}, \quad x > 0.$$

An element of G can be represented by a point in the (x, y)-plane. Draw the partitions of the plane into left and into right cosets of H.

7. Restriction of a Homomorphism to a Subgroup

1. Let G and G' be finite groups whose orders have no common factor. Prove that the only homomorphism $\varphi: G \longrightarrow G'$ is the trivial one $\varphi(x) = 1$ for all x.
2. Give an example of a permutation of even order which is odd and an example of one which is even.
3. **(a)** Let H and K be subgroups of a group G. Prove that the intersection $xH \cap yK$ of two cosets of H and K is either empty or else is a coset of the subgroup $H \cap K$.
   (b) Prove that if H and K have finite index in G then $H \cap K$ also has finite index.

4. Prove Proposition (7.1).
5. Let H, N be subgroups of a group G, with N normal. Prove that $HN = NH$ and that this set is a subgroup.
6. Let $\varphi\colon G \longrightarrow G'$ be a group homomorphism with kernel K, and let H be another subgroup of G. Describe $\varphi^{-1}(\varphi(H))$ in terms of H and K.
7. Prove that a group of order 30 can have at most 7 subgroups of order 5.
*8. Prove the *Correspondence Theorem:* Let $\varphi\colon G \longrightarrow G'$ be a surjective group homomorphism with kernel N. The set of subgroups H' of G' is in bijective correspondence with the set of subgroups H of G which contain N, the correspondence being defined by the maps $H \rightsquigarrow \varphi(H)$ and $\varphi^{-1}(H') \leftsquigarrow H'$. Moreover, normal subgroups of G correspond to normal subgroups of G'.
9. Let G and G' be cyclic groups of orders 12 and 6 generated by elements x, y respectively, and let $\varphi\colon G \longrightarrow G'$ be the map defined by $\varphi(x^i) = y^i$. Exhibit the correspondence referred to the previous problem explicitly.

8. Products of Groups

1. Let G, G' be groups. What is the order of the product group $G \times G'$?
2. Is the symmetric group S_3 a direct product of nontrivial groups?
3. Prove that a finite cyclic group of order rs is isomorphic to the product of cyclic groups of orders r and s if and only if r and s have no common factor.
4. In each of the following cases, determine whether or not G is isomorphic to the product of H and K.
   (a) $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \{\text{positive real numbers}\}$.
   (b) $G = \{\text{invertible upper triangular } 2 \times 2 \text{ matrices}\}$, $H = \{\text{invertible diagonal matrices}\}$, $K = \{\text{upper triangular matrices with diagonal entries } 1\}$.
   (c) $G = \mathbb{C}^\times$ and $H = \{\text{unit circle}\}$, $K = \{\text{positive reals}\}$.
5. Prove that the product of two infinite cyclic groups is not infinite cyclic.
6. Prove that the center of the product of two groups is the product of their centers.
7. (a) Let H, K be subgroups of a group G. Show that the set of products $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup if and only if $HK = KH$.
   (b) Give an example of a group G and two subgroups H, K such that HK is not a subgroup.
8. Let G be a group containing normal subgroups of orders 3 and 5 respectively. Prove that G contains an element of order 15.
9. Let G be a finite group whose order is a product of two integers: $n = ab$. Let H, K be subgroups of G of orders a and b respectively. Assume that $H \cap K = \{1\}$. Prove that $HK = G$. Is G isomorphic to the product group $H \times K$?
10. Let $x \in G$ have order m, and let $y \in G'$ have order n. What is the order of (x, y) in $G \times G'$?
11. Let H be a subgroup of a group G, and let $\varphi\colon G \longrightarrow H$ be a homomorphism whose restriction to H is the identity map: $\varphi(h) = h$, if $h \in H$. Let $N = \ker \varphi$.
   (a) Prove that if G is abelian then it is isomorphic to the product group $H \times N$.
   (b) Find a bijective map $G \longrightarrow H \times N$ without the assumption that G is abelian, but show by an example that G need not be isomorphic to the product group.

9. Modular Arithmetic

1. Compute $(7 + 14)(3 - 16)$ modulo 17.
2. **(a)** Prove that the square a^2 of an integer a is congruent to 0 or 1 modulo 4.
   (b) What are the possible values of a^2 modulo 8?
3. **(a)** Prove that 2 has no inverse modulo 6.
   (b) Determine all integers n such that 2 has an inverse modulo n.
4. Prove that every integer a is congruent to the sum of its decimal digits modulo 9.
5. Solve the congruence $2x \equiv 5$ **(a)** modulo 9 and **(b)** modulo 6.
6. Determine the integers n for which the congruences $x + y \equiv 2$, $2x - 3y \equiv 3$ (modulo n) have a solution.
7. Prove the associative and commutative laws for multiplication in $\mathbb{Z}/n\mathbb{Z}$.
8. Use Proposition (2.6) to prove the *Chinese Remainder Theorem:* Let m, n, a, b be integers, and assume that the greatest common divisor of m and n is 1. Then there is an integer x such that $x \equiv a$ (modulo m) and $x \equiv b$ (modulo n).

10. Quotient Groups

1. Let G be the group of invertible real upper triangular 2×2 matrices. Determine whether or not the following conditions describe normal subgroups H of G. If they do, use the First Isomorphism Theorem to identify the quotient group G/H.
   (a) $a_{11} = 1$ **(b)** $a_{12} = 0$ **(c)** $a_{11} = a_{22}$ **(d)** $a_{11} = a_{22} = 1$
2. Write out the proof of (10.1) in terms of elements.
3. Let P be a partition of a group G with the property that for any pair of elements A, B of the partition, the product set AB is contained entirely within another element C of the partition. Let N be the element of P which contains 1. Prove that N is a normal subgroup of G and that P is the set of its cosets.
4. **(a)** Consider the presentation (1.17) of the symmetric group S_3. Let H be the subgroup $\{1, y\}$. Compute the product sets $(1H)(xH)$ and $(1H)(x^2H)$, and verify that they are not cosets.
   (b) Show that a cyclic group of order 6 has two generators satisfying the rules $x^3 = 1$, $y^2 = 1$, $yx = xy$.
   (c) Repeat the computation of (a), replacing the relations (1.18) by the relations given in part (b). Explain.
5. Identify the quotient group $\mathbb{R}^\times/P$, where P denotes the subgroup of positive real numbers.
6. Let $H = \{\pm 1, \pm i\}$ be the subgroup of $G = \mathbb{C}^\times$ of fourth roots of unity. Describe the cosets of H in G explicitly, and prove that G/H is isomorphic to G.
7. Find all normal subgroups N of the quaternion group H, and identify the quotients H/N.
8. Prove that the subset H of $G = GL_n(\mathbb{R})$ of matrices whose determinant is positive forms a normal subgroup, and describe the quotient group G/H.
9. Prove that the subset $G \times 1$ of the product group $G \times G'$ is a normal subgroup isomorphic to G and that $(G \times G')/(G \times 1)$ is isomorphic to G'.
10. Describe the quotient groups $\mathbb{C}^\times/P$ and $\mathbb{C}^\times/U$, where U is the subgroup of complex numbers of absolute value 1 and P denotes the positive reals.
11. Prove that the groups $\mathbb{R}^+/\mathbb{Z}^+$ and $\mathbb{R}^+/2\pi\mathbb{Z}^+$ are isomorphic.

Miscellaneous Problems

1. What is the product of all mth roots of unity in $\mathbb{C}$?
2. Compute the group of automorphisms of the quaternion group.
3. Prove that a group of even order contains an element of order 2.
4. Let $K \subset H \subset G$ be subgroups of a finite group G. Prove the formula $[G : K] = [G : H][H : K]$.

*5. A *semigroup* S is a set with an associative law of composition and with an identity. But elements are not required to have inverses, so the cancellation law need not hold. The semigroup S is said to be generated by an element s if the set $\{1, s, s^2, \ldots\}$ of nonnegative powers of s is the whole set S. For example, the relations $s^2 = 1$ and $s^2 = s$ describe two different semigroup structures on the set $\{1, s\}$. Define isomorphism of semigroups, and describe all isomorphism classes of semigroups having a generator.

6. Let S be a semigroup with finitely many elements which satisfies the Cancellation Law (1.12). Prove that S is a group.

*7. Let $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ be points in k-dimensional space $\mathbb{R}^k$. A ***path*** from a to b is a continuous function on the interval $[0, 1]$ with values in $\mathbb{R}^k$, that is, a function f: $[0, 1] \longrightarrow \mathbb{R}^k$, sending $t \rightsquigarrow f(t) = (x_1(t), \ldots, x_k(t))$, such that $f(0) = a$ and $f(1) = b$. If S is a subset of $\mathbb{R}^k$ and if $a, b \in S$, we define $a \sim b$ if a and b can be joined by a path lying entirely in S.
   (a) Show that this is an equivalence relation on S. Be careful to check that the paths you construct stay within the set S.
   (b) A subset S of $\mathbb{R}^k$ is called *path connected* if $a \sim b$ for any two points $a, b \in S$. Show that every subset S is partitioned into path-connected subsets with the property that two points in different subsets can not be connected by a path in S.
   (c) Which of the following loci in $\mathbb{R}^2$ are path-connected? $\{x^2 + y^2 = 1\}$, $\{xy = 0\}$, $\{xy = 1\}$.

*8. The set of $n \times n$ matrices can be identified with the space $\mathbb{R}^{n \times n}$. Let G be a subgroup of $GL_n(\mathbb{R})$. Prove each of the following.
   (a) If $A, B, C, D \in G$, and if there are paths in G from A to B and from C to D, then there is a path in G from AC to BD.
   (b) The set of matrices which can be joined to the identity I forms a normal subgroup of G (called the *connected component* of G).

*9. (a) Using the fact that $SL_n(\mathbb{R})$ is generated by elementary matrices of the first type (see exercise 18, Section 2), prove that this group is path-connected.
   (b) Show that $GL_n(\mathbb{R})$ is a union of two path-connected subsets, and describe them.

10. Let H, K be subgroups of a group G, and let $g \in G$. The set

$$HgK = \{x \in G \mid x = hgk \text{ for some } h \in H, k \in K\}$$

is called a *double coset*.
   (a) Prove that the double cosets partition G.
   (b) Do all double cosets have the same order?

11. Let H be a subgroup of a group G. Show that the double cosets HgH are the left cosets gH if H is normal, but that if H is not normal then there is a double coset which properly contains a left coset.

*12. Prove that the double cosets in $GL_n(\mathbb{R})$ of the subgroups $H = \{\text{lower triangular matrices}\}$ and $K = \{\text{upper triangular matrices}\}$ are the sets HPK, where P is a permutation matrix.

2.1 The Definition of a Group

(1) (a)

$$1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, x = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, y = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$x^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, xy = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, x^2y = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$x^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, y^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, yx = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = x^2y$$

(b)

	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	x^3

(2) (a) Let $A, B, C \in GL(\mathbb{R})$.

Note that $\det(AB) = \det(A)\det(B) \neq 0$, so $AB \in GL(\mathbb{R})$, so multiplication is a law of composition of $GL(\mathbb{R})$.

Further for $1 \leq i, j \leq n$,

$$((AB)C)_{ij} = \sum_{k=1}^{n} (AB)_{ik} c_{kj} = \sum_{k=1}^{n} \left(\sum_{m=1}^{n} a_{im} b_{mk} \right) c_{kj}$$

$$= \sum_{k=1}^{n} \sum_{m=1}^{n} a_{im} b_{mk} c_{kj} = \sum_{m=1}^{n} a_{im} \left(\sum_{k=1}^{n} b_{mk} c_{kj} \right)$$

$$= \sum_{m=1}^{n} a_{im} (BC)_{mj} = (A(BC))_{ij}$$

So multiplication is associative on $GL(\mathbb{R})$.

Note that $I \in GL(\mathbb{R})$, and $AI = IA = A$, so $GL(\mathbb{R})$ contains the identity matrix.

Since $\det A \neq 0$, then A is invertible. Necessarily, $\det A^{-1} \neq 0$, and $AA^{-1} = A^{-1}A = I$, so A has an inverse.

Thus, $GL(\mathbb{R})$ is a group.

(b) Let $X, Y, Z \in S_n$. Then for some $a, b, c \in 1...n$, $(XY)(a) = X(Y(a)) = X(b) = c$. So we have a law of composition of S_n.

Further,

$$((XY)Z)(a) = (XYZ)(a) = (X(YZ))(a)$$

So the law of composition is associative.

Note that $i \in S_n$, and $(Xi)(a) = X(i(a)) = X(a) = b$, and $(iX)(a) = i(X(a)) = i(b) = b$. so S_n contains the identity permutation.

Suppose X is a permutation such that $X(a) = b, X(b) = c$. Then there exists a permutation Y such that $Y(b) = a, Y(c) = b$. So then $(XY)(b) = X(Y(b)) = X(a) = b$, and $(YX)(b) = Y(X(b)) = Y(c) = b$. Thus X is invertible, and its inverse is Y.

(3) Let $T = \{s \in S | s \text{ is invertible}\}$. Note that $I \in T$, since $II = I$. Let $t \in T$. t is invertible, and has inverse w. Since $tw = I$, and $wt = I$, then w is also invertible with inverse t. Thus, $w \in T$. Thus, since T has an associative law of composition and the identity, then T is a group.

(4)
$$xyz^{-1}w = 1 \to yz^{-1}w = x^{-1} \to yz^{-1} = x^{-1}w^{-1} \to y = x^{-1}w^{-1}z$$

(5)
$$xyz = 1 \to yz = x^{-1} \to yzx = 1$$

It does not follow that $yxz = 1$. Let $a = x, b = y, c = xy$. Then $abc = 1$. But $bac = yxxy = yx^2y = yyx = y^2x = x \neq 1$.

(6)
$$(abcd), a(bcd), (abc)d, (ab)(cd), (ab)cd, a(bc)d, ab(cd), abcd$$

(7) Let $a, b, c \in S$. Then
$$(ab)c = ac = a = ab = a(bc)$$
Thus, the law of composition is associative.

(8) Let
$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$
Note that
$$A^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
So
$$A^{-1}B = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$
But
$$BA^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$
So $A^{-1}B \neq BA^{-1}$

(9)
$$ab = a \to a^{-1}ab = a^{-1}a \to b = 1$$
$$ab = 1 \to a^{-1}ab = a^{-1} \to b = a^{-1}$$

(10)
$$ax = b \to x = a^{-1}b$$
Since a, b are distinct elements, then x is unique.

(11) Let $a, b, c \in G^\circ$. Since $a \circ b = ba \in G$, then $\circ$ is a law of composition in G. And,
$$(a \circ b) \circ c = (ba) \circ c = cba = (cb)a = a \circ (cb) = a \circ (b \circ c)$$
So $\circ$ is associative.
Since $I \in G$, then $a \circ I = Ia = a = aI = I \circ a$, so $I \in G^\circ$.
Let a^{-1} be the inverse of a in G. Then
$$a \circ a^{-1} = a^{-1}a = I = aa^{-1} = a^{-1} \circ a$$
So therefore a has an inverse in G°, namely a^{-1}. Thus G° is a group.

2.2 Subgroups

(1)
$$x = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}, x^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, x^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$x^4 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, x^5 = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, x^6 = 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(2)
$$a^3b = ba^3 \to a^3a^3b = a^3ba^3 \to ab = a^5ab = a^3b^3$$
And
$$a^3b = ba^3 \to a^3ba^3 = ba^3a^3 \to a^3ba^3 = baa^5 = ba$$
Thus, $ab = ba$

(3) (a) Yes. $GL_N(\mathbb{R})$ is a group, so it is a subgroup of $GL_N(\mathbb{C})$.

(b) Yes. Let $A, B \in \{1, -1\}$. Clearly, $AB \in \{1, -1\}$. And, $1 \in \{1, -1\}$, $1^{-1} = 1$, and $(-1)^{-1} = -1$. So, $\{1, -1\}$ is a subgroup of $\mathbb{R}^\times$.

(c) No. Let $\mathcal{A}$ be the set of positive integers in $\mathbb{Z}^+$. For $a \in \mathcal{A}$ where $a \neq 0$, $-a \notin \mathcal{A}$. So $\mathcal{A}$ is not a subgroup.

(d) Yes. Let $\mathcal{A}$ be the set of positive reals in $\mathbb{R}^\times$. For $a, b \in \mathcal{A}$, clearly $ab \in \mathcal{A}$. And, $1 \in \mathcal{A}$. For $a \in \mathcal{A}$, since $a^{-1} > 0$, then $a^{-1} \in \mathcal{A}$. so $\mathcal{A}$ is a subgroup of $\mathbb{R}^\times$.

(e) No. Let $a = 1$. Then
$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \notin GL_2(\mathbb{R})$$
Since
$$\det \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

(4) Let $x \in H$. Since $1 = xx^{-1} \in H$, then H contains the identity. And, since $x^{-1} = 1x^{-1} \in H$, then H is closed under inverses. Let $x, y \in H$. Then $y^{-1} \in H$. Then $xy = x(y^{-1})^{-1} \in H$. Thus, H is a subgroup of G.

(5) Let $\mathcal{A}$ be the nth roots of unity. Let $a, b \in \mathcal{A}$. Since $(ab)^n = a^n b^n = 1$, then $ab \in \mathcal{A}$. And, since $1^n = 1$, then $1 \in \mathcal{A}$. And, $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$. Thus $\mathcal{A} \subseteq \mathbb{C}^\times$. There are n such roots: $z = e^{\frac{2\pi k}{n}}$ for $k = 0, ..., n-1$. $\mathcal{A}$ is generated by $z = e^{\frac{2\pi}{n}}$, so $\mathcal{A}$ is a cyclic subgroup of order n.

(6) (a) Let

$$a = \begin{bmatrix} -1 & \\ & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}$$

$a^2 = b^2 = I$, and $ab = ba$.

(b) For each of the following sets the identity matrix is contained, they are closed under multiplication, and they are closed under inverses (in particular, the inverse of any matrix in the Klein four group is itself). Thus, the subgroups of the Klein four group are:

$$\left\{ \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} \pm 1 & \\ & \pm 1 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} -1 & \\ & -1 \end{bmatrix} \right\}$$
$$\left\{ \begin{bmatrix} \pm 1 & \\ & 1 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 1 & \\ & \pm 1 \end{bmatrix} \right\}$$

(7) (a) Let $ar + bs, ax + by \in a\mathbb{Z} + b\mathbb{Z}$. Then $ar + bs + ax + by = a(r + x) + b(s + y) \in a\mathbb{Z} + b\mathbb{Z}$. Further, $0 = 0r + bs \in a\mathbb{Z} + b\mathbb{Z}$, and $ar + bs + a(-r) + b(-s) = 0$, so $a\mathbb{Z} + b\mathbb{Z}$ is closed under inverses. Thus, $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$.

(b) Let $c = ar + bs \in a\mathbb{Z} + b\mathbb{Z}$. Then

$$c = ar + bs = s(b + 7a) + ar - 7as = s(b + 7a) + (r - 7s)a$$

Thus, $a\mathbb{Z} = b\mathbb{Z}$ is generated by a and $b + 7a$.

(8)

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

(9) Let $x \in H$. Then we can write x has a string of products of a and b and their inverses. Ie. $x = a^{a_1} b^{b_1} ... a^{a_n} b^{b_n}$, where a_n, b_n are integers. Since $ab = ba$ and hence $a^{-1}b^{-1} = b^{-1}a^{-1}$, $ab^{-1} = b^{-1}a$, and $a^{-1}b = ba^{-1}$, then we can also write $x = a^{a_1 + ... + a_n} b^{b_1 + ... + b_n} = a^{b_1 + ... + b - n} a^{a_1 + ... + a_n}$, or equivalently for some integers c, d, $x = a^c b^d = b^d a^c$.

So, let $x = a^{x_a} b^{x_b}, y = a^{y_a} b^{y_b} \in H$, where x_a, x_b, y_a, y_b are integers. Then

$$xy = a^{x_a} b^{x_b} a^{y_a} b^{y_b} = a^{y_a} b^{y_b} a^{x_a} b^{x_b} = yx$$

Thus, H is abelian.

(10) (a) If x has order rs, then $(x^r)^s = x^{rs} = 1$. Suppose for some $k < s$, $(x^r)^k = 1$. Then this implies $x^{rk} = 1$. But $rk < rs$, so rs is not the order of x. Contradiction. Thus s is the order of x^r.

