(here the primes denote derivatives with respect to t). Let A be the matrix whose i, j entry is a_{ij}, so that $(*)$ may be written as

$$\begin{pmatrix} y_1' \\ y_2' \\ \vdots \\ y_n' \end{pmatrix} = A \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

or, more succinctly, as $y' = Ay$, where y is the column vector of functions $y_1(t), \ldots, y_n(t)$.

An $n \times n$ matrix whose entries are functions of t and whose columns are independent solutions to the system $(*)$ is called a *fundamental matrix* of $(*)$. By the theory of differential equations, the set of vectors y that are solutions to the system $(*)$ form an n-dimensional vector space over K and so the columns of a fundamental matrix are a *basis for the vector space of all solutions to* $(*)$.

53. Prove that $\exp(At)$ is a fundamental matrix of $(*)$. Show also that if C is the $n \times 1$ constant vector whose entries are $y_1(0), \ldots, y_n(0)$ then $y(t) = \exp(At)C$ is the particular solution to the system $(*)$ satisfying the initial condition $y(0) = C$. (Note how this generalizes the 1-dimensional result that the single differential equation $y' = ay$ has e^{at} as a basis for the 1-dimensional space of solutions and the unique solution to this differential equation satisfying the initial condition $y(0) = c$ is $y = ce^{at}$.) [Use the preceding exercises.]

54. Prove that if M is a fundamental matrix of $(*)$ and if Q is a nonsingular matrix in $M_n(K)$, then MQ is also a fundamental matrix of $(*)$. [The columns of MQ are linear combinations of the columns of M.]

Now apply the preceding two exercises to solve some specific systems of differential equations as follows: given the matrix A in a system $(*)$, calculate a change of basis matrix P such that $B = P^{-1}AP$ is in Jordan canonical form. Then $\exp(At) = P\exp(Bt)P^{-1}$ is a fundamental matrix for $(*)$. By the preceding exercise, $P\exp(Bt)$ is also a fundamental matrix for $(*)$ and $\exp(Bt)$ can be calculated by the method described in the discussion following Exercise 45 (in particular, one does not have to find the inverse of the matrix P to obtain a fundamental matrix for $(*)$). Thus, for example, if $A = D$ and P are the matrices given in Exercise 46, then we saw that the Jordan canonical form for A is the matrix $B = P^{-1}AP$ consisting of two 2×2 Jordan blocks with eigenvalues 1. A fundamental matrix for the system $y' = Ay$ is therefore

$$P\exp(B) = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 2 & 0 & -2 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} e^t & te^t & 0 & 0 \\ 0 & e^t & 0 & 0 \\ 0 & 0 & e^t & te^t \\ 0 & 0 & 0 & e^t \end{pmatrix} = \begin{pmatrix} 0 & e^t & 2e^t & 2te^t \\ 2e^t & 2te^t & -2e^t & e^t(1-2t) \\ e^t & te^t & 0 & 0 \\ 0 & 0 & e^t & te^t \end{pmatrix}.$$

Writing this out more explicitly, this shows that the general solution to the system of differential equations

$$\begin{aligned} y_1' &= y_1 + 2y_2 - 4y_3 + 4y_4 \\ y_2' &= 2y_1 - y_2 + 4y_3 - 8y_4 \\ y_3' &= y_1 + y_3 - 2y_4 \\ y_4' &= y_2 - 2y_3 + 3y_4 \end{aligned}$$

is given by

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \alpha_1 \begin{pmatrix} 0 \\ 2e^t \\ e^t \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} e^t \\ 2te^t \\ te^t \\ 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 2e^t \\ -2e^t \\ 0 \\ e^t \end{pmatrix} + \alpha_4 \begin{pmatrix} 2te^t \\ e^t(1-2t) \\ 0 \\ te^t \end{pmatrix}$$

where $\alpha_1, \ldots, \alpha_4$ are arbitrary elements of the field K (this describes the 4-dimensional vector space of solutions).

