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 $0 \le r \le n$. 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 $a_{ij} = \overline{a}_{ji}$ 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 $(e_1, \dots, e_n)$ and the new basis is $(e_n, e_{n-1}, \dots, e_1)$.
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 $\mathbf{B} = (v_1, \dots, v_n)$ 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.