(b) If x has order n, then for some s and k such that $rs = kn$, then $(x^r)^s = x^{rs} = x^{kn} = (x^n)^k = 1$. Choose k such that $k = r/\gcd(n, r)$. Then r divides kn, so s is an integer, namely $s = n/\gcd(n, r)$. We now claim that s is the order of x^r. Let a be the order of x^r. Then a divides s. Since $(x^r)^a = x^{ra} = 1$, then n divides ra. Since $n/\gcd(n, r)$ does not divide r unless $\gcd(n, r) = n$ or $r = 1$, then $s = n/\gcd(n, r)$ divides a. Thus, $s = a$.

(11) Let $|ab| = n$. Then $1 = (ab)^n = a(ba)^{n-1}b \to a^{-1}b^{-1} = (ba)^{n-1} \to (ba)^{-1} = (ba)^{n-1} \to 1 = (ba)^n$. Suppose now that $|ba| = m$, so that $n \geq m$. We can similarly show that $(ab)^m = 1$, so then $n \leq m$. Thus, $n = m$.

(12) Clearly, the trivial group has no proper subgroup.

Suppose we have a nontrivial group G with no proper subgroup. So for all $g \in G$ where $g \neq e$, where e is the identity, g generates G. Suppose $|G| = \infty$. Then g^2 generates a nontrivial subgroup, since it does not contain g. Thus, for $|G| < \infty$, $G = \left\{e, g, g^2, ..., g^{|G|-1}\right\}$. Furthermore, for all $1 \leq k \leq |G| - 1$, $G = \left\{e, g^k, (g^k)^2, ..., (g^k)^{|G|-1}\right\}$, where for each i, $g^{ik} \neq 1$. Suppose $|G|$ is composite. Then for some k and a, $|G| = ka$. Thus, $(g^k)^a = 1$. Thus, $|G|$ must be prime.

So, a nontrivial group G with no proper subgroup is a cyclic subgroup with prime order.

(13) Let G be a cyclic group with generator g, and let A be a subgroup of G. Then for some $a \in A, a = g^k$ for some k, and a has order n. Suppose for some $b \in A$, b is not generated by a, and a is not generated by b. Then for some ℓ, $b = g^\ell$, where $\gcd(k, \ell) = 1$, and b has order m. But since for some c, d, $g^{ck+d\ell} = g$, then $A = G$, so A is cyclic. Thus, b is generated by a, or a is generated by b. Thus, A is a cyclic group.

(14) Suppose G is generated by g, and $n = pr$ for some p. Note that $\mathcal{A} = \left\{e, g^p, ..., g^{p(r-1)}\right\}$ is a cyclic subgroup of G of order r generated by g^p. I claim that $\mathcal{A}$ is the only cyclic subgroup of G of order r. Suppose there exists some other subgroup of G, $\mathcal{B}$, where the order of $\mathcal{B}$ is r, and $\mathcal{B}$ is generated by g^q for some q. Then $(g^q)^r = g^{qr} = 1$. So n divides qr, and so p divides q. But then g^p generates g^q. So, $\mathcal{B}$ is generated by g^p. Thus, $\mathcal{A} = \mathcal{B}$.

(15) (a) Let e be the identity of H and f be the identity of G. Then $e^2 = e = ef \to e = f$.

(b) Let $a, b \in H, c \in G$, where b is the inverse of a in H, and c is the inverse of a in G. Then $e = ab = ac \to bab = bac \to b = c$.

(16) (a) Let $G = \left\{1, g, g^2, g^3, g^4, g^5\right\}$. Since $1^1 = 1, g^6 = 1, (g^2)^3 = 1, (g^3)^2 = 1, (g^4)^3 = 1, (g^5)^6 = 1$, then g and g^5 generate G

(b) Let $A = \left\{1, a, a^2, a^3, a^4\right\}$. Since $1^1 = 1, a^5 = 1, (a^2)^5 = 1, (a^3)^5 = 1, (a^4)^5 = 1$, then a, a^2, a^3, a^4 generate A.

Let $B = \left\{1, b, b^2, b^3, b^4, b^5, b^6, b^7\right\}$. Since $1^1 = 1, b^8 = 1, (b^2)^4 = 1, (b^3)^8 = 1, (b^4)^2 = 1, (b^5)^8 = 1, (b^6)^4 = 1, (b^7)^8 = 1$, then b, b^3, b^5, b^7 generate B.

Let $C = \left\{1, c, c^2, c^3, c^4, c^5, c^6, c^7, c^8, c^9\right\}$. Since $1^1 = 1, c^{10} = 1, (c^2)^5 = 1, (c^3)^{10} = 1, (c^4)^5 = 1, (c^5)^2 = 1, (c^6)^5 = 1, (c^7)^{10} = 1, (c^8)^5 = 1, (c^9)^{10} = 1$, then c, c^3, c^7, c^9 generate C.

(c) If g generates G and has order n, then g^k generates G if $\gcd(k, n) = 1$.

(17) Let $a, b \in G$. Then $a^2 = b^2 = 1 \to a = a^{-1}, b = b^{-1}$. Furthermore, $(ab)^2 = 1 \to ab = (ab)^{-1}$. Then

$$a = a^{-1}, b = b^{-1} \to ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$

(18) (a) Let A be an elementary matrix of the second kind whose operation is interchanging rows i and j. Ie.

$$A = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

Let

$$E_1 = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & -1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

$$E_2 = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & -1 & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

$$E_3 = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & 1 & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

Ie. E_1 scales row j by -1, E_2 sets row j equal to row j minus row i, and E_3 sets row i equal to row i plus row j. Then $A = E_1E_2E_3E_2$. So, we can write an elementary matrix

of the second kind as a product of elementary matrices of the first and third kinds. So then we can generate any invertible matrix with elementary matrices of the first and third kinds.

(b) Clearly, $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. Let $A, B \in SL_n(\mathbb{R})$. Since $\det(AB) = \det(A)\det(B) = 1$, then $AB \in SL_n(\mathbb{R})$. Since $I_n \in SL_n(\mathbb{R})$, and $\det(A^{-1}) = \det(A)^{-1} = 1$, then $A^{-1} \in SL_n(\mathbb{R})$. Thus, $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

(c) Consider the 2×2 matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Since $\det A = 1$, then $ad - bc = 1$.

If $c \neq 0$, then reducing A:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to \begin{bmatrix} 1 & b + d(1-a)/c \\ c & d \end{bmatrix} \to \begin{bmatrix} 1 & b + d(1-a)/c \\ & ad - bc \end{bmatrix} \to \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

If $c = 0$, then $a \neq 0$ (otherwise $\det A = 0$). Then:

$$\begin{bmatrix} a & b \\ & d \end{bmatrix} \to \begin{bmatrix} a & b \\ 1-a & d + b(1-a)/a \end{bmatrix} \to \begin{bmatrix} 1 & d + b/a \\ 1-a & d + b(1-a)/a \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & d + b/a \\ & ad \end{bmatrix} \to \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

A was reduced only with type 1 operations, so we can write A as a product of elementary matrices of the first kind.

Suppose for all $X \in SL_{n-1}(\mathbb{R})$ we can write X as a product of elementary matrices of the first kind. Now consider an $n \times n$ matrix B. Suppose $b_{21} = ... = b_{n1} = 0$. Then $b_{11} \neq 0$ (otherwise $\det B = 0$). The following operations set $b_{11} = 1$ while keeping $b_{21} = ... = b_{n1} = 0$:

$$\begin{bmatrix} 1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \begin{bmatrix} & 1 & & \\ (1-b_1)/b_1 & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

Suppose now that $b_{11} = 0$. Then for some b_{i1}, $b_{i1} \neq 0$. Then the following operation sets $b_{11} = 1$:

$$\begin{bmatrix} 1 & & 1/b_{i1} & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

If $b_{11} = 1$, then we can perform type 1 operations to set $b_{21} = ... = b_{n1} = 0$: namely if $b_{i1} \neq 0$, then we can perform the following operation:

$$\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ -b_{i1} & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}$$

After applying the above operations, now $b_{11} = 1$ and $b_{21} = ... = b_{n1} = 0$. Consider the submatrix B_{11}. Since $1 = \det B = b_{11} \det B_{11}$, then $\det B_{11} = 1$, since $B_{11} \in SL_{n-1}(\mathbb{R})$. By the inductive hypothesis, there exists a series of type 1 matrices such that B_{11} can be reduced to the identity. So, B can be reduced to an upper triangular matrix B' with 1s as its diagonal entries. Now we can apply type one operations to clear the entries above the diagonal, so that B' is row reduced to the identity. Since for elementary matrices of the first kind $E_1, ..., E_p$ exist such that $E_1...E_pB = I$, then $B = E_p^{-1}...E_1^{-1}$ is a product of elementary matrices of the first kind. Thus elementary matrices of the first kind generate $SL_n(\mathbb{R})$.

(19)

$$\begin{bmatrix} & 1 & & \\ 1 & & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \begin{bmatrix} & & 1 & \\ & 1 & & \\ 1 & & & \\ & & & 1 \end{bmatrix}, \begin{bmatrix} & & & 1 \\ & 1 & & \\ & & 1 & \\ 1 & & & \end{bmatrix}$$

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & & & 1 \\ & & 1 & \\ & 1 & & \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix}$$

$$\begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{bmatrix}, \begin{bmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{bmatrix}, \begin{bmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{bmatrix}$$

There are 9 elements with order 2 in S_4.

(20) (a) Note that

$$\begin{aligned} (ab)^{nm/\gcd(n,m)} &= a^{nm/\gcd(n,m)} b^{nm/\gcd(n,m)} \\ &= (a^m)^{n/\gcd(n,m)} (b^n)^{m/\gcd(n,m)} = 1 \end{aligned}$$

So ab has finite order as most $\frac{nm}{\gcd(n,m)}$.

(b) Consider

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$$

Note that $A^4 = I, B^6 = I$. But

$$AB = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, (AB)^n = \begin{bmatrix} 1 & n \\ & 1 \end{bmatrix}$$

So, AB does not have finite order.

(21) From the previous exercise, then if $a, b \in G$, where G is an abelian group and a, b have finite order, then ab also has finite order. Let H be the subset of G whose elements have finite order. Clearly, $e \in H$, where e is the identity. And, for $a \in H$, where $|a| = n$, then $a^{-1} = a^{n-1}$. So, H is a subgroup of G.

(22) Let $a = p_1^{a_1}...p_n^{a_n}, b = p_1^{b_1}...p_n^{b_n}$, where $p_1...p_n$ are primes and $a_1, ..., a_n, b_1, ..., b_n \geq 0$. Such product of primes is unique by the Fundamental Theorem of Arithmetic. Let g be the greatest common divisor of a and b. Since g divides a and g divides b, then $g = p_1^{c_1}...p_n^{c_n}$, where for all i, $c_i \geq 0, c_i \leq a_i, c_i \leq b_i$. Suppose some integer h also divides a and b. Then $h = p_1^{d_1}...p_n^{d_n}$. Then g also divides h. So for all i, $c_i \geq d_i$, ie. c_i is the largest integer such that $c_i \leq a_i$ and $c_i \leq b_i$. Thus, $g = p_1^{\min(a_1,b_1)}...p_n^{\min(a_n,b_n)}$.

2.3 Isomorphisms

(1) Let $\varphi(x) = 2^x$. Then for $a, b \in \mathbb{R}^+$, $\varphi(a+b) = 2^{a+b} = 2^a 2^b = \varphi(a)\varphi(b)$. Since $2^x > 0$ for all x, then φ is injective. And, $\log_2(2^x) = x$, so φ is surjective, and is therefore bijective. So, φ is an isomorphism from $\mathbb{R}^+$ to P. Thus, $\mathbb{R}^+$ and P are isomorphic.

(2) $a(ba)a^{-1} = ab$, so ab and ba are conjugate elements.

(3) Suppose $a = a'$. Then

$$a = bab^{-1} \rightarrow ab = ba$$

Now suppose $ab = ba$. Then

$$ab = ba \rightarrow b^{-1}ab = a \rightarrow a = a'$$

(4) (a) Suppose for $n - 1 \geq 1$, $b'^{n-1} = ab^{n-1}a^{-1}$. Then

$$b'^n = (aba^{-1})^n = aba^{-1}(aba^{-1})^{n-1} = aba^{-1}ab^{n-1}a^{-1} = ab^n a^{-1}$$

If $n = 0$, Then $ab^0a^{-1} = 1 = b'^0$.
If $n \leq -1$, then

$$b'^n = (b^{-n})^{-1} = (ab^{-n}a^{-1})^{-1} = ab^n a^{-1}$$

(b) Note that $ab = b^2a$. Then

$$a^3ba^{-3} = a^2b^2a^{-2} = ab^2aba^{-2} = ab^4a^{-1} = b^8$$

(5) Since φ is a bijection, then φ^{-1} is also a bijection. And, for $c, d \in G'$, then for some $a, b \in G$, $\varphi(a) = c$ and $\varphi(b) = d$. Then

$$\varphi^{-1}(cd) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(c)\varphi^{-1}(d)$$

Thus, φ^{-1} is an isomorphism.

(6) (a) Let n, m be the orders of x and x' respectively. Then

$$1 = \varphi(1) = \varphi(x^n) = \varphi(x)^n = x'^n$$

So $m \leq n$. But

$$1 = x'^m = \varphi(x)^m = \varphi(x^m) \to x^m = 1$$

So, $n \leq m$. Therefore, $n = m$.

(b)

$$x'y'x' = \varphi(x)\varphi(y)\varphi(x) = \varphi(xyx) = \varphi(yxy)$$
$$= \varphi(y)\varphi(x)\varphi(y) = y'x'y'$$

(c) Since

$$1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$$

Then

$$\varphi(x^{-1}) = \varphi(x)^{-1} = x'^{-1}$$

(7) Note that

$$\begin{bmatrix} & 1 \\ 1 & \end{bmatrix}\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\begin{bmatrix} & 1 \\ 1 & \end{bmatrix} = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & \end{bmatrix} = \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$$

Thus,

$$\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix}$$

are conjugate elements in $GL_2(\mathbb{R})$. Now, let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R})$$

Then

$$A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

So if the two matrices are conjugate, then now we have

$$\begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d-c & a-b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad-ac-bc & a^2 \\ -c^2 & ac+ad-bc \end{bmatrix}$$

$$= \begin{bmatrix} -ac & a^2 \\ -c^2 & ac \end{bmatrix}$$

So, we have $1 = ac$ and $a^2 = 0$. So $a = 0$. But then we have $1 = 0$, a contradiction. Thus, they are not conjugate in the group $SL_n(\mathbb{R})$.

(8) Let

$$A = \begin{bmatrix} 1 & 3 \\ & 1 \end{bmatrix}, A^{-1} = \begin{bmatrix} 1 & -3 \\ & 1 \end{bmatrix}$$

Then

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

So,

$$\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ & 2 \end{bmatrix}$$

are conjugate elements in $GL_2(\mathbb{R})$.

(9) Denote $\cdot$ to be the group operation of G^0. Consider $\varphi(x) = x^{-1}$. Since $x = \varphi(x)^{-1}$, then φ is a bijection. Then for $a, b \in G$,

$$\varphi(ab) = (ab^{-1}) = b^{-1}a^{-1} = a^{-1} \cdot b^{-1} = \varphi(a) \cdot \varphi(b)$$

Thus, φ is an isomorphism between G and G^0.

(10) Denote $\varphi(A) = (A^\top)^{-1}$. Since

$$\varphi(A^\top)^{-1}) = (((A^\top)^{-1})^\top)^{-1} = (((A^\top)^{-1})^{-1})^\top = A$$

Then φ is a bijection. Then for $A, B \in GL_n(\mathbb{R})$,

$$\varphi(AB) = ((AB)^\top)^{-1} = (B^\top A^\top)^{-1} = (A^\top)^{-1}(B^\top)^{-1} = \varphi(A)\varphi(B)$$

Thus, φ is an automorphism of $GL_n(\mathbb{R})$.

(11) Consider $\varphi, \tau \in \text{Aut } G$. Let $a, b \in G$. Then

$$(\varphi \circ \tau)(ab)\varphi(\tau(a)\tau(b)) = \varphi(\tau(a))\varphi(\tau(b)) = (\varphi \circ \tau)(a)(\varphi \circ \tau)(b)$$

Furthermore, φ^{-1} and τ^{-1} exist since φ and τ are bijections. Then $((\tau^{-1} \circ \varphi^{-1}) \circ (\varphi \circ \tau))(a) = a$, so $\varphi \circ \tau$ is a bijection. Therefore, function composition is a law of composition of Aut G. Further, function composition is associative.

Let e be the trivial automorphism, ie. $e(a) = a$. Note that $\varphi \circ e = e \circ \varphi$. So, e is the identity automorphism.

Further, $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = e$. so Aut G is closed under inverses, and is therefore a group.

(12) (a) $\varphi(x^{-1} = x$, so φ is bijective.

(b) Suppose φ is an automorphism. Then for $x, y \in G$, then

$$y^{-1}x^{-1} = \varphi(xy) = \varphi(x)\varphi(y) = x^{-1}y^{-1} \to xy = yx$$

So, G is abelian.

Now suppose G is abelian. Then

$$\varphi(xy) = (xy)^{-1} = (yx)^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$$

So, φ is an automorphism.

(13) (a) Suppose for some $a \in G$, that $a^n = 1$, where $n > 4$. Then $1, a, a^2, a^3, a^4$ are all distinct (if $a^i = a^j$ for some i, j, $n > j > i$, then $a^{j-i} = 1$, so $|a| < n$). So, $|G| \geq 5$, a contradiction. Thus, $n \leq 4$. Suppose $n = 3$. Then for some $b \in G$, $1 \neq a \neq a^2 \neq b$. Consider the product ab. If $ab = b$, then $a = 1$, a contradiction. For $i = 1, 2$, if $ab = a^i$, then $b = a^{i-1}$, a contradiction. And, if $ab = 1$, then $b = a^{-1} = a^2$, a contradiction. Therefore, $ab \notin G$, so therefore if G has order 4, then no element can have order 3.

(b) (i) Consider $a \in G$, where $|a| = 4$. Then $1, a, a^2, a^3$ are distinct. Since $|G| = 4$, then a generates G, so G is a cyclic group of order 4.

(ii) Consider $a \in G$. If $a^1 = 1$, then $a = 1$. If $a^2 = 1$, then $a = a^{-1}$. So, the elements of G are their own inverses.

(14) (a) Let φ be an automorphism of $\mathbb{Z}^+$. Note that for $n \in \mathbb{Z}^+$,

$$\varphi(n) = \varphi(n1) = n\varphi(1)$$

So, if $\varphi(1) = a$, then $an = \varphi(n)$, ie. φ is determined by the mapping $1 \mapsto a$. Furthermore, since $\varphi^{-1}(n) = \frac{n}{a}$, then $\frac{1}{a}$, then for all n, a divides n. Thus, $a = 1, -1$. So, φ is the mapping determined by $1 \mapsto \{-1, 1\}$.

(b) Let G be a cyclic group of order 10 generated by g. For an automorphism φ of G and $x \in G$, then $|x| = |\varphi(x)|$. So, g maps to one of g, g^3, g^7, g^9. Then for all i, $\varphi(g^i) = \varphi(g)^i = g^{ik}$, where $k = 1, 3, 7, 9$. For i, j, if $g^{ik} = g^{jk}$, then $g^{k(j-i)} = 1$. Then $j = i$, so therefore each g^{ik} is distinct. Thus, φ is the mapping determined by $g \mapsto \left\{g, g^3, g^7, g^9\right\}$.

(c) Let

$$x = \begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix}, y = \begin{bmatrix} & 1 & \\ 1 & & \\ & & 1 \end{bmatrix}$$

Let φ be an automorphism of S_3. Then for $0 \leq i \leq 2, 0 \leq j \leq 1$,

$$\varphi(x^i y^j) = \varphi(x)^i \varphi(y)^j$$

Ie. φ is determined by $\varphi(x)$ and $\varphi(y)$. Since $|x| = |x^2|$ and $|y| = |xy| = |x^2 y|$, then x maps to one of x, x^2, and y maps to one of $y, xy, x^2 y$. Thus, φ is the mapping determined by $x \mapsto \left\{x, x^2\right\}$ and $y \mapsto \left\{y, xy, x^2 y\right\}$.