55. In each of Parts (a) to (c) find a fundamental matrix for the system (*), where the coefficient matrix A of (*) is specified.
- **(a)** A is the matrix in Part (a) of Exercise 47.
- **(b)** A is the matrix in Part (b) of Exercise 47.
- **(c)** A is the matrix in Part (c) of Exercise 47.

56. Consider the system (*) whose coefficient matrix A is the matrix D listed in Exercise 46 and whose fundamental matrix was computed just before the preceding exercise. Find the particular solution to (*) that satisfies the initial condition $y_i(0) = 1$ for $i = 1, 2, 3, 4$.

Next we explore a special case of (*). Given the linear n^{th} *order* differential equation with constant coefficients

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y = 0 \qquad (**)$$

(where $y^{(k)}$ is the k^{th} derivative of y and $y^{(0)} = y$) one can form a *system* of linear *first order* differential equations by letting $y_i = y^{(i-1)}$ for $1 \leq i \leq n$ (the coefficient matrix of this system is described in the next exercise). A basis for the n-dimensional vector space of solutions to the n^{th} order equation (**) may then obtained from a fundamental matrix for the linear system. Specifically, in each of the $n \times 1$ columns of functions in a fundamental matrix for the system, the 1, 1 entry is a solution to (**) and so the n functions in the first row of the fundamental matrix for the system form a basis for the solutions to (**).

57. Prove that the matrix, A, of coefficients of the system of n first order equations obtained from (**) is the transpose of the companion matrix of the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.

58. Use the above methods to find a basis for the vector space of solutions to the following differential equations
- **(a)** $y''' - 3y' + 2y = 0$
- **(b)** $y'''' + 4y''' + 6y'' + 4y' + y = 0$.

A system of differential equations

$$\begin{aligned} y_1' &= F_1(y_1, y_2, \ldots, y_n) \\ y_2' &= F_2(y_1, y_2, \ldots, y_n) \\ &\vdots \\ y_n' &= F_n(y_1, y_2, \ldots, y_n) \end{aligned}$$

where $F_1, F_2, \ldots, F_n$ are functions of n variables, is called an *autonomous* system and it will be written more succinctly as $y' = F(y)$, where $F = (F_1, \ldots, F_n)$. (The expression autonomous means "independent of time" and it indicates that the variable t — which may be thought of as a time variable — does not appear explicitly on the right hand side.) The system (*) is the special type of autonomous system in which each F_i is a linear function. In many instances it is desirable to analyze the behavior of solutions to an autonomous system of differential equations without explicitly finding these solutions (indeed, it is unlikely that it will be possible to find explicit solutions for a given nonlinear system). This investigation falls under the rubric "qualitative analysis" of autonomous differential equations and the rudiments of this study are often treated in basic calculus courses for 1×1 systems. The first step in a qualitative analysis of an $n \times n$ autonomous system is to find the *steady states*, namely the

constant solutions (these are called steady states since they do not change with t). Note that a constant function $y = c$, where c is the $n \times 1$ constant vector with entries $c_1, \ldots, c_n$, is a solution to $y' = F(y)$ if and only if

$$c_i' = 0 = F_i(c_1, \ldots, c_n) \quad \text{for } i = 1, 2, \ldots, n,$$

so the steady states are found by computing the zeros of F (in the case of a nonlinear system this may require numerical methods). Next, given the initial value of some solution, one wishes to analyze the behavior of this solution as $t \to \infty$. This is called the *asymptotic behavior* of the solution. Again, it may not be possible to find the solution explicitly, although by the general theory of differential equations a solution to the initial value problem is unique provided the functions F_i are differentiable. A steady state $y = c$ is called *globally asymptotically stable* if every solution tends to c as $t \to \infty$, i.e., for any solution $y(t)$ we have $\lim_{t \to \infty} y_i(t) = c_i$ for all $i = 1, 2, \ldots, n$.