(15) First, denote $e(x) = x$. Note that for some function f, $e(f(x)) = f(x) = f(e(x))$, so $e(x)$ is an identity function. Further,

$$f^2(x) = \frac{1}{\frac{1}{x}} = x = e(x)$$

$$g^2(x) = \frac{\frac{x-1}{x} - 1}{\frac{x-1}{x}} = \frac{x - 1 - x}{x - 1} = \frac{-1}{x - 1}$$

$$g^3(x) = \frac{\frac{-1}{x-1} - 1}{\frac{-1}{x-1}} = \frac{-1 - (x - 1)}{-1} = x = e(x)$$

$$(g \circ f)(x) = \frac{\frac{1}{x} - 1}{\frac{1}{x}} = \frac{1 - x}{x}$$

$$(g^2 \circ f)(x) = \frac{-1}{\frac{1}{x} - 1} = \frac{-x}{1-x}$$

$$(f \circ g)(x) = \frac{1}{\frac{x-1}{x}} = \frac{x}{x-1} = (g^2 \circ f)(x)$$

So, f has order 2 and g has order 3. So, we can write any composition of functions as $g^i f^j$, where $0 \leq i \leq 2, 0 \leq j \leq 1$. Define φ such that $\varphi(f) = y$ and $\varphi(g) = x$ and $\varphi(g^i f^j) = x^i y^j$. Since $\varphi^{-1}(x^i y^j) = g^i f^j$, then φ is a bijection. Then let $(g^a f^b)(g^c f^d) = g^m f^n$, so then $(x^a y^b)(x^a y^b) = x^m y^n$. Then

$$\varphi((g^a f^b)(g^c f^d)) = \varphi(g^m f^n) = x^m y^n = (x^a y^b)(x^c y^d) = \varphi(g^a f^b)\varphi(g^c f^d)$$

So f and g generates a group G where G is isomorphic to S_3.

(16) Consider groups G and S_3 from the previous exercise. Consider $\tau(f) = x^2 y$ and $\tau(g) = x$, and $\tau(g^i f^j) = x^i (x^2 y)^j$. If $j = 0$, then $\tau(g^i) = x^i$. If $j = 1$, then $\tau(g^i f) = x^i x^2 y = x^{i+2} y$. Since $\tau^{-1}(x^i y^j)$, then $g^i f^j$, then τ is a bijection. Let $(g^a f^b)(g^c f^d) = g^m f^n$, so then $(x^a (x^2 y)^b)(x^a (x^2 y)^b) = x^m (x^2 y)^n$. Then

$$\tau((g^a f^b)(g^c f^d)) = \tau(g^m f^n) = x^m (x^2 y)^n$$

$$= (x^a (x^2 y)^b)(x^a (x^2 y)^b) = \tau(g^a f^b)(g^c f^d)$$

So, τ is an isomorphism. But, $\varphi(f) = y$, but $\tau(f) = x^2 y$. So, $\varphi \neq \tau$. So, there is more than one isomorphism between f and g.

2.4 Homomorphisms

(1) For $x, y \in G$, then for $u, v \in H$ such that $\varphi(x) = u$ and $\varphi(y) = v$, then $\varphi(x \# y) = u \circ v = \varphi(x) \circ \varphi(y)$, so φ is a homomorphism.

(2) Let $k = 2$. Then clearly $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$. Suppose for $k = n - 1$, $\varphi(a_1 ... a_k) = \varphi(a_1) ... \varphi(a_k)$, Then, for $k = n$,

$$\varphi(a_1 ... a_{n-1} a_n) = \varphi((a_1 ... a_{n-1}) a_n) = \varphi(a_1 ... a_{n-1})\varphi(a_n) = \varphi(a_1) ... \varphi(a_n)$$

(3) Let $\varphi : G \to G'$ by a homomorphism.

Let K be the kernel of φ. So for $a \in G$, $\varphi(a) = 1$. Let $a, b \in G$, then $\varphi(ab) = \varphi(a)\varphi(b) = 1$, so $ab \in G$. And $\varphi(1) = 1$ so $1 \in G$. And, $\varphi(a^{-1}) = \varphi(a)^{-1} = 1^{-1} =$, so $a^{-1} \in G$. Thus, K is a subgroup.

Let I be the image of φ. So for $x \in G'$, then for some $a \in G$, $\varphi(a) = x$. Let $x, y \in G'$, where $\varphi(a) = x, \varphi(b) = y$. Then $\varphi(ab) = \varphi(a)\varphi(b) = xy$, so $xy \in I$. And, $\varphi(1) = 1$, so $1 \in I$. And, $\varphi(a^{-1}) = \varphi(a)^{-1} = x^{-1}$, so x^{-1}, then $x^{-1} \in I$. Thus, I is a subgroup.

(4) Let $a, b \in \mathbb{Z}$. Then for a homomorphism φ, then $\varphi(a + b) = \varphi(a) + \varphi(b)$. And, $\varphi(a) = a\varphi(1)$ if $a > 0$, and $\varphi(a) = (-a)\varphi(-1) = a\varphi(1)$ if $a < 0$. So, $\varphi(a) = a\varphi(1)$.

Suppose $\varphi(1) \to 0$. Since $\varphi(a) = 0$ for all a, then φ is neither subjective nor injective.

Suppose $\varphi(1) \to n$, for $n \neq 0$. Then for $a \neq b$, then $\varphi(a) = a\varphi(1) \neq b\varphi(1) = \varphi(b)$. So, φ is injective.

Suppose $\varphi(1) \to k$, where $k = 1$ or -1. Then $\varphi(a) = a\varphi(1) = a$, or $\varphi(a) = -a$, ie. $\varphi(a) = ka$. Define $\varphi^2(a) = a$. So, φ is surjective.

Suppose $k > |1|$. Then, $\varphi(1) = k$. But, there is no inverse map such that $\varphi^{-1}(k) = 1$. Thus, φ is not surjective.

(5) For $a, b \in G$, then

$$\varphi(ab) = (ab)^n = a^n b^n = \varphi(a)\varphi(b)$$

So, φ is a homomorphism.

(6) For $a, b \in \mathbb{R}$, then

$$f(a+b) = e^{i(a+b)} = e^{ia}e^{ib} = f(a)f(b)$$

So, f is a homomorphism.

Let K be the kernel of f. For $x \in K$, then $0 = f(x) = e^{ix}$. But since there is no such x, then $K = \emptyset$.

Let I be the image of f. For $y \in I$, then $y = e^{ix}$ for some x. Since $e^{i2\pi} = e^0$, then $I = \left\{e^{ix}, 0 \leq x < 2\pi\right\}$.

(7) Let $a + bi, c + di \in \mathbb{R}^\times$. Then

$$|(a+bi)(c+di)| = |ac - bd + (ad+bc)i| = \sqrt{(ac-bd)^2 + (ad+bc)^2}$$

$$= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2}$$

$$= \sqrt{a^2(c^2+d^2) + b^2(c^2+d^2)} = \sqrt{a^2+b^2}\sqrt{c^2+d^2} = |a+bi||c+di|$$

Thus, the absolute value map is a homomorphism.

Let K be the kernel of the map. For $x \in K$, then $0 = |a+bi| = \sqrt{a^2+b^2} \to a = b = 0$. So, $K = \{0\}$.

Let I be the image of the map. For $y \in I$, then $y = \sqrt{a^2+b^2}$ for $a + bi \in \mathbb{C}$. Clearly, $y \geq 0$. So, $I = \{x, x \geq 0\}$.

(8) (a)

$$\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}\right\}, \left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}, \begin{bmatrix}&1&\\1&&\\&&1\end{bmatrix}\right\},$$

$$\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}, \begin{bmatrix}&&1\\&1&\\1&&\end{bmatrix}\right\}, \left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}, \begin{bmatrix}1&&\\&&1\\&1&\end{bmatrix}\right\},$$

$$\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix}, \begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix}, \begin{bmatrix}&&1\\1&&\\&1&\end{bmatrix}\right\},$$

$$\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix},\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix},\begin{bmatrix}&&1\\1&&\\&1&\end{bmatrix},\right.$$
$$\left.\begin{bmatrix}&1&\\1&&\\&&1\end{bmatrix},\begin{bmatrix}&&1\\&1&\\1&&\end{bmatrix},\begin{bmatrix}1&&\\&&1\\&1&\end{bmatrix}\right\}$$

Since

$$\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix}\begin{bmatrix}&1&\\1&&\\&&1\end{bmatrix}\begin{bmatrix}&&1\\1&&\\&1&\end{bmatrix}$$
$$=\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix}\begin{bmatrix}1&&\\&&1\\&1&\end{bmatrix}=\begin{bmatrix}&&1\\&1&\\1&&\end{bmatrix}$$

Then

$$\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix},\begin{bmatrix}&1&\\1&&\\&&1\end{bmatrix}\right\}$$

is not normal. Similarly, once can show that

$$\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix},\begin{bmatrix}&&1\\&1&\\1&&\end{bmatrix}\right\},\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix},\begin{bmatrix}1&&\\&&1\\&1&\end{bmatrix}\right\}$$

are also not normal. Furthermore,

$$A_3=\left\{\begin{bmatrix}1&&\\&1&\\&&1\end{bmatrix},\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix},\begin{bmatrix}&&1\\1&&\\&1&\end{bmatrix}\right\}$$

is a normal subgroup of S_3, since A_3 is the kernel of the sign homomorphism. Thus, $\{I\}$, A_3, S_3 are the normal subgroups of S_3.

(b)

$$\{1\},\{1,-1\},\{1,i,-1,-i\},\{1,j,-1,-j\},\{1,k,-1,-k\},$$
$$\{1,-1,i,-i,j,-j,k,-k\}$$

Since $\{1,-1\}$ is the center of the quaternion group, it is also a normal subgroup. Further,

$$(-j)i(j)=-(jij)=-(jk)=i$$
$$=(j)i(-j)=(k)(-i)(-k)=(-k)(-i)(k)$$

And

$$(-k)i(k)=-(kik)=kj=-i$$
$$=(k)i(-k)=(j)(-i)(-j)=(-j)(-i)(j)$$

Thus $\{1,i,-1,i\}$ is normal. Similarly, $\{1,j,-1,-j\}$ and $\{1,k,-1,-k\}$ are normal. Thus all subgroups of the quaternion group are normal.

(9) (a)
$$(\varphi \circ \psi)(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b))$$
$$= \varphi(\psi(a))\varphi(\psi(b)) = (\varphi \circ \psi)(a)(\varphi \circ \psi)(b)$$

(b) Let K_ψ be the kernel of ψ. For $a \in K_\psi$, then $\varphi(\psi(a)) = \varphi(1) = 1$. So, $K_\psi \subseteq K$, where K is the kernel of $\varphi \circ \psi$.
In general, $a \in K$ if $\psi(a) \in K_\varphi$, where K_φ is the kernel of φ.

(10) Suppose $\varphi(x) = \varphi(y)$. Then
$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(x)^{-1} = 1$$
Thus, $xy^{-1} \in \ker \varphi$
Suppose $xy^{-1} \in \ker \varphi$. Then
$$1 = \varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} \to \varphi(y) = \varphi(x)$$

(11) For all i, $\varphi(x^i) = y^i$. If $i = m$, then $\varphi(x^m) = \varphi(1) = 1$. Since $y^m = n$, then, n divides m.

(12) Let
$$X = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}, X' = \begin{bmatrix} A' & B' \\ 0 & D' \end{bmatrix}$$
Observe that $\det X = (\det A)(\det D) \neq 0$, so $X \in GL_r(\mathbb{R})$. And,
$$XX' = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \begin{bmatrix} A' & B' \\ 0 & D' \end{bmatrix} = \begin{bmatrix} AA' & AB' + BD' \\ 0 & DD' \end{bmatrix}$$
Since $AA' \in GL_r(\mathbb{R})$ and $DD' \in GL_{n-r}(\mathbb{R})$, then $XX' \in P$.
Furthermore, trivially $I \in P$. And, let
$$X^{-1} = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix}$$
Then
$$XX^{-1} = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix}$$
$$= \begin{bmatrix} AA^{-1} & -AA^{-1}BD^{-1} + BD^{-1} \\ 0 & DD^{-1} \end{bmatrix} = \begin{bmatrix} I_r & 0 \\ 0 & I_{n-r} \end{bmatrix}$$
And
$$X^{-1}X = \begin{bmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{bmatrix} \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$$
$$= \begin{bmatrix} A^{-1}A & A^{-1}B - A^{-1}BD^{-1}D \\ 0 & D^{-1}D \end{bmatrix} = \begin{bmatrix} I_r & 0 \\ 0 & I_{n-r} \end{bmatrix}$$
Thus, $X^{-1} \in P$. So, P is a subgroup of $GL_n(\mathbb{R})$. Denote φ to be the map sending X to A. Then for $X, X' \in P$, then $\varphi(XX') = AA' = \varphi(X)\varphi(X')$. So, φ is a homomorphism.
The kernel of P is all $X \in P$ such that $A = I_r$.

(13) (a) Let
$$a_1 = gh_1g^{-1}, a_2 = gh_2g^{-1}$$
Then
$$a_1a_2 = gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1}$$
So, $a_1a_2 \in gHg^{-1}$.
Further, $g1g^{-1} = gg^{-1} = 1$, so $1 \in gHg^{-1}$. And, Let $a^{-1} = gh^{-1}g^{-1}$. Then, $aa^{-1} = ghg^{-1}gh^{-1}g^{-1} = ghh^{-1}g^{-1} = gg^{-1} = 1$, and $a^{-1}a = gh^{-1}g^{-1}ghg^{-1} = gh^{-1}hg^{-1} = gg^{-1} = 1$. Thus, gHg^{-1} is a subgroup of G.

(b) Suppose H is normal. Then for all $g \in G$ and for $h \in H$, $ghg^{-1} \in H$. So, $gHg^{-1} \subseteq H$. And, let $a = ghg^{-1}$. Then $h = g^{-1}ag$, so $h \in gHg^{-1}$. Sp $H \subseteq gHg^{-1}$. Thus, $H = gHg^{-1}$.
Suppose for all $g \in G$, $gHg^{-1} = H$. Then, for all $h \in H$, $ghg^{-1} \in H$. Then, H is normal.

(14) Let $a = g^{-1}$. Since N is normal, then $g^{-1}ng = ana^{-1} \in N$

(15) Let $x, y \in H$. Then $\varphi(xy) = \varphi(x)\varphi(y) = \psi(x)\psi(y) = \psi(xy)$. So, $xy \in H$. Further, since $1 = \varphi(1) = \psi(1)$, then $1 \in H$. And, $\varphi(x^{-1}) = \varphi(x)^{-1} = \psi(x)^{-1} = \psi(x^{-1})$. Then, $x^{-1} \in H$. So, H is a subgroup of G.

(16) Since $1 = \varphi(1) = \varphi(x^r) = \varphi(x)^r$, then the order of $\varphi(x)$ divides r.

(17) Let Z be the center of a group G. So for $z \in Z$, then for all $g \in G$, then $zg = gz \to gzg^{-1} = z \in Z$. So, Z is a normal subgroup.

(18) Since for all $A \in GL_n(\mathbb{R})$, $cIA = A(cI)$, then $Z \subseteq Z'$, where Z' is the center of $GL_n(\mathbb{R})$.
Let $z \in Z'$, then $zA = Az \to (zA)_{ij} = (Az)_{ij} \to \sum_{x=1}^{n} z_{ix}A_{xj} = \sum_{y=1}^{n} A_{iy}z_{yj}$. For $x \neq i$, if $A_{xj} = 0$, and for all y, $A_{iy} = 0$, then if $x \neq i$, $z_{ix} = 0$. Similarly, $z_{xi} = 0$. But, if $A_{xj} = A_{iy} = 0$ for all $x \neq i, y \neq j$, then we have $z_{ii}A_{ij} = A_{ij}z_{jj} \to z_{ii} = z_{jj}$. Thus, $Z' \subseteq Z$. Therefore, $Z = Z'$.

(19) Let a be the single element of G with order 2. Consider $a' = bab^{-1}$, where $b \in G$. Since $|a'| = |a| = 2$, then $a' = a$. So $a = bab^{-1} \to ab = ba$. So a is in the center of the group.

(20) (a) Let $A, B \in U$. Clearly, $\det A = \det B = 1$, so $A, B \in SL_3(\mathbb{R})$. And,
$$AB = \begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix}$$
So $AB \in U$. Clearly also, $I \in U$, and let
$$A = \begin{bmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{bmatrix}$$
Then
$$A^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ & 1 & -c \\ & & 1 \end{bmatrix}$$

Since $AA^{-1} = A^{-1}A = I$, and $A^{-1} \in U$, then U is a subgroup if $SL_3(\mathbb{R})$.

(b) Consider

$$B = \begin{bmatrix} 1 & & \\ 1 & 1 & \\ 1 & 1 & 1 \end{bmatrix}$$

Then

$$B^{-1} = \begin{bmatrix} 1 & & \\ -1 & 1 & \\ & -1 & 1 \end{bmatrix}$$

Let

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

Then

$$BAB^{-1} = \begin{bmatrix} 1 & & \\ 1 & 1 & \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ & 1 & 1 \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & & \\ -1 & 1 & \\ & -1 & 1 \end{bmatrix}$$

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

Since $BAB^{-1} \notin U$, then U is a normal subgroup of $SL_3(\mathbb{R})$.

(c) Consider

$$A = \begin{bmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{bmatrix}, X = \begin{bmatrix} 1 & d & e \\ & 1 & f \\ & & 1 \end{bmatrix}$$

If A is in the center of U, then $AX = XA$. So

$$\begin{bmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & d & e \\ & 1 & f \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & d & e \\ & 1 & f \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & a+d & b+e+af \\ & 1 & c+f \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & b+e+cd \\ & 1 & c+f \\ & & 1 \end{bmatrix}$$

So $b + e + af = b + e + cd \rightarrow af = cd$. Since f and d are arbitrary, then $a = c = 0$. So the center of U is matrices of the form:

$$\begin{bmatrix} 1 & & a \\ & 1 & \\ & & 1 \end{bmatrix}$$

(21) Consider

$$A = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & \\ i & 1 \end{bmatrix}, B^{-1} = \begin{bmatrix} 1 & \\ -i & 1 \end{bmatrix}$$

Then

$$BAB^{-1} = \begin{bmatrix} 1 & \\ i & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ -i & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & \\ i & 1 \end{bmatrix} \begin{bmatrix} 1-i & 1 \\ -i & 1 \end{bmatrix} = \begin{bmatrix} 1-i & 1 \\ 1 & i+1 \end{bmatrix}$$

Since $BAB^{-1} \notin GL_2(\mathbb{R})$, then $GL_2(\mathbb{R})$ is not a normal subgroup of $GL_2(\mathbb{C})$.

(22) (a) Suppose $x \in G$ generates G. Let n be the order x. Then for $a = x^i \in G$, for some $i < n$,

$$\varphi(a) = \varphi(x^i) = \varphi(x)^i$$

Since φ is surjective, then

$$\left\{1, \varphi(x), \varphi(x)^2, ..., \varphi(x)^{n-1}\right\} = G'$$

Since $\varphi(x)^n = 1$, then the order of $\varphi(x)$ divides n. Let m be the order of $\varphi(x)$. Then

$$\left\{1, \varphi(x), \varphi(x)^2, ..., \varphi(x)^{m-1}\right\} = G'$$

So G' is a cyclic group generated by $\varphi(x)$.

(b) Let $a', b' \in G'$ such that $\varphi(a) = a', \varphi(b) = b'$ for $a, b \in G$ Then

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a'$$

Thus, G' is abelian.

(23) Let $a, b \in N$ Let $c = ab \in N$. Then $\varphi(c) = \varphi(ab) = \varphi(a)\varphi(b)$. So, $\varphi(a)\varphi(b) \in N$. And, trivially $1 = \varphi(1) \in \varphi(N)$. And, $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(N)$. So, $\varphi(N)$ is a subgroup of G'.

Let $a' = \varphi(a) \in \varphi(N)$. Then for $g' \in G'$ such that $\varphi(g) = g'$ where $c = gag^{-1}$ (so that $c \in N$ and $\varphi(c) \in \varphi(N)$), then

$$\varphi(c) = \varphi(gag^{-1}) = g'a'g'^{-1}$$

Thus, $\varphi(N)$ is a normal subgroup of G'.

2.5 Equivalence Relations and Partitions

(1) Denote φ to be a map. Consider nonempty fibres α, β such that $a \in \alpha \cap \beta$, and: for $x \in \alpha$, $\varphi(x) = X$, and for $y \in \beta$, $\varphi(y) = Y$. So $\varphi(a) = X$, but $\varphi(a) = Y$. Thus, $X = Y$. So, $\alpha = \beta$. Thus, the fibres of φ are disjoint. And, each x is in some fibre of φ. And by definition each fibre of φ is a subset of the domain of φ. Therefore, the fibres of φ form a partition of the domain.

(2) Note that G is isomorphic to itself (via the trivial isomorphism). Thus, $G \sim G$.

Suppose $G \sim H$. Then G is isomorphic to H, through the isomorphism φ. Then φ^{-1} is also an ismorphism, so then H is isomorphic to G, and therefore $H \sim G$.

Suppose $A \sim B$ and $B \sim C$. Then A is isomorphic to B through the isomorphism φ, and B is isomorphic to C through the isomorphism τ. Then for $a, b \in A$, $\tau(\varphi(ab)) = \tau(\varphi(a)\varphi(b)) = \tau(\varphi(a))\tau(\varphi(b))$. And, $\tau \circ \varphi$ is a bijection, so $\tau \circ \varphi$ is an isomorphism. Thus, A is isomorphic to C, and $A \sim C$.

(3) Let $A = \{a, b, c, d, e\}$ be a set of five elements. There are several types of equivalence relations:

- There is one partition of 5 elements. There is one such relation.
- There is one partition of 4 elements, and one of 1 element. There are 5 such relations.
- There is one partition of 3 elements, and one of 2 elements. There are 10 such relations.
- There is one partition of 3 elements, and two of 1 element. There are 10 such relations.
- There are 2 partitions of 2 elements, and one of 1 element. There are 15 such relations.
- There is 1 partition of 2 elements, and three of 1 element. There are 10 such relations.
- There are 5 partitions of 1 element. There is 1 such relation.

So there are 52 equivalence relations.

(4) Let $A = R \cap R'$. Let $a, b, c \in S$. Since $(a, a) \in R, R'$, then $(a, a) \in A$. If $(a, b) \in R, R'$, then $(b, a) \in R, R'$, and so $(a, b) \in A$. If $(a, b), (b, c) \in R, R'$, then $(a, c) \in R, R'$, so $(a, c) \in A$. Thus, A is an equivalence relation.

Let $B = R \cup R'$. Consider $(a, b) \in R$ and $(b, c) \in R'$. But, $(a, c) \notin R$, and $(a, c) \notin R'$. So $(a, c) \notin B$. So B is not an equivalence relation.

(5) Let $a, b, c \in H$. Since $a^{-1}a = 1 \in H$, then $a \sim a$. Suppose $a \sim b$. Then $b^{-1}a \in H \rightarrow a^{-1}b \in H$, so $b \sim a$. Suppose $a \sim b$ and $b \sim c$. Then $b^{-1}a \in H$ and $c^{-1}b \in H$, so $c^{-1}bb^{-1}a = c^{-1}a \in H$. So $a \sim c$. Thus, $a \sim b$ is an equivalence relation.

(6) (a) Let $a, b, c \in G$. Since $1a1^{-1} = a$, then $a \sim a$. Suppose $a \sim b$. Then for some x, $xax^{-1} = b \rightarrow a = x^{-1}bx = (x^{-1})^{-1}bx^{-1}$, so $b \sim a$. Suppose $a \sim b$ and $b \sim c$. Then for some x, y, $xax^{-1} = b$ and $yby^{-1} = c$. Then $c = yxax^{-1}y^{-1} = yxa(yx)^{-1}$. So $a \sim c$.

(b) If a's conjugacy class consists only of a, then for all b, $bab^{-1} = a \rightarrow ba = ab$. So, a is a member of the center of G.

(7) According to the reflexive property, $(x, x) \in R$. This corresponds to the line $y = x$.

According to the symmetric property, if $(x, y) \in R$, then $(y, x) \in R$. Note that if (x, y) is reflected across the line $y = x$, then we have (y, x). So, R includes the line $y = x$, and is symmetric about $y = x$.

(8) (a) Let $a \in \mathbb{R}$. Clearly, $(a, a) \in R$, so R is reflexive.
Let $(a, b) \in \mathbb{R}$. Then $a = b$. So, $(b, a) \in \mathbb{R}$. So R is symmetric.
Let $(a, b), (b, c) \in \mathbb{R}$. Then $a = b = c$. So $(a, c \in \mathbb{R}$. So R is transitive.
Thus R is an equivalence relation.

(b) R is not reflexive, since for $x \in \mathbb{R}$, $(x, x) \notin R$.
R is symmetric, since $(a, b) \notin R$ for $a, b \in \mathbb{R}$.
R is transitive, since $(a, b) \notin R$ for $a, b \in \mathbb{R}$.

(c) R is not reflexive, since $(1, 1) \notin R$.
R is not symmetric, since $(1, 0) \in R$, bit $(0, 1) \notin R$.
Let $(a, b), (b, c) \in R$. Since $b = c = 0$, then $(a, c) = (a, 0) \in R$. So, R is transitive.

(d) R is not reflexive, since $(0,0) \notin R$.

Suppose $(a,b) \in R$. Then $ab+1=0 \to ba+1=0$, so $(b,a) \in R$, and R is symmetric.

Let $a=1, b=-1, c=1$. Then $ab+1=bc+1=0$, so $(a,b),(b,c) \in R$. But $ac+1=2$, so $(a,c) \notin R$. So R is not transitive.

(e) Let $x \in \mathbb{R}$. Then $x^2x - xx^2 - x + x = 0$, so $(x,x) \in R$. So R is reflexive.

Let $(x,y) \in R$. Then $x^2y-xy^2-x+y=0 \to 0=-(x^2y-xy^2-x+y)=y^2x-yx^2-y+x$. Therefore, $(y,x) \in R$, and R is symmetric.

Let $(a,b),(b,c) \in R$. Fixing b, we know that $a^2b-ab^2-a+b=0$ has two possible solutions for a, one of which is b. And, $c^2b-bc^2-b+c=0$ again has two solutions: in fact they have the same solutions. Suppose $a=b$. Then trivially, $(a,c)=(b,c) \in R$ Similarly, if $c=b$, then $(a,c)=(a,b) \in R$. If $a \neq b$ and $c \neq b$, then $a=c$. So, $(a,c)=(a,a) \in R$ from reflexivity. Thus, R is transitive.

Thus R is an equivalence relation.

(f) Let $x \in \mathbb{R}$. Then $x^2 - xx + 2x - 2x = 0$. So R is reflexive.

Let $a=-2, b=0$. Then $a^2-ab+2a-2b=4-0-4-0=0$ So $(-2,0) \in R$. But $b^2-ba+2b-2a=0-0+0-2(-2)=4 \neq 0$. So $(b,a) \notin R$. So R is not symmetric.

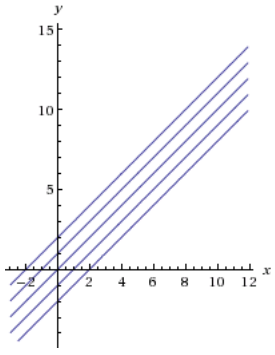
Let $(a,b),(b,c) \in R$. So $a^2-ab+2a-2b=(a+2)(a-b)=0$. So, either $a=-2$, or $a=b$. If $a=b$, then $(a,c)=(b,c) \in R$. If $a=-2$, then since c is arbitrary, then $(a,c) \in R$. So R is transitive.

(9) Suppose R is the set of all points that satisfies $0=\prod_{i=-\infty}^{\infty}(x-y-i)$

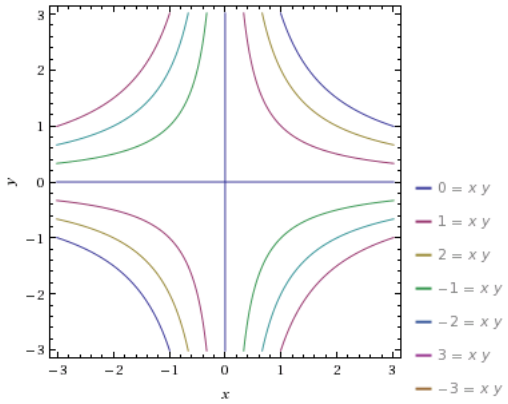
Then, for all $x \in \mathbb{R}$, $(x,x) \in R$, so R is reflexive.

For $(a,b) \in R$, then $0=\prod_{i=-\infty}^{\infty}(a-b-i)=\prod_{i=-\infty}^{\infty}(b-a-i)$, so $(b,a) \in R$. So R is symmetric.

Let $(a,b),(b,c) \in R$. If $a=b$, then $(a,c) \in R$. Similarly, if $b=c$, then $(a,c) \in R$. Suppose $a \neq b$ and $b \neq c$. Let $a-b-j=b-c-k=0$, for some k. Then $a-c-(j+k)=0$. So, $(a,c) \in R$. So R is transitive.



(10) Graph:



(11)

$$\overline{0} + \overline{0} = \overline{1} + \overline{1} = \overline{0}$$
$$\overline{1} + \overline{0} = \overline{1}$$
$$\overline{0} \cdot \overline{0} = \overline{0} \cdot \overline{1} = \overline{0}$$
$$\overline{1} \cdot \overline{1} = \overline{1}$$

Note that the commutative, associative, and distributive properties of addition and multiplication hold as well.

(12) Consider the coset aN and the fiber of φ on a, $\varphi^{-1}(a)$. Consider $g \in \varphi^{-1}(a)$, ie. g is a member of the fiber of φ on a. Then $\varphi(g) = \varphi(a)$. So $g \in aN$, and $\varphi^{-1}(a) \subseteq aN$. And, if $g \in aN$, then by definition $\varphi(g) = \varphi(a)$, so $g \in \varphi^{-1}(a)$. And $aN \subseteq \varphi^{-1}(a)$. Thus, $aN = \varphi^{-1}(a)$. Therefore the cosets are precisely the fibres of φ.

2.6 Cosets

(1) Consider $a \in \mathbb{Z}$, $hn \in n\mathbb{Z}$. Let $b = a + hn$. Using the division algorithm, we can write a as $qn + r$, for $r < n$. So $b = (q + h)n + r$. Let $b_1 = (q_1 + h)n + r_1$, $b_2 = (q_2 + h)n + r_2$. b_1, b_2 are in the same coset if and only if $r_1 = r_2$. Since there are n possible values of r_1 or r_2, then $[\mathbb{Z} : n\mathbb{Z}] = n$.

(2) Consider the left cosets aH and bH. Suppose for some c, $c \in aH$ and $c \in bH$. So $c = ah_1$ and $c = bh_2$, for $h_1, h_2 \in H$. So $ah_1 = bh_2 \to a = bh_2h_1^{-1}$. So $a \in bH$, ie. $a = bh_b = h_2h_1^{-1}$. So for $x \in aH$, then $x = ah_a = bh_2h_1^{-1}h_a \to x \in bH$. Thus, $aH \subseteq bH$. Similarly, $bH \subset aH$, so $aH = bH$. Thus, if $aH \neq bH$, then $aH \cap bH = \emptyset$.

Similarly, we can show all distinct right cosets do not overlap.

(3) Suppose G has order p^n, for $n \geq 1$. If $n = 1$, then G is a cyclic group of order p, so for some a, a generates G, and $a^p = 1$.

Suppose the statement is true for all $n \leq k - 1$. Then if $n = k$, for some $a \in G$, where $a \neq 1$, then a generates some subgroup $H = \{1, a, a^2, ..., a^{x-1}\}$, where x is the order of a. From the Counting Theorem, $|H|$ divides $|G|$, ie. $|H|$ is a power of p. If $|H| = p^n$, then $|a| = p^n$. So,

$|a^{p^{n-1}}| = p$. If $|H| = p^i$, where $i < n$, then by the inductive hypothesis, the statement is true for H, and thus also for G.

(4) Consider

$$H_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, H_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in GL_2(\mathbb{R}), A = \begin{bmatrix} i & i \\ & 1 \end{bmatrix} \in GL_2(\mathbb{C})$$

Then

$$H_1 A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} 1 & i \\ & 1 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 + a_1 i \\ c_1 & d_1 + c_1 i \end{bmatrix}$$

And

$$AH_2 = \begin{bmatrix} 1 & i \\ & 1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_2 + c_2 i & b_2 + d_2 i \\ c_2 & d_2 \end{bmatrix}$$

For $c_2 \neq 0$, then $AH_2 \neq H_1 A$. Thus the left and right cosets are different.

(5) Since 3 and 5 are prime, then for some $h \neq 1 \in H$ and $k \neq 1 \in K$, then $H = \{1, h, h^2\}$, and $K = \{1, k, k^2, k^3, k^4\}$. Suppose for some $0 \leq i < 5$, $h = k^i$. Then $1 = k^{3i} \to i = 0 \to h = 1$, a contradiction The suppose for some $0 \leq j < 5$, then $h^2 = k^j$. Then $1 = k^{3j} \to j = 0 \to h^2 = 1$, a contradiction. So, $H \cap K = \{1\}$

(6) From (5.13), the left cosets of $\ker \varphi$ are the fibres of φ. Let τ map fibres of φ onto im . Let $A, B \in \text{im } \varphi$, and $\varphi^{-1}(A), \varphi^{-1}(B)$ be fibres of φ on A and B respectively, where $A \neq B$. That is, $\tau(\varphi^{-1}(A)) = A$, and $\tau(\varphi^{-1}(B)) = B$. For $a \in \varphi^{-1}(A), b \in \varphi^{-1}(B)$, then clearly $a \neq b$, and so $\varphi(a) = A, \varphi(b) = B$. So τ is injective. And since φ is surjective onto im φ by definition, then τ is surjective. Thus, τ is a bijection. So, $[G : \ker G] = |\text{im } \varphi|$. Thus by the Counting Theorem, $|G| = |\ker \varphi|[G : \ker G] = |\ker \varphi| \cdot |\text{im } \varphi|$.

(7) (a) Let $a, b \in G$. Then $\varphi(ab) = (ab)^2 = a^2 b^2 = \varphi(a)\varphi(b)$. So φ is a homomorphism.

Let H be the subgroup generated by x. Since $|H|$ divides $|G|$, and $|G|$ is odd, then $|x| = |H| = 2k+1$ is odd. Let $\tau(x) = x^{k+1}$. Then $\varphi(\tau(x)) = \tau(\varphi(x)) = x^{2(k+1)} = x$. So, φ is a bijection. Thus, φ is an automorphism.

(b) Claim: Let G be an abelian group. Consider r, where $gcd(r, |G|) = 1$, ie. r is relatively prime to $|G|$. Then $\varphi(x) = x^r$ is an automorphism.

Let $a, b \in G$. Then $\varphi(ab) = (ab)^2 = a^2 b^2 = \varphi(a)\varphi(b)$. So φ is a homomorphism.

Let H be the subgroup generated by x. Since $|H|$ divides $|G|$, and $|G|$ is relatively prime with r, then $|x| = |H|$ is also relatively prime with r. Write $1 = cr + d|H|$ for some c, d. Let $\tau(x) = x^c$. Then $\varphi(\tau(x)) = \tau(\varphi(x)) = x^{cr} = x^{1-d|H|} = x$. So, φ is a bijection. Thus, φ is an automorphism.

(8) Consider the coset $x + W$, where $Ax = B$. If $y \in x + W$, then $y = x + w$, where $w \in W$. Then $Ay = A(x + w) = Ax + Aw = B$. So, y is a solution to $AX = B$.

Consider y such that $Ay = B$. Then $B = B + 0 = Ay + Aw = A(y + w)$, where $w \in W$. So $y + w \in x + W$.

Therefore, the solutions of $AX = B$ forms a coset.

(9) (a) Suppose $|G|$ is finite. Then $[G : H]$ is also finite. So there are a finite number of left cosets: $a_1H, a_2H, ..., a_nH$. Let $x \in a_iH \to x = a_ih$. Then $a_i^{-1}x = h \to x^{-1}a_i = h^{-1} \to x^{-1} = h^{-1}a_i \to x^{-1} \in Ha_i^{-1}$. So there is a 1:1 correspondence between a_iH and Ha_i^{-1}. Thus there are n right cosets.

(b) Consider the cosets aH and Ha^{-1}. Define φ as $\varphi(aH) = Ha^{-1}$. Note that if $aH = bH$, then for $h_a, h_b \in H$, $ah_a = bh_b \to b^{-1}a \in H \to b^{-1}(a^{-1})^{-1} \in H \to b^{-1}(a^{-1})^{-1} = h_1h_2 \to h_1^{-1}b^{-1} = h_2a^{-1} \to Ha^{-1} = Hb^{-1}$. So φ is well defined. Define $\varphi^{-1}(Ha) = a^{-1}H$ Note that $\varphi^{-1}(\varphi(aH)) = aH$, and $\varphi(\varphi^{-1}(Ha)) = Ha$, so there is a bijective correspondence between left and right cosets. Thus the number of left and right cosets are equal.

(10) (a) Consider the two left cosets aH and bH. I claim that $aH = Ha$, and $bH = Hb$. Suppose for $ah_1 \in aH$, that $ah_1 \in Hb$. Then for some h_2, $ah_1 = h_2b \to ah_1h_2^{-1} \in b$. So $b \in aH$. But $b \in bH$, and $aH \cap bH = \emptyset$ Thus, $ah_1 \notin Hb$. Then $ah_1 \in Ha$. Similarly, for $h_1a \in Ha$, then $h_1a \in aH$. Thus, $aH = Ha$. We can similarly show that $bH = Hb$. Therefore, H is normal.

(b) Consider the subgroup $H = \{1, xy\}$ of S_3. Then H has index 3: the left cosets are $H = \{1, xy\}, xH = \{x, x^2y\}, yH = \{y, x^2y\}$. But the right cosets are $H = \{1, xy\}, Hx = \{x, y\}, Hx^2 = \{x^2, x^2y\}$. Since the left and right cosets do not correspond, then H is not normal.

(11) (a) If G contains an element x of order 6, then G is a cyclic group generated by x.

Define $\varphi(x^n) = n \in 6\mathbb{Z}$. Then $\varphi(x) = 1$, so φ is a homomorphism. And, let $\tau(n) = x^n$. Then $\varphi(\tau(n)) = 1$, and $\tau(\varphi(x^n)) = x^n$. So, φ is a bijection, and is therefore an isomorphism. Thus, $G \simeq 6Z$

(b) Suppose G is abelian, ie. $xy = yx$. Let x be of order 3. y is of order 2 or 3. If y is of order 3, then $J = \{1, y, y^2\}$ is a subgroup of G. Note that $y \in H$ (otherwise $H + J = \{1, x, x^2, y, y^2\}$, so $1 \neq a \notin H + J$ has order 1, a contradiction), so $H = J$. Thus there exists some y such that y has order 2. Then 6 is the order of xy, a contradiction. So G is not abelian.

Let a have order 3 and b have order 2. Then $\varphi(a^ib^j) = x^ib^j$. Thus is clearly an isomophism. Thus $G \simeq S_3$.

(c) Suppose all elements of G have order 1 or 2. Let $x, y \in G$. Then $(xy)^2 = y^2 = 1$. Then $xy = yx$. So G is abelian. But, for distinct x, y, z, then $1, x, y, z, xy, yz, xz$ are all distinct. Thus G does not exist.