In the case of the linear autonomous system $(*)$ the solutions form a vector space, so the only constant solution is the zero solution. The next exercise gives a *sufficient* condition for zero to be globally asymptotically stable and it gives one example of how the behavior of a linear system may be analyzed in terms of the eigenvalues of its coefficient matrix. Nonlinear systems can be approximated by linear systems in some neighborhood of a steady state by considering $y' = Ty$, where $T = \left(\dfrac{\partial F_i}{\partial y_j} \right)$ is the $n \times n$ Jacobian matrix of F evaluated at the steady state point. In this way the analysis of linear systems plays an important role in the local analysis of general autonomous systems.

59. Prove that the solution of $(*)$ given by $y_i(t) = 0$ for all $i \in \{1, \ldots, n\}$ (i.e., the zero solution) is globally asymptotically stable if all the eigenvalues of A have negative real parts. [For those unfamiliar with the behavior of the complex exponential function, assume all eigenvalues are real (hence are negative real numbers). Use the explicit nature of the solutions to show that they all tend to zero as $t \to \infty$.]

Part IV

FIELD THEORY AND GALOIS THEORY

The previous sections have developed the theory of some of the basic algebraic structures of groups, rings and fields. The next two chapters consider properties of fields, particularly fields which arise from trying to solve equations (such as the simple equation $x^2 + 1 = 0$), and fields which naturally arise in trying to perform "arithmetic" (adding, subtracting, multiplying and dividing). The elegant and beautiful Galois Theory relates the structure of *fields* to certain related *groups* and is one of the basic algebraic tools. Applications include solutions of classical compass and straightedge construction questions, finite fields and Abel's famous theorem on the insolvability (by radicals) of the general quintic polynomial.

CHAPTER 13

Field Theory

13.1 BASIC THEORY OF FIELD EXTENSIONS

Recall that a field F is a commutative ring with identity in which every nonzero element has an inverse. Equivalently, the set $F^\times = F - \{0\}$ of nonzero elements of F is an abelian group under multiplication.

One of the first invariants associated with any field F is its *characteristic*, defined as follows: If 1_F denotes the identity of F, then F contains the elements 1_F, $1_F + 1_F$, $1_F + 1_F + 1_F, \ldots$ of the additive subgroup of F generated by 1_F, which may not all be distinct. For n a positive integer, let $n \cdot 1_F = 1_F + \cdots + 1_F$ (n times). Then two possibilities arise: either all the elements $n \cdot 1_F$ are distinct, or else $n \cdot 1_F = 0$ for some positive integer n.

Definition. The *characteristic* of a field F, denoted $\mathrm{ch}(F)$, is defined to be the smallest positive integer p such that $p \cdot 1_F = 0$ if such a p exists and is defined to be 0 otherwise.

It is easy to see that

$$n \cdot 1_F + m \cdot 1_F = (m+n) \cdot 1_F \qquad \text{and that}$$
$$(n \cdot 1_F)(m \cdot 1_F) = mn \cdot 1_F \tag{13.1}$$

for positive integers m and n. It follows that the characteristic of a field is either 0 or a *prime* p (hence the choice of p in the definition above), since if $n = ab$ is composite with $n \cdot 1_F = 0$, then $ab \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F) = 0$ and since F is a field, one of $a \cdot 1_F$ or $b \cdot 1_F$ is 0, so the smallest such integer is necessarily a prime. It also follows that if $n \cdot 1_F = 0$, then n is divisible by p.

Proposition 1. The characteristic of a field F, $\mathrm{ch}(F)$, is either 0 or a prime p. If $\mathrm{ch}(F) = p$ then for any $\alpha \in F$,

$$p \cdot \alpha = \underbrace{\alpha + \alpha + \cdots + \alpha}_{p \text{ times}} = 0.$$

Proof: Only the second statement has not been proved, and this follows immediately from the evident equality $p \cdot \alpha = p \cdot (1_F \alpha) = (p \cdot 1_F)(\alpha)$ in F.