(12) Let

$$A = \begin{bmatrix} a_1 & a_2 \\ 0 & 1 \end{bmatrix}$$

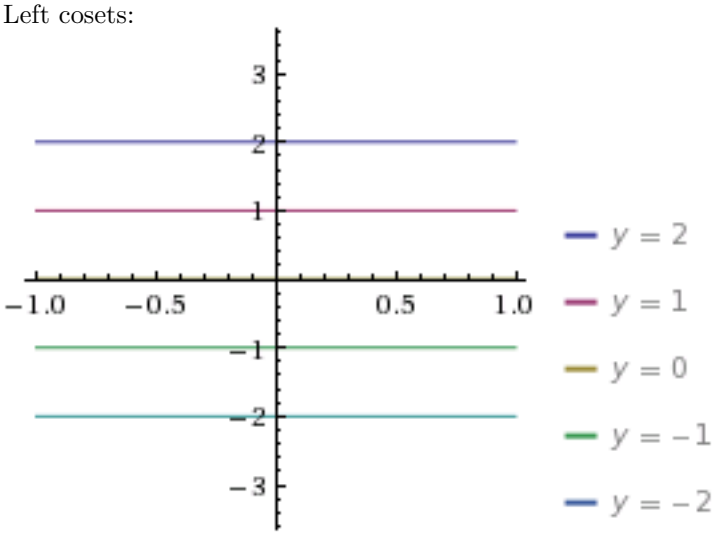
Then

$$AH = \begin{bmatrix} a_1 & a_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} xa_1 & a_2 \\ 0 & 1 \end{bmatrix}$$

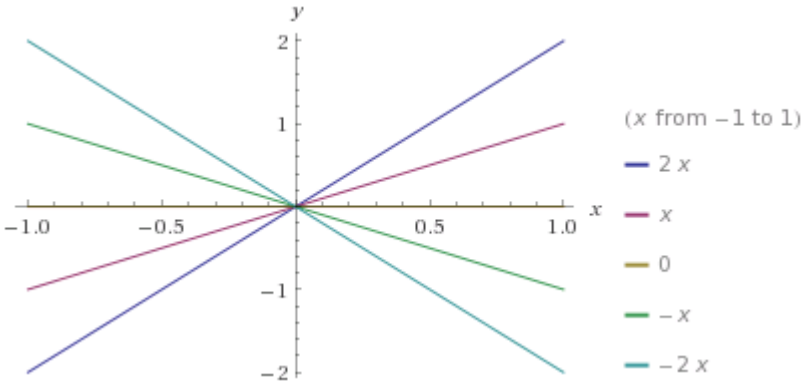
And

$$HA = \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} xa_1 & xa_2 \\ 0 & 1 \end{bmatrix}$$

Left cosets:



Right cosets:



2.7 Restriction of a Homomorphism to a Subgroup

(1) $|\text{im } \varphi|$ divides both G and G', so since $|G|$ and $|G'|$ have no common factors, then $|\text{im } \varphi| = 1$. Since $\varphi(1) = 1$, then for all x, $\varphi(x) = 1$.

(2) Consider S_4. Consider

$$A = \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{bmatrix}, B = \begin{bmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{bmatrix}$$

Note that $A^2 = B^2 = I_4$, and $\det A = -1$ and $\det B = 1$.

(3) (a) First, consider H to be a nontrivial subgroup. Then for some x, y, $xH \neq yH$. Then $xH \cap yH = \emptyset$.

Now consider arbitrary subgroups H and K. Suppose $xH \cap yK$ is nonempty. Then there exists some $a \in xH \cap yK$, where for some $h \in H, k \in K$, $xh = yk$. So, $aH = xH$ and $aK = yK$. So $xH \cap yK = aH \cap aK$. So $z \in aH \cap aK \to z \in aH, aK \to a^{-1}z \in H \cap K \to z \in a(H \cap K)$.

(b) Suppose $[G : H]$ and $[G : K]$ are finite. Then for $a \in G$, then $a(H \cap K) = aH \cap aK$. Since there are finite aH and aK, then there is finite $aH \cap aK$. So $[G : H \cap K]$ is finite.

(4) Let $a, b \in K \cap H$. Then $ab \in H$, and $ab \in K$, so $ab \in K \cap H$. And, $1 \in K \cap H$. And, if $a \in K \cap H$, then $a \in K$ and $a \in H$, so $a^{-1} \in K$ and $a^{-1} \in H$, so $a^{-1} \in K \cap H$. So, $K \cap H$ is a subgroup of both H and K.

Suppose K is a normal subgroup of G. Then for $g \in G, k \in K$, then $gkg^{-1} = k' \in K$. Consider $k' \in K \cap H$. Then for $a, h \in H$, $hk'h^{-1} \in H, K$. Thus, $H \cap K$ is a normal subgroup of H.

(5) Let $x \in HN$. Then for $h \in H, n \in N$, $x = hn$. Suppose $hnh^{-1} = n'$, for some $n' \in N$. Then $n = h^{-1}n'h$, so $x = hh^{-1}n'h = n'h \to x \in NH$. So $HN \subseteq NH$. Similarly, $NH \subseteq HN$. So $HN = NH$.

Let $h_1n_1, h_2n_2 \in HN$. Then for some $n' \in N, h' \in H$, $h_1n_1h_2n_2 = h_1h'n'n_2 \in HN$. And, $1 \in HN$. And, let $hn \in HN$. Note that $n^{-1}h^{-1} \in HN$, and $hnn^{-1}h^{-1} = 1$, so $(hn)^{-1} \in HN$. So HN is a subgroup.

(6) Let $kh \in KH$. Then $\varphi(kh) = \varphi(k)\varphi(h)$, so $kh \in \varphi^{-1}(\varphi(H))$. And, let $x \in \varphi^{-1}(\varphi(H))$. Then for some $h \in H$, $\varphi(x) = \varphi(h)$. For $k \in K$, $\varphi(x) = \varphi(kh) \to x \in KH$. Thus $KH = \varphi^{-1}(\varphi(H))$.

(7) Consider two subgroups A and B of order 5. Since 5 is prime, then $A \cap B$ is either 1 or 5. Suppose there are at least 8 such subgroups. Suppose for any two subgroups A, B, $|A \cap B| = 1$, ie. $A \cap B = \{1\}$. Then $30 = |G| \geq 8(4) + 1 = 33$. Contradiction. So for some A, B, $A = B$. So, we must have at most 7 distinct subgroups of order 5.

(8) Let $A, B \in G$, where $A \neq B$, and A and B contain N Suppose for sake of contradiction that $\varphi(A) = \varphi(B)$. Without loss of generality assume that there exists some $a \in A$, and $a \notin B$, so $a \notin N$. Then $\varphi(ab) = \varphi(a)\varphi(b) \in \varphi(B)$. Then, for some $b' \in B$, $\varphi(a)\varphi(b) = \varphi(b')$. If $b \in N$, then $\varphi(a) = \varphi(b')$, so $a \in B$. Otherwise, then $1 = \varphi(b'b^{-1}a^{-1}) \to b'b^{-1}a^{-1} \in N \to a \in B$. This is a contradiction. Thus, $\varphi(A) \neq \varphi(B)$, so φ is injective on subgroups of G.

Consider $H' \leq G'$. For $h \in H'$, since φ is surjective, then for some $g \in G$, $\varphi(g) = h$. Define $H = \{g \in G : \varphi(g) \in H'\}$. For $a, b \in H$, then $\varphi(ab) = \varphi(a)\varphi(b) \in H'$. And, $1 \in H$. And, $\varphi(a)^{-1} = \varphi(a^{-1}) \in H' \to a^{-1} \in H$. Thus, H is a group. So φ is surjective on subgroups of G.

Thus, φ is a bijective correspondence.

Normal subgroups corresponding follows from Proposition 7.4.

(9)

$$G \leftrightarrow G', \left\{1, x^6\right\} \leftrightarrow \{1\},$$

$$\left\{1, x^3, x^6, x^9\right\} \leftrightarrow \left\{1, y^3\right\}, \left\{1, x^2, x^4, x^6, x^8, x^{10}\right\} \leftrightarrow \left\{1, y^2, y^4\right\}$$

2.8 Products of Groups

(1) Let $(g, g') \in G \times G'$. There are $|G|$ possible values of g, and $|G'|$ possible values of g'. Then $|G \times G'| = |G||G'|$.

(2) Consider $X = \{1, x, x^2\}$ and $Y = \{1, y\}$. X and Y are nontrivial groups, and $S_3 = XY$.

(3) Let G be a finite cyclic group of order rs, and let R and S be cyclic groups of orders r and s respectively.

Suppose $G \simeq R \times S$. Then there exists an isomorphism $\varphi : G \mapsto R \times S$. Let $g \in G$ and $(a, b) \in R \times S$ such that $\varphi(g) = (a, b)$. Note that $|g| = |(a, b)|$. If g generates G, then $|g| = |(a, b)| = rs \to (a^{rs}, b^{rs}) = 1$. Suppose $c = gcd(r, s) \neq 1$, so $r = cr'$ and $s = cs'$. So $(a, b)^{r's'c} = (a^{r's'c}, b^{r's'c}) = (a^{rs'}, b^{r's}) = (1, 1)$. But since $r's'c < rs$, then $|(a, b)| < rs$. So, φ is not an isomorphism. By contradiction, r, s have no common factor.

Suppose r and s have no common factors. Define $\varphi(g) = (a, b)$, where a, b, g generate R, S, G respectively. Then for $i < rs$, $\varphi(g^i) = (a, b)^i$. So $\varphi(g^i g^j) = \varphi(g^{i+j}) = (a, b)^{i+j} = (a, b)^i (a, b)^j$. So φ is a homomorphism.

Suppose $g^i \neq g^j$, ie. $i \neq j$ where $i, j < rs$. If $\varphi(g^i) = \varphi(g^j)$, then $(a, b)^i = (a, b)^j \to a^i = a^j, b^i = b^j$. If $a^i = a^j$, then r divides both $j - i$. Similarly, if $b^i = b^j$, then s divides both $j - i$. But since $gcd(r, s) = 1$, then this implies rs divides $j - i$. So if $j - i < rs$, then $j = i$. So, φ is injective. And, for m, n, c, d $(a^m, b^n) = (a^{cr+m}, b^{ds+n}) = (a^i, b^i) = \varphi(g^i)$ for some i. So φ is surjective, and thus φ is an isomorphism.

(4) (a) Since G is abelian, then H and K are normal. And, $H \cap K = \{1\}$. Consider $g \in G$. If $g > 0$, then for some $k \in K$, $g = k \to g \in HK$. If $g < 0$, then $g = -k \to g \in HK$. So $G = HK$. Thus, $G \simeq H \times K$.

(b) Let

$$g = \begin{bmatrix} a & b \\ & c \end{bmatrix}, g^{-1} = \begin{bmatrix} a^{-1} & -ba^{-1}c^{-1} \\ & c^{-1} \end{bmatrix}, k = \begin{bmatrix} 1 & d \\ & 1 \end{bmatrix}$$

Then

$$gkg^{-1} = \begin{bmatrix} a & b \\ & c \end{bmatrix} \begin{bmatrix} 1 & d \\ & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & -ba^{-1}c^{-1} \\ & c^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ & c \end{bmatrix} \begin{bmatrix} a^{-1} & dc^{-1} - ba^{-1}c^{-1} \\ & c^{-1} \end{bmatrix} = \begin{bmatrix} 1 & adc^{-1} \\ & 1 \end{bmatrix} \in K$$

And, since H is in the center of G, then H is normal. And, $H \cap K = \{I\}$. And, for $g \in G$, $a \neq 0, b \neq 0$,

$$g = \begin{bmatrix} a & b \\ & c \end{bmatrix} = \begin{bmatrix} a & \\ & c \end{bmatrix} \begin{bmatrix} 1 & a^{-1}b \\ & 1 \end{bmatrix} \in HK$$

So, $HK = G$. So, $G \simeq H \times K$.

(c) Since $C^\times$ is abelian, then H and K are normal. And, $H \cap K = \{1\}$. Consider $a + bi \in C^\times$. Then

$$a + bi = \left(\frac{a}{\sqrt{a^2 + b^2}} + \frac{b}{\sqrt{a^2 + b^2}} i \right) \frac{1}{a^2 + b^2} \in HK$$

So, $HK = G$. So $G \simeq H \times K$.

(5) Suppose (g_1, g_2) generates $G_1 \times G_2$. Then for some i, $(g_1, g_2)^i = (1, g)$, where $g \neq 1$. Since G_1, G_2 are infinite cyclic, then for $g_1^i = 1$, then $i = 0 \to g = 1$. Since no generator then exists, then $G_1 \times G_2$ is not infinite cyclic.

(6) Consider the two groups A, B. Let $(a, b) \in A \times B$ be part of the center of $A \times B$. Then for $(c, d) \in C \times D$, then $(c, d)(a, b) = (a, b)(c, d)$. Then $(ca, db) = (ac, bd) \to ca = ac, db = bd$, so a is part of the center of A, and b is part of the center of B. So, the center of $A \times B$ is part of the product of the centers of A and B.

Let $a \in A$ and $b \in B$ be parts of the centers of A and B. Then for $c \in A, d \in D$, $ac = ca$ and $bd = db$. Then $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$, so (a, b) is part of the center of $A \times B$.

Thus, the product of the centers of A and B is precisely the center of $A \times B$.

(7) (a) Suppose HK is a subgroup. Note for any $kh \in KH$, $(kh)^{-1} = h^{-1}k^{-1} \in HK$, so $KH \subseteq HK$. And, since for h, k, $(hk)^{-1} = k^{-1}h^{-1} \in KH$. So $HK \subseteq KH$. Then $HK = KH$.

Let $HK = KH$. Let $h_1, k_1, h_2k_2 \in HK$. First, note that $k_1h_2 = h_3k_3 \in HK$. Then $h_1k_1h_2k_2 = h_1h_3k_3k_2 \in HK$. And, clearly $1 \in HK$. And, for $hk \in HK$, note that $k^{-1}h^{-1} \in HK$, and $hkk^{-1}h^{-1} = 1$. So, HK is a subgroup.

(b) Consider the subgroups of S_3

$$A = \left\{ \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & & \\ & & 1 \end{bmatrix} \right\}, B = \left\{ \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix} \right\}$$

Then

$$AB = \left\{ \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & & \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix}, \begin{bmatrix} & & 1 \\ 1 & & \\ & 1 & \end{bmatrix} \right\}$$

But

$$BA = \left\{ \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & & \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix}, \begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix} \right\}$$

So $AB \neq BA$.

(8) Let A, B be normal subgroups of orders 3 and 5 respectively. Then $AB \leq G$. And, since $A \cap B = \{1\}$, then AB is isomorphic to $A \times B$. Since $|(a, b)| = 15$, then AB has an element that is order 15.

(9) Suppose $h_1k_1 = h_2k_2$. Then $h_2^{-1}h_1 = k_2k_1^{-1} \in H, K$. Since $H \cap K = \{1\}$, then $h_1 = h_2$ and $k_2 = k_1$. So, $|HK| = ab = |G|$, so $HK = G$.

Let $G = \left\{1, x, ..., x^7\right\}, H = \left\{1, x^4\right\}, K = \left\{1, x^2, x^4, x^6\right\}$. Since $H \times K$ has no elements of order 8, then G is not isomorphic to $H \times K$.

(10) Consider $(x, y)^k$. If $k = lcm(m, n)$, then $(x, y)^k = (1, 1)$. Suppose $i < k$, where $(x, y)^i = (1, 1)$. Then $x^i = y^i = 1$. But i is a multiple of m and n, a contradiction since k is the least such number by definition. Thus, $|(x, y)| = lcm(m, n)$

(11) (a) Since G is abelian, then H and K are normal. And, $H \cap K = \{1\}$. And, since $|H||K| = |G|$ and $HK \leq G$, then $HK = G$. Thus, G is isomorphic to $H \times N$.

(b) Since the left cosets of N correspond to the fibres of φ, then for $g \in G$ we can write $g = hn$, where $h \in H, n \in N$. So, we can define $\tau(g) = (h, n)$. Clearly, τ is a bijection. Consider S_3 and the subgroup $A = \{1, y\}$, where $\varphi : S_3 \to S_3 \times A$ is a bijection:

$$\varphi(1) = (1,1), \varphi(y) = (y,1), \varphi(x) = (1,x),$$
$$\varphi(x^2) = (1,x^2), \varphi(yx) = (y,x), \varphi(yx^2) = (y,x^2)$$

And

$$\varphi(yxyx^2) = \varphi(yyx^2x^2) = \varphi(x) = (1,x)$$

But

$$\varphi(yx)\varphi(yx^2) = (y,x)(y,x^2) = (1,1) \neq \varphi(x)$$

Thus φ is not an isomorphism.

2.9 Modular Arithmetic

(1)

$$(7+14)(3-16) \equiv (21)(-13) \equiv (4)(4) \equiv 16 \mod 17$$

(2) (a)

$$0^2 \equiv 0 \mod 4$$
$$1^2 \equiv 1 \mod 4$$
$$2^2 \equiv 4 \equiv 0 \mod 4$$
$$3^2 \equiv 9 \equiv 1 \mod 4$$

So $a^2 \mod 4$ is always either 0 or 1.

(b)

$$0^2 \equiv 0 \mod 8$$
$$1^2 \equiv 1 \mod 8$$
$$2^2 \equiv 4 \mod 8$$
$$3^2 \equiv 9 \equiv 1 \mod 8$$
$$4^2 \equiv 16 \equiv 0 \mod 8$$
$$5^2 \equiv 25 \equiv 1 \mod 8$$
$$6^2 \equiv 36 \equiv 4 \mod 8$$
$$7^2 \equiv 49 \equiv 1 \mod 8$$

So $a^2 \mod 8$ is always either 0, 1, or 4.

(3) (a)

$$(0)(2) \equiv 0 \mod 6$$
$$(1)(2) \equiv 2 \mod 6$$
$$(2)(2) \equiv 4 \mod 6$$
$$(3)(2) \equiv 6 \equiv 0 \mod 6$$
$$(4)(2) \equiv 8 \equiv 2 \mod 6$$
$$(5)(2) \equiv 10 \equiv 4 \mod 6$$

So, 2 has no inverse modulo 6.

(b) Suppose a is the inverse of 2 modulo n. Then for some $b \in \mathbb{Z}$,

$$1 = 2a + bn \rightarrow n = (1 - 2a)b^{-1}$$

Since $1 - 2a$ is not even, then n is odd.

(4) Note that $(10)^i \equiv 1^i \equiv 1 \mod 9$. So,

$$a = d_0 + 10d_1 + ... + 10^n d_n \equiv d_0 + d_1 + ... + d_n \mod 9$$

(5) (a)

$$x = 2^{-1}5 \equiv (5)(5) \equiv 7 \mod 9$$

(b)

$$2x \equiv 5$$

has no solution modulo 6, since the possible values of $2x$ are $0, 2, 4$ modulo 6.

(6) For all n, $x + y \equiv 2$ has a solution: $x = y = 1$. Note if $n = 1$, then $0 \equiv 1 \equiv 2$ modulo n, so the statement is trivially true.

If $2x - 3y \equiv 3 \mod n$, then $2x - 3y - 3$ divides n. If $x = 0, y = -1$, then $2x - 3y - 3 = 0$. 0 divides all integers, so the statement has a solution for all n.

(7)

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = ((a + cn)(b + dn))(c + en)$$
$$= (a + cn)((b + dn)(c + en)) = \overline{a} \cdot (\overline{b} \cdot \overline{c})$$

$$\overline{a} \cdot \overline{b} = (a + cn)(b + dn) = (b + dn)(a + cn) = \overline{b} \cdot \overline{a}$$

(8) From Proposition 2.6, $1 = an + bm$. Then

$$1 \equiv an + bm \mod m \rightarrow 1 \equiv an \mod m$$

Since $gcd(n, m) = 1$, then $n^{-1} \equiv a \mod m$.

Similarly, $m^{-1} \equiv b \mod n$.

2.10 Quotient Groups

(1) Let

$$G = \begin{bmatrix} b & c \\ & d \end{bmatrix} \to G^{-1} = \begin{bmatrix} 1/b & -c/(bd) \\ & 1/d \end{bmatrix}$$

(a)

$$GAG^{-1} = \begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} 1 & a_{12} \\ & a_{22} \end{bmatrix} \begin{bmatrix} 1/b & -c/(bd) \\ & 1/d \end{bmatrix}$$

$$= \begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} 1/b & -c/(bd) + a_{12}/d \\ & a_{22}/d \end{bmatrix} = \begin{bmatrix} 1 & -c/d + a_{12}b/d + ca_{22}/d \\ & a_{22} \end{bmatrix}$$

So $a_{11} = 1$ describes a normal subgroup H of G. Define

$$\varphi(B) = \varphi\left(\begin{bmatrix} a_{11} & a_{12} \\ & a_{22} \end{bmatrix}\right) = a_{11} \in \mathbb{R}^\times$$

Clearly, φ is a surjective homomorphism, and $H = \ker \varphi$. So, $G/H \simeq \mathbb{R}^\times$.

(b)

$$GAG^{-1} = \begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} a_{11} & \\ & a_{22} \end{bmatrix} \begin{bmatrix} 1/b & -c/(bd) \\ & 1/d \end{bmatrix}$$

$$= \begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} a_{11}/b & -a_{11}c/(bd) \\ & a_{22}/d \end{bmatrix} = \begin{bmatrix} a_{11} & -a_{11}c/d + a_{22}c/d \\ & a_{22} \end{bmatrix}$$

So if $a_{11} = 1, a_{22} = 2$, $c = d$, then

$$GAG^{-1} = \begin{bmatrix} 1 & 1 \\ & 2 \end{bmatrix} \notin H$$

So, $a_{12} = 0$ does not describe a normal subgroup of G.

(c)

$$GAG^{-1} = \begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ & a_{11} \end{bmatrix} \begin{bmatrix} 1/b & -c/(bd) \\ & 1/d \end{bmatrix}$$

$$= \begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} a_{11}/b & -ca_{11}/(bd) + a_{12}/d \\ & a_{11}/d \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12}b/d \\ & a_{11} \end{bmatrix}$$

So $a_{11} = a_{22}$ defines a subgroup H of G. Define

$$\varphi\left(\begin{bmatrix} a_{11} & a_{12} \\ & a_{22} \end{bmatrix}\right) = a_{11}a_{22}^{-1} \in \mathbb{R}^\times$$

Clearly, φ is a surjective homomorphism, and $H = \ker \varphi$. So, $G/H \simeq \mathbb{R}^\times$.

(d)

$$GAG^{-1} = \begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} 1 & a_{12} \\ & 1 \end{bmatrix} \begin{bmatrix} 1/b & -c/(bd) \\ & 1/d \end{bmatrix}$$

$$\begin{bmatrix} b & c \\ & d \end{bmatrix} \begin{bmatrix} 1/b & -c/(bd) + a_{12}/d \\ & 1/d \end{bmatrix} = \begin{bmatrix} 1 & -c/d + ba_{12}/d + c/d \\ & 1 \end{bmatrix}$$

So $a_{11} = a_{22} = 1$ describes a normal subgroup H of G. Define

$$\varphi\left(\begin{bmatrix} a_{11} & a_{12} \\ & a_{22} \end{bmatrix}\right) = (a_{11}, a_{22}) \in \mathbb{R}^\times \times \mathbb{R}^\times$$

Clearly, φ is a surjective homomorphism, and $H = \ker \varphi$. So, $G/H \simeq \mathbb{R}^\times \times \mathbb{R}^\times$.

(2) Let $an_1 \in aN, bn_2 \in bN$. Note first that for some $n_3 \in N$, $n_1 b = bn_3$, since N is normal. Then

$$an_1 bn_2 = abn_3 n_2 \in abN$$

And, let $abn \in abN$. Note that for some $m \in N$, $bn = mb$. So,

$$abn = amb = amb1 \in (aN)(bN)$$

So, $(aN)(bN) = abN$.

(3) Consider $AN = B$. Since $a \in AN$, and $a \in NA$, then $AN = NA$. So, N is normal, and since A is arbitrary, and the cosets of N form a partition, then the cosets of N is clearly P.

(4) (a)

$$(1H)(xH) = \left\{x, x^2, xy, x^2y\right\}$$

$$(1H)(x^2H) = \left\{x, x^2, xy, x^2y\right\}$$

Note that $xy \in xH$, but $xH = \{x, xy\}$, so $(1H)(xH)$ and $(1H)(x^2H)$ are not cosets.

(b) Let G be a cyclic group of order 6 with generator g. Let $x = g^2$ and $y = g^3$. Then $x^3 = 1, y^2 = 1, xy = yx$. And, $g = x^2y, g^4 = x^2, g^5 = xy$, so x, y generate G.

(c)

$$(1H)(xH) = \{x, xy\} = xH$$

$$(1H)(x^2H) = \left\{x^2, x^2y\right\} = x^2H$$

The generators from part b) describe an abelian group, so H is a normal subgroup, whereas in part (a) H was not a normal subgroup, so 10.1 did not hold.

(5) Define $\varphi(a) = \operatorname{sgn} a$. Clearly, φ is a surjective homomorphism. And, $P = \ker \varphi$. So, $\mathbb{R}^\times \simeq \operatorname{sgn} a$.

(6)

$$(a + bi)H = \{a + bi, -a - bi, -b + ai, b - ai\}$$

Note that $(a + bi)H = (-a - bi)H = (-b + ai)H = (b - ai)H$.

Define

$$\varphi(a + bi) = (a + bi)^4$$

Clearly, φ is a surjective homomorphism. And, $\ker \varphi = H$. So, $G/H \simeq G$.

(7) All subgroups of H are normal: let N be a subgroup of H. Then for $h \in H$, $n \in N$,

$$hnh^{-1} = h(-h^{-1}n) = -hh^{-1}n = -n = n^{-1} \in N$$

If $N = H$ or $N = \{1\}$, then $N/H = N$.

Let $N = \{1, -1\}$. Define $\varphi(\pm i) = (1, -1), \varphi(\pm j) = (-1, 1), \varphi(\pm k) = (-1, -1), \varphi(\pm 1) = (1, 1)$. Clearly, φ is surjective onto $(\pm 1, \pm 1) \simeq V_4$. And, $\varphi(ab) = \varphi(a)\varphi(b)$, so φ is a homomorphism. And, $\ker \varphi = N$. Thus, $H/N \simeq V_4$.

Let $N = \{1, -1, i, -i\}$. Define $\varphi(a)$ as folllows: if $a \in N$, then $\varphi(a) = 1$, otherwise $\varphi(a) = -1$. If $a, b \in N$ or $a, b \notin N$, then $\varphi(ab) = 1$. Otherwise, $\varphi(ab) = -1$. So φ is an isomorphism, and is surjective onto $\{1, -1\}$. And, $\ker \varphi = N$. Thus, $H/N \simeq \{1, -1\}$.

(8) Let $g \in G, h \in H$. Then $\det(ghg^{-1}) = \det(g)\det(h)\det(g^{-1}) = \det(h)\det(g)\det(g)^{-1} = \det h > 0$. So, H is a normal subgroup.

Define $\varphi(g) = \operatorname{sgn}(\det(g))$. For $a, b \in G$, then $\varphi(ab) = \operatorname{sgn}(\det(ab)) = \operatorname{sgn}(\det(a)\det(b)) = \operatorname{sgn}(\det(a))\operatorname{sgn}(\det(b)) = \varphi(a)\varphi(b)$. So φ is a homomorphism, and it is surjective onto $\{1, -1\}$. And, $\ker \varphi = H$. Thus, $G/H \simeq \{1, -1\}$.

(9) Let $(g, g') \in G \times G'$, and $(h, 1) \in G \times 1$. Then $(g, g')(h, 1)(g, g')^{-1} = (ghg^{-1}, 1) \in G \times 1$. So $G \times 1$ is a normal subgroup of $G \times G'$. And, define $\varphi((h, 1)) = h$. Clearly, φ is a bijection, and $\varphi((h_1, 1)(h_2, 1)) = \varphi((h_1h_2, 1)) = h_1h_2 = \varphi((h_1, 1))\varphi((h_2, 1))$. So, $G \times 1 \simeq G$. And, define $\tau((g, g')) = g'$. Clearly, τ is surjective. And, $\tau((g_1, g_1')(g_2, g_2')) = \tau((g_1g_2, g_1'g_2')) = g_1'g_2' = \tau((g_1, g_1'))\tau((g_2, g_2'))$. And, $\ker \tau = G \times 1$. Thus, $(G \times G')/(G \times 1) \simeq G'$.

(10) Define $\varphi(a + bi) = \frac{1}{\sqrt{a^2+b^2}}(a + bi)$. Then for $a + bi, c = di$,

$$\varphi((a + bi)(c + di)) = \varphi(ac - bd + (ad + bc)i)$$

$$= \frac{ac - bd + (ad + bc)i}{\sqrt{(ac - bd)^2 + (ad + bc)^2}} = \frac{ac - bd + (ad + bc)i}{\sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2}}$$

$$= \frac{(a + bi)(c + di)}{\sqrt{(a^2 + b^2)(c^2 + d^2)}} = \varphi(a + bi)\varphi(c + di)$$

So, φ is a homomorphism, and it is surjective onto U. And, $\ker \varphi = P$. So, $\mathbb{C}^\times/P \simeq U$.

Define $\tau(a + bi) = \sqrt{a^2 + b^2}$. Then for $a + bi, c + di$,

$$\tau((a + bi)(c + di)) = \tau(ac - bd + (ad + bc)i)$$

$$= \sqrt{(ac - bd)^2 + (ad + bc)^2} = \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2}$$

$$= \sqrt{(a^2 + b^2)(c^2 + d^2} = \tau(a + bi)\tau(c + di)$$

So, τ is a homomorphism, and it is surjective onto P^+, the subgroup of positive reals. And, $\ker \varphi = U$. So, $\mathbb{C}^\times/P \simeq P^+$.

(11) Let $a = p + r$, where $p \in \mathbb{Z}$, and $0 \leq r < 1$. Define $\varphi(a) = r$. Then for $a_1 = p_1 + r_1, a_2 = p_2 + r_2 \in \mathbb{R}$, with $r_1 + r_2 = p_3 + r_3$. Then

$$\varphi(a_1 + a_2) = \varphi(p_1 + r_1 + p_2 + r_2)$$

$$= \varphi((p_1 + p_2 + p_3) + r_3) = r_3 = \varphi(a_1) + \varphi(a_2)$$

So φ is a homomorphism, and it is surjective onto $[0, 1]$. And, $\ker \varphi = \mathbb{Z}^+$. So, $\mathbb{R}^+/\mathbb{Z}^+ \simeq [0, 1)$ modulo 1.

Let $a = 2\pi p + r$, where $p \in \mathbb{Z}$, and $0 \leq r < 2\pi$. Define $\varphi(a) = r$. Then for $a_1 = 2\pi p_1 + r_1, a_2 = 2\pi p_2 + r_2 \in \mathbb{R}$, with $r_1 + r_2 = 2\pi p_3 + r_3$. Then

$$\varphi(a_1 + a_2) = \varphi(2\pi p_1 + r_1 + 2\pi p_2 + r_2)$$

$$= \varphi(2\pi(p_1 + p_2 + p_3) + r_3) = r_3 = \varphi(a_1) + \varphi(a_2)$$

So φ is a homomorphism, and it is surjective onto $[0, 2\pi]$. And, $\ker \varphi = \mathbb{Z}^+$. So, $\mathbb{R}^+/2\pi\mathbb{Z}^+ \simeq [0, 2\pi)$ modulo 2π.

Let $a \in [0, 1)$ modulo 1. Define $f(a) = 2\pi a \in [0, 2\pi)$ modulo 2π. Clearly, f is a bijection and is an isomorphism. So, $\mathbb{R}^+/\mathbb{Z}^+ \simeq \mathbb{R}^+/2\pi\mathbb{Z}^+$.

2.11 Miscellaneous Problems

(1)

$$\prod_{j=0}^{m-1} e^{\frac{j2\pi}{m}i} = e^{\frac{2\pi}{m}i(\sum_{j=0}^{m-1} j)} = e^{\pi(m-1)i} = (e^{\pi i})^{m-1} = (-1)^{m-1}$$

(2) For all automorphisms f, $f(1) = 1$ and $f(-1) = -1$. And, if $f(i) = a$, then $f(-i) = -a$. So, each automorphism f can be described by $f(i)$ and $f(j)$: there are 6 possibilities for $f(i)$, and given $f(i)$ there are 4 possibilities for $f(j)$. With these facts, it is trivial to compute $Aut(Q_8)$.

(3) Let $|G| = 2n$. For $a \in G$, if $|a| \neq 2$, then either $a = 1$, or $a \neq a^{-1}$. Counting these elements, there is an odd number of elements. Therefore, there must be at least one element of order 2.

(4)

$$G = |H|[G : H], G = |K|[G : K] \rightarrow |H|[G : H] = |K|[G : K]$$

$$|H| = |K|[H : K] \rightarrow |K|[H : K][G : H] = |K|[G : K]$$

$$\rightarrow [G : K] = [G : H][H : K]$$

(5) $\varphi : S \rightarrow T$ is an isomorphism of semigroups if for $a, b \in S$, $\varphi(ab) = \varphi(a)\varphi(b)$, and φ is a bijection.

If $|S| = \infty$, and s generates S, then $S \simeq (\mathbb{Z}^+ \geq 0)$, that is the additive semigroup of positive integers, that is described by the map $\varphi(s) = 1$.

If $|S| = n < \infty$, and s generates S, then for some $0 \leq k < n$, then $s^n = s^k$. Then $\{s^k, ..., s^{n-1}\}$ forms a cyclic subgroup.

(6) Since S satisfies the Cancellation Laws, then for $a, b, c \in S$, if $ab = ac$, then $b = c$. Therefore, for some $x \in S, ax = 1 \to a, x$ have inverses. Therefore, S is a group.

(7) (a) Note that the path from a onto itself is $f(t) = a \forall t$, so $a \simeq a$.
If $a \sim b$, then $f(t)$ is a path joining a and b. Then $g(t) = f(1-t)$ is a path joining b and a. So, $b \sim a$.
If $a \sim b$ and $b \sim c$, then $f(t)$ is a path joining a and b, and $g(t)$ is a path joining b and c. Define $h(t)$ as follows: If $t \in [0, 1/2]$, then $h(t) = f(2t)$. If $t \in [1/2, 1]$, then $h(t) = g(2t-1)$. Since for all t, $h(t) \in S$, then $a \sim c$.

(b) Since $\sim$ is an equivalence relation on S, then $\sim$ partitions S. Since a subset S is path connected if all points in S follow $\sim$, then by definition S is partitioned by path connected subsets.

(c) $\left\{x^2 + y^2 = 1\right\}, \{xy = 0\}$ are path connected since they are continuous loci. $\{xy = 1\}$ is not continuous at $x = 0$ or $y = 0$, so it is not path connected.

(8) (a) Note that $AC, BD \in G$. Let $f(t)$ be the path from A to B, and $g(t)$ be the path from C to D. Then $f(0)g(0) = AC$, and $f(1)g(1) = BD$. And, $f(t)g(t) \in G$. So, $f(t)g(t)$ is a path from AC to BD.

(b) Let $A \in G$ where there is a path from A to I. Then for $B \in G$, there is a path from BA to B. So, there is a path from BAB^{-1} to $BB^{-1} = I$. So, therefore the set of matrices connected to I forms a connected component.

(9) (a) Let E be an elementary matrix of the first kind, where $e_{ij} = a, i \neq j$. Note that $E \in SL_n(\mathbb{R})$. And, there is a path $f(t)$ in $SL_n(\mathbb{R})$ from E to I defined as an operation on e_{ij}: $e_{ij}(t) = (1-t)a$. For $A \in SL_n(\mathbb{R})$, then there is a path from A to I. Thus $SL_n(\mathbb{R})$ is path connected.

(b) Let E be an elementary matrix of the third kind, where $e_{ii} = a$. There is a path $f(t)$ from E to I defined as an operation on e_{ii}: $e_{ii}(t) = 1 + (1-t)(a-1)$. So, elementary matrices of the third kind is a path connected subset.
So, for $A \in GL_n(\mathbb{R})$, since A can be written as a product of elementary matrices of the first and third kinds, there is a path from A to I within the union of the elementary matrices of the first and third kinds.

(10) (a) For $g \in G$, then for some x, $x = hgk \to h^{-1}xk^{-1} = g \in HgK$. So, g is contained in some double coset. So the double cosets of G covers all of G.
Suppose $x \in G$ is contained in Hg_1K and Hg_2K. So, for some $h_1, h_2 \in H, k_1, k_2 \in K$, we have $h_1g_1k_1 = h_2g_2k_2 \to h_2^{-1}h_1g_1k_1k_2^{-1} = g_2 \in Hg_1K \to Hg_2K \subseteq Hg_1K$. Similarly, $g_1 \in Hg_2K \to Hg_1K \subseteq Hg_2K$. So, $Hg_1K = Hg_2K$. So, the double cosets are disjoint, and therefore partition G.

(b) Consider S_3. Let $A = \{1, y\}$ and $B = \{1, xy\}$ be subgroups of S_3. Then

$$BA = \{1, x, xy, y\}$$

But

$$Bx^2A = \left\{x^2, x^2y\right\}$$

So, not all double cosets have the same order.

(11) Suppose H is normal. Then for $h_1, h_2, h_3 \in H$, then $h_1 g = g h_3$, so $h_1 g h_2 = g h_3 h_2 \in gH$. So, $HgH \subseteq gH$. Similarly, $gh_4 = gh_2 h_3 = h_1 g h_3$, so $gH \subseteq HgH$. Thus, $HgH = gH$.

Suppose H is not normal. Clearly, $gH \in HgH$. And, there must exist some $h_1 \in H$ such that for some other $h_2 \in H$, $h_1 g h_2 \notin gH$: otherwise H is normal. Thus gH is a proper subset of HgH.

(12) Let $A \in GL_n(\mathbb{R})$. Since A is invertible, then A can be written as LPU, where L is a lower triangular matrix, P is a permutation matrix, and U is a upper triangular matrix with diagonal entries all 1. Then, for $B \in H, C \in K$, then

$$BAC = BLPUC \in HPK$$

Chapter 3

Vector Spaces

Exercises

I don't need to learn 8 + 7: I'll remember 8 + 8 and subtract 1.

T. Cuyler Young, Jr.

EXERCISES

1. Real Vector Spaces

1. Which of the following subsets of the vector space of real $n \times n$ matrices is a subspace?
   (a) symmetric matrices ($A = A^t$)
   (b) invertible matrices
   (c) upper triangular matrices
2. Prove that the intersection of two subspaces is a subspace.
3. Prove the cancellation law in a vector space: If $cv = cw$ and $c \neq 0$, then $v = w$.
4. Prove that if w is an element of a subspace W, then $-w \in W$ too.
5. Prove that the classification of subspaces of $\mathbb{R}^3$ stated after (1.2) is complete.
6. Prove that every solution of the equation $2x_1 - x_2 - 2x_3 = 0$ has the form (1.5).
7. What is the description analogous to (1.4) obtained from the particular solutions $u_1 = (2, 2, 1)$ and $u_2 = (0, 2, -1)$?

2. Abstract Fields

1. Prove that the set of numbers of the form $a + b\sqrt{2}$, where a, b are rational numbers, is a field.
2. Which subsets of $\mathbb{C}$ are closed under $+$, $-$, $\times$, and $\div$ but fail to contain 1?
3. Let F be a subset of $\mathbb{C}$ such that F^+ is a subgroup of $\mathbb{C}^+$ and $F^\times$ is a subgroup of $\mathbb{C}^\times$. Prove that F is a subfield of $\mathbb{C}$.
4. Let $V = F^n$ be the space of column vectors. Prove that every subspace W of V is the space of solutions of some system of homogeneous linear equations $AX = 0$.
5. Prove that a nonempty subset W of a vector space satisfies the conditions (2.12) for a subspace if and only if it is closed under addition and scalar multiplication.
6. Show that in Definition (2.3), axiom (ii) can be replaced by the following axiom: $F^\times$ is an abelian group, and $1 \neq 0$. What if the condition $1 \neq 0$ is omitted?
7. Define homomorphism of fields, and prove that every homomorphism of fields is injective.
8. Find the inverse of 5 (modulo p) for $p = 2, 3, 7, 11, 13$.
9. Compute the polynomial $(x^2 + 3x + 1)(x^3 + 4x^2 + 2x + 2)$ when the coefficients are regarded as elements of the fields (a) $\mathbb{F}_5$ (b) $\mathbb{F}_7$.
10. Consider the system of linear equations $\begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \end{bmatrix}$.
    (a) Solve it in $\mathbb{F}_p$ when $p = 5, 11, 17$.
    (b) Determine the number of solutions when $p = 7$.

11. Find all primes p such that the matrix

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & -1 \\ -2 & 0 & 2 \end{bmatrix}$$

is invertible, when its entries are considered to be in $\mathbb{F}_p$.

12. Solve completely the systems of linear equations $AX = B$, where

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$$

(a) in $\mathbb{Q}$ **(b)** in $\mathbb{F}_2$ **(c)** in $\mathbb{F}_3$ **(d)** in $\mathbb{F}_7$.

13. Let p be a prime integer. The nonzero elements of $\mathbb{F}_p$ form a group $\mathbb{F}_p^\times$ of order $p - 1$. It is a fact that this group is always cyclic. Verify this for all primes $p < 20$ by exhibiting a generator.

14. **(a)** Let p be a prime. Use the fact that $\mathbb{F}_p^\times$ is a group to prove that $a^{p-1} \equiv 1$ (modulo p) for every integer a not congruent to zero.

(b) Prove *Fermat's Theorem:* For every integer a,

$$a^p \equiv a \text{ (modulo } p).$$

15. **(a)** By pairing elements with their inverses, prove that the product of all nonzero elements of $\mathbb{F}_p$ is -1.

(b) Let p be a prime integer. Prove *Wilson's Theorem:*

$$(p - 1)! \equiv -1 \text{ (modulo } p).$$

16. Consider a system $AX = B$ of n linear equations in n unknowns, where A and B have integer entries. Prove or disprove: If the system has an integer solution, then it has a solution in $\mathbb{F}_p$ for all p.

17. Interpreting matrix entries in the field $\mathbb{F}_2$, prove that the four matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ form a field.

18. The proof of Lemma (2.8) contains a more direct proof of (2.6). Extract it.

3. Bases and Dimension

1. Find a basis for the subspace of $\mathbb{R}^4$ spanned by the vectors $(1, 2, -1, 0)$, $(4, 8, -4, -3)$, $(0, 1, 3, 4)$, $(2, 5, 1, 4)$.

2. Let $W \subset \mathbb{R}^4$ be the space of solutions of the system of linear equations $AX = 0$, where $A = \begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix}$. Find a basis for W.

3. **(a)** Show that a subset of a linearly independent set is linearly independent.

(b) Show that any reordering of a basis is also a basis.

4. Let V be a vector space of dimension n over F, and let $0 \leq r \leq n$. Prove that V contains a subspace of dimension r.

5. Find a basis for the space of symmetric $n \times n$ matrices.
6. Prove that a square matrix A is invertible if and only if its columns are linearly independent.
7. Let V be the vector space of functions on the interval $[0, 1]$. Prove that the functions x^3, $\sin x$, and $\cos x$ are linearly independent.
8. Let A be an $m \times n$ matrix, and let A' be the result of a sequence of elementary row operations on A. Prove that the rows of A span the same subspace as the rows of A'.
9. Let V be a complex vector space of dimension n. Prove that V has dimension $2n$ as real vector space.
10. A complex $n \times n$ matrix is called *hermitian* if $a_{ij} = \bar{a}_{ji}$ for all i, j. Show that the hermitian matrices form a real vector space, find a basis for that space, and determine its dimension.
11. How many elements are there in the vector space $\mathbb{F}_p{}^n$?
12. Let $F = \mathbb{F}_2$. Find all bases of F^2.
13. Let $F = \mathbb{F}_5$. How many subspaces of each dimension does the space F^3 contain?
14. (a) Let V be a vector space of dimension 3 over the field $\mathbb{F}_p$. How many subspaces of each dimension does V have?
    (b) Answer the same question for a vector space of dimension 4.
15. (a) Let $F = \mathbb{F}_2$. Prove that the group $GL_2(F)$ is isomorphic to the symmetric group S_3.
    (b) Let $F = \mathbb{F}_3$. Determine the orders of $GL_2(F)$ and of $SL_2(F)$.
16. Let W be a subspace of V.
    (a) Prove that there is a subspace U of V such that $U + W = V$ and $U \cap W = 0$.
    (b) Prove that there is no subspace U such that $W \cap U = 0$ and that $\dim W + \dim U > \dim V$.

4. Computation with Bases

1. Compute the matrix P of change of basis in F^2 relating the standard basis $\mathbf{E}$ to $\mathbf{B}' = (v_1, v_2)$, where $v_1 = (1, 3)^t$, $v_2 = (2, 2)^t$.
2. Determine the matrix of change of basis, when the old basis is the standard basis $(e_1, \ldots, e_n)$ and the new basis is $(e_n, e_{n-1}, \ldots, e_1)$.
3. Determine the matrix P of change of basis when the old basis is (e_1, e_2) and the new basis is $(e_1 + e_2, e_1 - e_2)$.
4. Consider the equilateral coordinate system for $\mathbb{R}^2$, given by the basis $\mathbf{B}'$ in which $v_1 = e_1$ and v_2 is a vector of unit length making an angle of 120° with v_1. Find the matrix relating the standard basis $\mathbf{E}$ to $\mathbf{B}'$.
5. (i) Prove that the set $\mathbf{B} = ((1, 2, 0)^t, (2, 1, 2)^t, (3, 1, 1)^t)$ is a basis of $\mathbb{R}^3$.
   (ii) Find the coordinate vector of the vector $v = (1, 2, 3)^t$ with respect to this basis.
   (iii) Let $\mathbf{B}' = ((0, 1, 0)^t, (1, 0, 1)^t, (2, 1, 0)^t)$. Find the matrix P relating $\mathbf{B}$ to $\mathbf{B}'$.
   (iv) For which primes p is $\mathbf{B}$ a basis of $\mathbb{F}_p{}^3$?
6. Let $\mathbf{B}$ and $\mathbf{B}'$ be two bases of the vector space F^n. Prove that the matrix of change of basis is $P = [\mathbf{B}']^{-1}[\mathbf{B}]$.
7. Let $\mathbf{B} = (v_1, \ldots, v_n)$ be a basis of a vector space V. Prove that one can get from $\mathbf{B}$ to any other basis $\mathbf{B}'$ by a finite sequence of steps of the following types:

(i) Replace v_i by $v_i + av_j$, $i \neq j$, for some $a \in F$.
(ii) Replace v_i by cv_i for some $c \neq 0$.
(iii) Interchange v_i and v_j.

8. Rewrite the proof of Proposition (3.16) using the notation of Proposition (4.13).
9. Let $V = F^n$. Establish a bijective correspondence between the sets $\mathcal{B}$ of bases of V and $GL_n(F)$.
10. Let F be a field containing 81 elements, and let V be a vector space of dimension 3 over F. Determine the number of one-dimensional subspaces of V.
11. Let $F = \mathbb{F}_p$.
    (a) Compute the order of $SL_2(F)$.
    (b) Compute the number of bases of F^n, and the orders of $GL_n(F)$ and $SL_n(F)$.
12. **(a)** Let A be an $m \times n$ matrix with $m < n$. Prove that A has no left inverse by comparing A to the square $n \times n$ matrix obtained by adding $(n - m)$ rows of zeros at the bottom.
    (b) Let $\mathbf{B} = (v_1, \ldots, v_m)$ and $\mathbf{B}' = (v_1', \ldots, v_n')$ be two bases of a vector space V. Prove that $m = n$ by defining matrices of change of basis and showing that they are invertible.

5. Infinite-Dimensional Spaces

1. Prove that the set $(w; e_1, e_2, \ldots)$ introduced in the text is linearly independent, and describe its span.
2. We could also consider the space of doubly infinite sequences $(a) = (\ldots, a_{-1}, a_0, a_1, \ldots)$, with $a_i \in \mathbb{R}$. Prove that this space is isomorphic to $\mathbb{R}^\infty$.
3. Prove that the space Z is isomorphic to the space of real polynomials.
4. Describe five more infinite-dimensional subspaces of the space $\mathbb{R}^\infty$.
5. For every positive integer, we can define the space ℓ^p to be the space of sequences such that $\Sigma|a_i|^p < \infty$.
    (a) Prove that ℓ^p is a subspace of $\mathbb{R}^\infty$.
    (b) Prove that $\ell^p < \ell^{p+1}$.
6. Let V be a vector space which is spanned by a countably infinite set. Prove that every linearly independent subset of V is finite or countably infinite.
7. Prove Proposition (5.7).

6. Direct Sums

1. Prove that the space $\mathbb{R}^{n\times n}$ of all $n \times n$ real matrices is the direct sum of the spaces of symmetric matrices ($A = A^t$) and of skew-symmetric matrices ($A = -A^t$).
2. Let W be the space of $n \times n$ matrices whose trace is zero. Find a subspace W' so that $\mathbb{R}^{n\times n} = W \oplus W'$.
3. Prove that the sum of subspaces is a subspace.
4. Prove Proposition (6.5).
5. Prove Proposition (6.6).

Miscellaneous Problems

1. **(a)** Prove that the set of symbols $\{a + bi \mid a, b \in \mathbb{F}_3\}$ forms a field with nine elements, if the laws of composition are made to mimic addition and multiplication of complex numbers.

(b) Will the same method work for $\mathbb{F}_5$? For $\mathbb{F}_7$? Explain.

***2.** Let V be a vector space over an infinite field F. Prove that V is not the union of finitely many proper subspaces.

***3.** Let W_1, W_2 be subspaces of a vector space V. The formula $\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$ is analogous to the formula $|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|$, which holds for sets. If three sets are given, then

$$|S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3|.$$

Does the corresponding formula for dimensions of subspaces hold?

4. Let F be a field which is not of characteristic 2, and let $x^2 + bx + c = 0$ be a quadratic equation with coefficients in F. Assume that the discriminant $b^2 - 4c$ is a square in F, that is, that there is an element $\delta \in F$ such that $\delta^2 = b^2 - 4c$. Prove that the quadratic formula $x = (-b + \delta)/2a$ solves the quadratic equation in F, and that if the discriminant is not a square the polynomial has no root in F.

5. **(a)** What are the orders of the elements $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, \begin{bmatrix} 2 & \\ & 1 \end{bmatrix}$ of $GL_2(\mathbb{R})$?

(b) Interpret the entries of these matrices as elements of $\mathbb{F}_7$, and compute their orders in the group $GL_2(\mathbb{F}_7)$.

6. Consider the function det: $F^{n\times n} \longrightarrow F$, where $F = \mathbb{F}_p$ is a finite field with p elements and $F^{n\times n}$ is the set of 2×2 matrices.

(a) Show that this map is surjective.

(b) Prove that all nonzero values of the determinant are taken on the same number of times.

7. Let A be an $n \times n$ real matrix. Prove that there is a polynomial $f(t) = a_r t^r + a_{r-1}t^{r-1} + \cdots + a_1 t + a_0$ which has A as root, that is, such that $a_r A^r + a_{r-1}A^{r-1} + \cdots + a_1 A + a_0 I = 0$. Do this by showing that the matrices $I, A, A^2, \ldots$ are linearly dependent.

***8.** An *algebraic curve* in $\mathbb{R}^2$ is the locus of zeros of a polynomial $f(x, y)$ in two variables. By a *polynomial path* in $\mathbb{R}^2$, we mean a parametrized path $x = x(t)$, $y = y(t)$, where $x(t)$, $y(t)$ are polynomials in t.

(a) Prove that every polynomial path lies on a real algebraic curve by showing that, for sufficiently large n, the functions $x(t)^i y(t)^j$, $0 \le i, j \le n$, are linearly dependent.

(b) Determine the algebraic curve which is the image of the path $x = t^2 + t$, $y = t^3$ explicitly, and draw it.

3.1 Real Vector Spaces

(1) (a) Let A, B be symmetric matrices. Then, $A + B = (A + B)^\top$. And, for $c \in \mathbb{R}$, $cA = cA^\top$. So, addition and scalar multiplication are closed rules of composition. So the symmetric matrices form a subspace.

(b) The invertible matrices do not form a subspace. Consider

$$A = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, B = \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$$

Then $\det(A + B) = 0$, so $A + B$ is not invertible.

(c) Let A, B be upper triangular matrices. Then, $A + B$ is also upper triangular. And, for $c \in \mathbb{R}$, cA is also upper triangular. So, addition and scalar multiplication are closed rules of composition. So the upper triangular matrices form a subspace.

(2) Consider the subspaces $\mathcal{A}, \mathcal{B}$. If $a, b \in \mathcal{A} \cap \mathcal{B}$, then $a + b \in \mathcal{A}$ and $a + b \in \mathcal{B}$, so $a + b \in \mathcal{A} \cap \mathcal{B}$. And, for $c \in \mathbb{R}$, similarly $ca \in \mathcal{A}$, and $cb \in \mathcal{B}$. So, $\mathcal{A} \cap \mathcal{B}$ is a subspace.

(3) Let $cv = cw, c \neq 0$. Then $cv - cw = 0 \to c(v - w) = 0 \to v - w = 0 \to v = w$.

(4) If W is a subspace, then W^+ forms an abelian group. So, if $w \in W$, then necessairly $-w \in W$.

(5) Clearly, the zero vector forms a subspace of $\mathbb{R}^3$.

Let $(x_1, y_1, z_1), (cx_1, cy_1, cz_1) \in \mathbb{R}^3$ be collinear passing through the origin. Then $(x_1, y_1, z_1) + (cx_1, cy_1, cz_1) = ((c + 1)x_1, (c + 1)y_1, (c + 1)z_1)$ lies on the same line. And, for $d \in \mathbb{R}^3$, (dx_1, dy_1, dz_1) is also collinear.

Let $v_1 = (x_1, y_1, z_1), v_2 = (x_2, y_2, z_2) \in \mathbb{R}^3$ that are not collinear. Then v_1, v_2 is coplanar to some plane. Clearly, $(x_1, y_1, z_1) + (x_2, y_2, z_2)$ also lies in the same plane. And, for $d \in \mathbb{R}^3$, (dx_1, dy_1, dz_1) is also coplanar.

And, clearly $\mathbb{R}^3$ is a subspace of itself: any three vectors that are not coplanar to each other forms $\mathbb{R}^3$.

(6) Let (x_1, x_2, x_3) be a solution. Then, $2x_1 - x_2 - 2x_3 = 0 \to x_1 = x_2/2 + x_3$. So, the solution has the form $(x_2/2 + x_3, x_2, x_3)$. And, letting $x_2/2 = y_2$. Then, the solution has the form $(y_2 + x_3, 2y_2, x_3)$.

(7) Every solution has the form

$$c_1 u_1 + c_2 u_2 = \begin{bmatrix} 2c_1 \\ 2c_1 + 2c_2 \\ c_1 - c_2 \end{bmatrix}$$

where c_1, c_2 are arbitrary constants.

3.2 Abstract Fields

(1) Let $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in F$. Then:

$$a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in F$$

$$-(a_1 + b_1\sqrt{2}) = -a_1 + (-b_1)\sqrt{2} \in F$$

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2} \in F$$

$$1 \in F$$

$$\left(a_1 + b_1\sqrt{2}\right)\left(\frac{a_1}{a_1^2 - 2b_1^2} - \frac{b_1}{a_1^2 - 2b_1^2}\sqrt{2}\right)$$

$$= \frac{a_1^2}{a_1^2 - 2b_1^2} - \frac{2b_1^2}{a_1^2 - 2b_1^2} + \frac{a_1b_1}{a_1^2 - 2b_1^2}\sqrt{2} - \frac{a_1b_1}{a_1^2 - 2b_1^2}\sqrt{2} = 1$$

$$\to (a_1 + b_1\sqrt{2})^{-1} \in F$$

Thus, F is a field.

(2) There is no such subset. If a subset S is closed under division, then if $a \in S$, then $a^{-1} \in S$. But then $aa^{-1} = 1 \in S$. So, S must contain 1.

(3) Since F^+ is a subgroup of $\mathbb{C}^+$, then F^+ is abelian.

Since $F^\times$ is a subgroup of $\mathbb{C}^\times$, then $F^\times$ is abelian.

Let $a_1 + b_1i, a_2 + b_2i, a_3 + b_3i \in F$. Then

$$(a_1 + b_1i + a_2 + b_2i)(a_3 + b_3i) = ((a_1 + a_2) + (b_1 + b_2)i)(a_3 + b_3i)$$

$$= (a_1 + a_2)a_3 - (b_1 + b_2)b_3 + ((a_1 + a_2)b_3 + (b_1 + b_2)a_3)i$$

$$= a_1a_3 + a_2a_3 - b_1b_3 - b_2b_3 + (a_1b_3 + a_2b_3 + a_3b_1 + a_3b_2)i$$

$$= (a_1 + b_1i)(a_3 + b_3i) + (a_2 + b_2i)(a_3 + b_3i)$$

Thus, the distributive law holds, and F is a subfield of $\mathbb{C}$.

(4) Let $w \in W$, and $v \in V$, where $v \notin W$. Note for all $x \in V$, we can write x as $x = w + v$, for any w, v. Then, define $\varphi(x) = \varphi(v + w) = w$. That is, $\varphi(x)$ is the projection of x onto W. Since W is the kernel of φ, then there exists some A such that W is the solution set of $Ax = 0$.

(5) Suppose W is a subspace by 2.12. By (a) and (b), W is closed under addition and scalar multiplication.

Suppose W is closed under addition and scalar multiplication. Then, for $w, w' \in W, w + w' \in W$, and for $c \in F$, then $cw \in W$. And, $(-1)w = -w \in W$. So, $0 = w - w \in W$. Thus, W is a subspace.

(6) Since multiplication is associative and commutative, then $F^\times$ is abelian. Since $F^\times$ is a group, then it contains an identity: 1.

If $F^\times$ is abelian, then multiplication is associative and commutative. And, since $F^\times$ does not contain 0, then $0 \neq 1$.

Suppose $0 = 1$. Then, $1 = 0 = 0 + 0 = 1 + 1$. This would mean that the real numbers are not a field.

(7) A homomorphism φ from a vector space V to a vector space V' both over the same field F is a map $\varphi : V \to V'$ satisfying, for $v, v' \in V, c \in F$:

$$\varphi(v + v') = \varphi(v) + \varphi(v'), \varphi(vv') = \varphi(v)\varphi(v')$$

Suppose for $v \neq u$, $\varphi(v) = \varphi(u)$. Then $\varphi(v-u) = \varphi(v) - \varphi(u) = 0$. So, $\varphi((v-u)(v-u)^{-1}) = \varphi(v-u)\varphi((v-u)^{-1}) = 0$, and $\varphi((v-u)(v-u)^{-1}) = \varphi(1) = 1$. So, $0 = 1$, a contradiction. Thus, φ must be injective.

(8)

$$5 \equiv 1 \mod 2 \to 5^{-1} \equiv 1 \mod 2$$
$$5 \equiv 2 \mod 3 \to 5^{-1} \equiv 2 \mod 3$$
$$5^{-1} \equiv 3 \mod 7$$
$$5^{-1} \equiv 9 \mod 11$$
$$5^{-1} \equiv 8 \mod 13$$

(9)

$$(x^2 + 3x + 1)(x^3 + 4x^2 + 2x + 2)$$
$$= x^5 + 3x^4 + x^3 + 4x^4 + 12x^3 + 4x^2 + 2x^3 + 6x + 2 + 2x^2 + 6x + 2$$
$$= x^5 + 7x^4 + 15x^3 + 6x^2 + 12x + 4$$

(a)

$$x^5 + 7x^4 + 15x^3 + 6x^2 + 12x + 4 \mod 5$$
$$\equiv 2x^4 + x^2 + 3x + 4 \mod 5$$

(b)

$$x^5 + 7x^4 + 15x^3 + 6x^2 + 12x + 4 \mod 7$$
$$\equiv x^5 + x^3 + 6x^2 + 5x + 4 \mod 7$$

(10) (a)

$$A = \begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix}, A^{-1} = \frac{1}{42}\begin{bmatrix} 6 & -3 \\ -2 & 8 \end{bmatrix} = \begin{bmatrix} 1/7 & -1/14 \\ -1/21 & 4/21 \end{bmatrix},$$
$$B = \begin{bmatrix} 3 \\ -1 \end{bmatrix}, A^{-1}B = \begin{bmatrix} 1/2 \\ -1/3 \end{bmatrix}$$

p = 5

$$A^{-1}B = \begin{bmatrix} 2^{-1} \\ (-1)3^{-1} \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix}$$

p = 11

$$A^{-1}B = \begin{bmatrix} 2^{-1} \\ (-1)3^{-1} \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \end{bmatrix}$$

p = 17

$$A^{-1}B = \begin{bmatrix} 2^{-1} \\ (-1)3^{-1} \end{bmatrix} = \begin{bmatrix} 9 \\ 11 \end{bmatrix}$$

(b) When $p = 7$, then A is not invertible, so there are no solutions.

(11)
$$\det \begin{bmatrix} 1 & 2 & \\ & 3 & -1 \\ -2 & & 2 \end{bmatrix} = 1(6) - 2(-2) = 10 = (2)(5)$$

A is invertible for all primes excluding 2 and 5.

(12)
$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, C = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}, A^{-1} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix}$$

(a)
$$AX = B \to X = A^{-1}B = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$
$$AX = C \to X = A^{-1}C = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1/3 \\ 2/3 \\ -4/3 \end{bmatrix}$$

(b)
$$A^{-1} \to \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, C \to \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$
$$X = A^{-1}B = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$
$$X = A^{-1}C = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

(c)
$$C \to \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$$
$$AX = B \to$$
$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 2 & 2 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$
$$\to X = \begin{bmatrix} 2x \\ x \\ x \end{bmatrix}$$
$$AX = C \to$$

$$\begin{bmatrix}1&1&0&1\\1&0&1&2\\1&2&2&1\end{bmatrix}\to\begin{bmatrix}1&1&0&1\\0&2&1&1\\0&1&2&0\end{bmatrix}\to\begin{bmatrix}1&1&0&1\\0&2&1&1\\0&0&0&1\end{bmatrix}\to\begin{bmatrix}1&0&1&2\\0&2&1&1\\0&0&0&1\end{bmatrix}$$

$$\to \text{no solution}$$

(d)

$$A^{-1}\to\begin{bmatrix}5&5&5\\3&2&2\\2&3&2\end{bmatrix}, C\to\begin{bmatrix}1\\6\\1\end{bmatrix}$$

$$X=A^{-1}B=\begin{bmatrix}5&5&5\\3&2&2\\2&3&2\end{bmatrix}\begin{bmatrix}0\\0\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix}$$

$$X=A^{-1}C=\begin{bmatrix}5&5&5\\3&2&2\\2&3&2\end{bmatrix}\begin{bmatrix}1\\6\\1\end{bmatrix}=\begin{bmatrix}5\\3\\1\end{bmatrix}$$

(13) p=2:

$$a=1$$

p=3:

$$a=2, a^2=1$$

p=5:

$$a=3, a^2=4, a^3=2, a^4=1$$

p=7:

$$a=3, a^2=2, a^3=6, a^4=4, a^5=5, a^6=1$$

p=11:

$$a=7, a^2=5, a^3=2, a^4=3, a^5=10,$$
$$a^6=4, a^7=6, a^8=9, a^9=8, a^{10}=1$$

p=13:

$$a=11, a^2=4, a^3=5, a^4=3, a^5=7, a^6=12,$$
$$a^7=2, a^8=9, a^9=8, a^{10}=10, a^{11}=6, a^{12}=1$$

p=17:

$$a=11, a^2=2, a^3=5, a^4=4, a^5=10, a^6=8, a^7=3, a^8=16,$$
$$a^9=6, a^{10}=15, a^{11}=12, a^{12}=13, a^{13}=7, a^{14}=9, a^{15}=14, a^{16}=1$$

p=19:

$$a=13, a^2=17, a^3=12, a^4=4, a^5=14, a^6=11,$$
$$a^7=10, a^8=16, a^9=18, a^{10}=6, a^{11}=2,$$
$$a^{12}=7, a^{13}=15, a^{14}=5, a^{15}=8, a^{16}=9, a^{17}=3, a^{18}=1$$

(14) (a) Let a be the generator of $\mathbb{F}_p^\times$. For $b \in \mathbb{F}_p^\times$, $a^m = b$ for some $1 \leq m \leq p$. Then, $b^{p-1} = (a^m)^{p-1} = (a^{p-1})^m = 1^m = 1$. So, if b is not congruent to 0, then $b^{p-1} \equiv 1 \mod p$.

(b) From part (a), if b is not congruent to 0, then $b^{p-1} \equiv 1 \mod p$. Then, $b^p \equiv b \mod p$. If b is congruent to 0, then $b^p \equiv 0$. So, $b^p \equiv b \mod p$.

(15) (a) Note that $(p-1)^2 = p^2 - 2p + 1 \to (p-1)^2 \equiv 1 \mod p$. And, since $\mathbb{F}_p^\times$ is cyclic, then $p-1$ is the unique element of order 2. Thus, the product of all elements of $F_p^\times$ modulo p is $p - 1 \equiv -1$.

(b) Directly followng from part (a), $(p-1)! \equiv -1 \mod p$.

(16) True. If $AX = B$ has an integer solution, since there is no division then clearly each equation $a_{i1}x_1 + a_{i2}x_2 + ... + a_{in}x_n = b_i$ is also true modulo p, for any p. So $AX = B$ also has a solution in $\mathbb{F}_p$.

(17) Let

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, C = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, D = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Note that matrix addition is commutative, and both addition and multiplication are associative and follow the distributive law. So, to prove that $\mathcal{A} = \{A, B, C, D\}$, is a field, it follows that addition and multiplication are closed on this set, and that multiplication is commutative. Also, note that $\mathcal{A}^\times = \{A, C, D\}$. Then,

$$A + B = A, A + C = D, A + D = C, B + C = C, B + D = D, C + D = A$$

$$AC = CA = C, AD = DA = D, CD = DC = A$$

So, $\mathcal{A}$ is a field.

(18) Let p be a prime, and a be any integer not divisible by p, ie. $gcd(a, p) = 1$. Then, there exists some r, s such that $1 = ra + sp \to ra \equiv 1 \mod p$. So, a has a multiplicative inverse r.

3.3 Bases and Dimension

(1) Let $v_1 = (1, 2, -1, 0), v_2 = (4, 8, -4, -3), v_3 = (0, 1, 3, 4), v_4 = (2, 5, 1, 4)$. Let's solve $c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4 = 0$. Then

$$\begin{bmatrix} 1 & 4 & 0 & 2 \\ 2 & 8 & 1 & 5 \\ -1 & -4 & 3 & 1 \\ 0 & -3 & 4 & 4 \end{bmatrix} \to \begin{bmatrix} 1 & 4 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 3 & 3 \\ 0 & -3 & 4 & 4 \end{bmatrix} \to \begin{bmatrix} 1 & 4 & 0 & 2 \\ 0 & -3 & 4 & 4 \\ 0 & 0 & 3 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

So, $v_4 \in Span(v_1, v_2, v_3)$. In particular: $v_4 = 2v_1 + v_3$. So, v_1, v_2, v_3 forms a basis.

(2)

$$\begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix} \to \begin{bmatrix} 2 & 1 & 2 & 3 \\ 0 & 0.5 & 2 & -1.5 \end{bmatrix}$$

So, we can describe the solutions of X as:

$$X = \begin{bmatrix} x_3 - 3x_4 \\ 3x_4 - 4x_3 \\ x_3 \\ x_4 \end{bmatrix}$$

with arbitrary x_3, x_4. So, a basis for W is:

$$\begin{bmatrix} 1 \\ -4 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 3 \\ 0 \\ 1 \end{bmatrix}$$

(3) (a) Suppose $v_1, ..., v_n$ is a linearly independent set, and $v_1, ..., v_i$ is linearly dependent. Then, for some $c_1, ..., c_i$ not all 0, $c_1v_1+...+c_iv_i = 0$. But then $c_1v_1+...+c_iv_i+0v_{i+1}+...+0v_n = 0$. So, $v_1, ..., v_n$ is linearly dependent, a contradiction. Thus, $v_1, ..., v_i$ must be linearly independent.

(b) A reordering of a basis maintains the same properties of a basis: its vectors remain a minimally spanning set (order is not relevant for this property).

(4) Let $r = 0$. Since $0 \in V$, then the 0 subspace of dimension 0 is contained in V.

Let $r > 0$. Let $v_1, ..., v_n$ be a basis for V. For any $c_1, ..., c_r$, $w = c_1v_1+...+c_rv_r \in V$. From the previous exercise, $v_1, ..., v_r$ is linearly independent, and thus defines a basis of some subspace V_r with dimension r.

(5) Let A be a symmetric $n \times n$ matrix. So, for each entry a_{ij} of A, $a_{ij} = a_{ji}$. We can construct a basis of the symmetric matrices in the following way: For $i \leq j$: set $a_{ij} = a_{ji} = 1$, and set all other entries of the matrix to 0.

(6) If A is invertible, then $AX = 0$ has only the trivial solution. So, the columns of A are linearly independent.

If the columns of A are linearly independent, then $AX = 0$ has only the trivial solution. Thus, A is invertible.

(7) Consider $c_1x^3 + c_2 \sin x + c_3 \cos x = 0$. Set $x = 0$. Then it must be the case that $c_3 = 0$. So, now consider $c_1x^3 + c_2 \sin x = 0$. Let $x = 1$, then $c_1 + c_2 \sin 1 = 0$. Let $x = \frac{\pi}{6}$, then $\frac{\pi^3}{256}c_1 + \frac{1}{2}c_2 = 0$. Clearly, the only solution is $c_1 = c_2 = 0$. Thus, $x^3, \sin x, \cos x$ are linearly independent.

(8) Let $x_1, ..., x_n$ be the rows of A. Let $Span(x_1, ..., x_n) = V$. Let $v \in V$, so $a_1x_1 + ... + a_nx_n = v$ for some $a_1, ..., a_n$. Now we shall consider each elementary matrix:

Elementary operation of the first kind, corresponding to replacing x_j with $x_j + cx_i$. Let $v = a_1x_1+...+a_ix_i+...+a_jx_j+...+a_nx_n$. And, $v = a_1x_1+...+(a_i-a_jc)x_i+...+a_j(x_j+cx_i)+...+a_n$. So, an elementary operation of the first kind preserves the span of the rows.

Elementary operation of the second kind, corresponding to swapping x_i and x_j. Clearly, this operation preserves the span of the rows.

Elementary operation of the third kind, corresponding to replacing x_i with cx_i. Let $v = a_1x_1 + ... + a_ix_i + ... + a_nx_n$. And, $v = a_1x_1 + ... + \frac{a_i}{c}cx_i + ... + a_nx_n$. So, an elementary operation of the third kind preserves the span of the rows.

Since each elementary operation preserves the span of the rows of A, then a series of elementary operations on the rows of A will also preserve the span of the rows of A. So, the rows of A' spans the span of the rows of A.

(9) Let $v_1, ..., v_n$ be a basis for V. Define a map from V to real vector space V_r: for $v = (a_1 + b_1i, ..., a_m + b_mi)$, then $\varphi(v) = (a_1, ..., a_m, b_1, ..., b_m)$. Clearly, V_r is a vector space. And, let $\alpha(v) = (a_1, ..., a_m, 0, ..., 0), \beta(v) = (0, ..., 0, b_1, ..., b_m)$. Then, $\alpha(v_1), ..., \alpha(v_n), \beta(v_1), ..., \beta(v_n)$ spans V_r: For $v = (c_1 + d_1i)v_1 + ... + (c_n + d_ni)v_n$, then $\varphi(v) = (c_1 - d_1)\alpha(v_1) + ... + (c_n - d_n)\alpha(v_n) + (c_1 + d_1)\beta(v_1) + ... + (c_n + d_n)\beta(v_n)$. Furthermore, $\alpha(v_1), ..., \alpha(v_n), \beta(v_1), ..., \beta(v_n)$ is a minimal spanning set: clearly then V would have dimension $< n$. Thus, V_r has dimension $2n$.

(10) Let A, B be hermitian matrices. Then $cA + dB$ is hermitian: $ca_{ij} + db_{ij} = c\overline{a}_{ji} + d\overline{b}_{ji} = \overline{ca_{ji} + b_{ji}}$.

A basis for this space is: the n matrices with a single 1 on the diagonal, the $n(n-1)/2$ matrices with a single pair of ones at positions ij and ji, and the $n(n-1)/2$ matrices with an i at position ij, and a $-i$ at position ji. The dimension of this space is thuse n^2.

(11) There are p^n elements in $\mathbb{F}_p^n$.

(12)
$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

(13) Dimension 0: 1 subspace

Dimension 1: There are $5^3 - 1 = 124$ vectors that can span a 1 dimensional subspace. For each vector, there are $5 - 1$ vectors that span this same subspace. So, there are $\frac{124}{4} = 31$ subspaces.

Dimension 2: There are $(5^3 - 1)(5^3 - 5)/2$ pairs of vectors that can span a 2 dimensional subspace. For each pair of vectors, there are $(5^2 - 1)(5^2 - 5)/2$ pairs that span this same subspace. So, there are $\frac{(5^3-1)(5^3-5)}{(5^2-1)(5^2-5)} = \frac{124}{4} = 31$ subspaces.

Dimension 3: 1 subspace

(14) (a) Dimension 0: 1 subspace

Dimension 1: There are $p^3 - 1$ vectors that can span a 1 dimensional subspace. For each vector, there are $p-1$ vectors that span this same subspace. So, there are $\frac{p^3-1}{p-1} = p^2+p+1$ subspaces.

Dimension 2: There are $(p^3-1)(p^3-p)/2$ vectors that can span a 2 dimensional subspace. For each pair of vectors, there are $(p^2-1)(p^2-p)/2$ pairs that span this same subspace. So, there are $p^2 + p + 1$ subspaces.

Dimension 3: 1 subspace

(b) Dimension 0: 1 subspace
Dimension 1: There are p^4-1 vectors that can span a 1 dimensional subspace. For each vector, there are $p-1$ vectors that span this same subspace. So, there are $\frac{p^4-1}{p-1} = (p^2+1)(p+1) = p^3+p^2+p+1$ subspaces.
Dimension 2: There are $(p^4-1)(p^4-p)/2$ vectors that can span a 2 dimensional subspace. For each pair of vectors, there are $(p^2-1)(p^2-p)/2$ pairs that span this same subspace. So, there are $\frac{(p^2+1)(p^2-1)p(p^3-1)}{(p^2-1)p(p-1)} = (p^2+1)(p^2+p+1) = p^4+p^3+2p^2+p+1$ subspaces.
Dimension 3: There are $(p^4-1)(p^4-p)(p^4-p^2)/6$ vectors that can span a 2 dimensional subspace. For each pair of vectors, there are $(p^3-1)(p^3-p)(p^3-p^2)/6$ pairs that span this same subspace. So, there are $\frac{(p^2+1)(p^2-1)p(p^3-1)p^2(p^2-1)}{(p^3-1)p(p^2-1)p^2(p-1)} = (p^2+1)(p+1) = p^3+p^2+p+1$ subspaces
Dimension 4: 1 subspace

(15) (a) Let

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Then, $A^2 = 1$, and $B^3 = 1$. So, A and B generate $GL_2(F)$. And, let $\varphi(A) = y$, $\varphi(B) = x$. Clearly then, $GL_2(F) \simeq S_3$.

(b) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(F)$. Then, $\det A = ad - bc \neq 0 \mod 3$. Since $ad = 1$ if $a = 1, d = 1$ or $a = 2, d = 2$, and $ad = 0$ if $a = 0, d = 2$ or $d = 0, a = 2$ or $a = 0, d = 0$ or $a = 0, d = 1$ or $a = 1, d = 0$, and $ad = 2$ if $a = 2, d = 1$ or $a = 1, d = 2$. So, there are $(2)(7) + (5)(4) + (2)(7) = 48$ possibilities for A. So $|GL_2(F)| = 48$.
Let $A \in SL_2(F)$. Then, $\det A = ad - bc = 1 \mod 3$. So, if $ad = 1$, then $bc = 0$. If $ad = 2$, then $bc = 1$. If $ad = 0$, then $bc = 2$. So there are $(2)(5) + (2)(2) + (5)(2) = 24$ possibilities. So $|SL_2(F)| = 24$.

(16) (a) If W is a subspace of V, then there exists some spanning set $w_1, ..., w_k$ of W. Since $W \neq V$, then there exists some vector $v \in V$ such that $v \notin W$, that is, v is not a linear combination of $w_1, ..., w_k$. So, we can add v to this spanning set. If $span(w_1, ..., w_k, v) = V$, then we have $span(v) = U$, and we are done. Otherwise, then we can continue this same process until have a set of vectors $v_1, ..., v_m$ such that $spam(v_1, ..., v_m) = U$. Since none of these vectors are members of W, then $U \cap W = 0$.

(b) Suppose $\dim W + \dim U > \dim V$ and $W \cap U = 0$. Let $w_1, ..., w_k$ be a basis for W, and $u_1, ..., u_m$ be a basis for U. Then $w_1, ..., w_k, u_1, ..., u_m$ is a basis for a subspace of V, denoted X. But $\dim X \leq \dim V$ by definition of a subspace. By contradiction then, $\dim W + \dim U \leq \dim V$.

3.4 Computation with Bases

(1)

$$E = B'P \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} p_{11} + 2p_{21} & p_{12} + 2p_{22} \\ 3p_{11} + 2p_{21} & 3p_{12} + 2p_{22} \end{bmatrix}$$

$$\rightarrow P = \begin{bmatrix} -1/2 & 1/2 \\ 3/4 & -3/4 \end{bmatrix}$$

(2)

$$I = BP \rightarrow P = B$$

$$\rightarrow P = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}$$

(3)

$$E = B'P \rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} p_{11} + p_{21} & p_{12} + p_{22} \\ p_{11} - p_{21} & p_{12} - p_{22} \end{bmatrix}$$

$$\rightarrow P = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{bmatrix}$$

(4)

$$E = B'P \rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} p_{11} - p_{21}/2 & p_{12} - p_{22}/2 \\ \sqrt{3}p_{21}/2 & \sqrt{3}p_{22}/2 \end{bmatrix}$$

$$\rightarrow P = \begin{bmatrix} 1 & 1/\sqrt{3} \\ 0 & 2/\sqrt{3} \end{bmatrix}$$

(5) (i) If we can find a P such that $B = EP$, then B is a basis for $\mathbb{R}^3$, since E is a basis. Clearly,

$$P = B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{bmatrix}$$

(ii)

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -1/7 & 4/7 & -1/7 \\ -2/7 & 1/7 & 5/7 \\ 4/7 & -2/7 & -3/7 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 4/7 \\ 15/7 \\ -9/7 \end{bmatrix}$$

(iii)

$$B' = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

1

$$B = B'P \rightarrow BB'^{-1} = P$$

$$\rightarrow \begin{bmatrix} -1/2 & 1 & 1/2 \\ 0 & 0 & 1 \\ 1/2 & 0 & -1/2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{bmatrix} = P$$

$$\rightarrow P = \begin{bmatrix} 3/2 & 1 & 0 \\ 0 & 2 & 1 \\ 1/2 & 0 & 1 \end{bmatrix}$$

(iv) B must be invertible. So, p and $\det B$ must be relatively prime. So, B is a basis of $\mathbb{F}_p^3$ for all p excluding $p = 7$.

(6) The two bases are related by: $[B] = [B']P$. $[B']$ is invertible, so therefore $P = [B']^{-1}[B]$.

(7) Note that each step corresponds to elementary matrices. There exists some P such that $B = B'P$. Since P is invertible, then we can write P as a product of elementary matrices, proving the statement.

(8) Since L is in the span of S, then there exists a matrix A such that $SA = L$. Let U be a linear combination of vectors of L: $U = LC = SAC$. If AC is the 0 matrix, then $U = 0$. If $AC = 0$ has a nontrivial solution (solving for C), then L is linearly dependent. But if $|S| < |L|$, then $AC = 0$ has a nontrivial solution: therefore $|S| \geq |L|$.

(9) Let $(v_1, ..., v_n)$ be a basis of F^n. Then, $\varphi((v_1, ..., v_n)) = [v_1|...|v_n]$. Clearly, φ is injective, and surjective onto $GL_n(F)$.

(10)

$$\frac{(81^3 - 1)}{81 - 1} = 6643$$

(11) (a)

$$|SL_2(F)| = \frac{1}{p-1}(p^2 - 1)(p^2 - p) = p(p^2 - 1)$$

(b)

$$|GL_n(F)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$$

$$|SL_n(f)| = \frac{1}{p-1}|GL_n(F)|$$

$$|\mathcal{B}| = |GL_n(F)|$$

(12) (a) Suppose B is the left inverse of A. Note that if $n - m$ rows of zeros are added to the bottom of A to form A', then the left inverse B' also contains B. But, since B' does not exist, then B also does not exist.

More concretely, suppose B exists. Since $(BA)_{ii} = 1$, then now column of A can be all 0s. Then, consider the first row of BA. The ith element of the first row is

$$c_i = \sum_j a_{ji} b_{1j}$$

Since $c_2 = ... = c_n = 0$ with $m < n$, then $b_{11} = ... = b_{1m}$. But then $c_1 = 0$, a contradiction. Thus, B cannot exist.

(b) Define P, P' such that $B = B'P', B' = BP$, ie. P, P' are matrices of change of basis. So, $P'P = I, PP' = I$. So, $P' = P^{-1}, P = P'^{-1}$. Thus, $m = n$.