Algebra

6

Key Topics

Simultaneous equations
Quadratic equations
Polynomials
Indices
Logs
Abstract Algebra
Groups
Rings
Fields
Vector Spaces

6.1 Introduction

Algebra is the branch of mathematics that uses letters in the place of numbers, where the letters stand for variables or constants that are used in mathematical expressions. Algebra is the study of such mathematical symbols and the rules for manipulating them, and it is a powerful tool for problem solving in science and engineering.

The origins of algebra are in work done by Islamic mathematicians during the Golden age in Islamic civilization, and the word '*algebra*' comes from the Arabic '*al-jabr*', which appears as part of the title of a book by the Islamic mathematician,

G. O'Regan, *Guide to Discrete Mathematics*, Texts in Computer Science,
DOI 10.1007/978-3-319-44561-8_6

Al Khwarizmi, in the ninth century A.D. The third century A.D. Hellenistic mathematician, Diophantus, also did early work on algebra.

Algebra covers many areas such as elementary algebra, linear algebra and abstract algebra. Elementary algebra includes the study of symbols and rules for manipulating them to form valid mathematical expressions; simultaneous equations; quadratic equations; polynomials; indices and logarithms. Linear algebra is concerned with the solution of a set of linear equations, and the study of matrices (see Chap. 8) and vectors. Abstract algebra is concerned with the study of abstract algebraic structures such as monoids, groups, rings, integral domains, fields and vector spaces.

6.2 Simple and Simultaneous Equations

A simple equation is an equation with one unknown, and the unknown may be on both the left-hand side and right-hand side of the equation. The method of solving such equations is to bring the unknowns to one side of the equation, and the values to the other side.

Simultaneous equations are equations with two (or more) unknowns. There are a number of methods to find a solution to two simultaneous equations such as elimination, substitution and graphical techniques. The solution of n linear equations with n unknowns may be done using Gaussian elimination and matrix theory (see Chap. 8).

Example (**Simple Equation**) Solve the simple equation $4 - 3x = 2x - 11$

Solution (**Simple Equation**)

$$\begin{aligned}
&4 - 3x = 2x - 11\\
&4 - (-11) = 2x - (3x)\\
&4 + 11 = 2x + 3x\\
&15 = 5x\\
&3 = x
\end{aligned}$$

Example (**Simultaneous Equation—Substitution Method**) Solve the following simultaneous equations by the method of substitution.

$$\begin{aligned}
x + 2y &= -1\\
4x - 3y &= 18
\end{aligned}$$

Solution

(**Simultaneous Equation—Substitution Method**) The method of substitution involves expressing x in terms of y and substituting it in the other equation (or vice versa expressing y in terms of x and substituting it in the other equation). For this example, we use the first equation to *express* x in terms of y.

$$\begin{aligned}x + 2y &= -1\\ x &= -1 - 2y\end{aligned}$$

We then substitute for x $(-1 - 2y)$ in the second equation, and we get a simple equation involving just the unknown y.

$$\begin{aligned}&4(-1-2y) - 3y = 18\\ &\Rightarrow -4 - 8y - 3y = 18\\ &\Rightarrow -11y = 18 + 4\\ &\Rightarrow -11y = 22\\ &\Rightarrow y = -2\end{aligned}$$

We then obtain the value of x from the substitution

$$\begin{aligned}&x = -1 - 2y\\ &\Rightarrow x = -1 - 2(-2)\\ &\Rightarrow x = -1 + 4\\ &\Rightarrow x = 3\end{aligned}$$

We can then verify that our solution is correct by checking our answer for both equations.

$$\begin{aligned}3 + 2(-2) &= -1 \quad ✓\\ 4(3) - 3(-2) &= 18 \quad ✓\end{aligned}$$

Example (**Simultaneous Equation—Method of Elimination**) Solve the following simultaneous equations by the method of elimination.

$$\begin{aligned}3x + 4y &= 5\\ 2x - 5y &= -12\end{aligned}$$

Solution

(**Simultaneous Equation—Method of Elimination**) The approach is to manipulate both equations so that we may eliminate either x or y, and so reduce to a simple equation with just x or y. For this example, we are going to eliminate x, and so we multiply equation (1) by 2 and equation (2) by –3 and this yields two equations with the opposite coefficient of x.

$$\begin{aligned}
&6x + 8y = 10\\
&-6x + 15y = 36\\
&-\,-\,-\,-\,-\,-\,-\,-\,-\\
&0x + 23y = 46\\
&\qquad\quad y = 2
\end{aligned}$$

We then add both equations together and conclude that $y = 2$. We then determine the value of x by replacing y with 2 in equation (1).

$$\begin{aligned}
&3x + 4(2) = 5\\
&3x + 8 = 5\\
&3x = 5 - 8\\
&3x = -3\\
&x = -1
\end{aligned}$$

We can then verify that our solution is correct as before by checking our answer for both equations

Example (**Simultaneous Equation—Graphical Techniques**) Find the solution to the following simultaneous equations using graphical techniques:

$$\begin{aligned}
&x + 2y = -1\\
&4x - 3y = 18
\end{aligned}$$

Solution
(**Simultaneous Equation—Graphical Techniques**) Each simultaneous equation represents a straight line, and so the solution to the two simultaneous equations is the point of intersection of both lines (if there is such a point). Therefore, the solution involves drawing each line and finding the point of intersection of both lines (Fig. 6.1).

First we find two points on line 1: e.g. (0, −0.5) and (−1, 0) are on line 1, since when $x = 0$ we have $2y = -1$ and so $y = -0.5$. Similarly, when $y = 0$ we have $x = -1$. Next we find two points on line 2 in a similar way: e.g. when x is 0 y is –6 and when y is 0 we have $x = 4.5$ and so the points (0–6) and (4.5, 0) are on line 2.

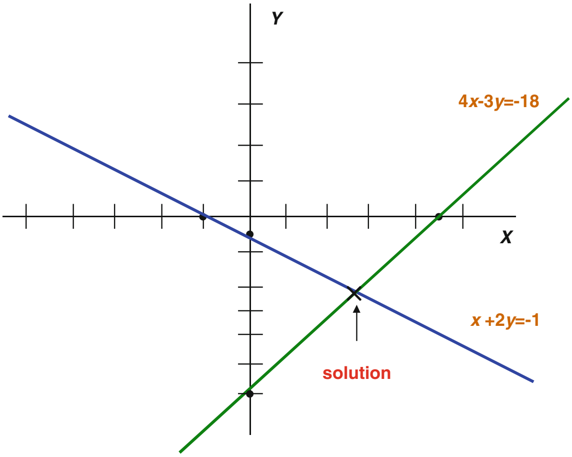

Fig. 6.1 Graphical solution to simultaneous equations

We then draw the *X* axis and the *Y* axis, draw the scales on the axes, label the axes, plot the points and draw both lines. Finally, we find the point of intersection of both lines (if there is such a point), and this is our solution to the simultaneous equations.

For this example, there is a point of intersection for the lines, and so we determine the *x* and *y* coordinate and the solution is then given by $x = 3$ and $y = -2$. The solution using graphical techniques requires care (as inaccuracies may be introduced from poor drawing) and graph paper is required for accuracy.

6.3 Quadratic Equations

A quadratic equation is an equation of the form $ax^2 + bx + c = 0$, and solving the quadratic equation is concerned with finding the unknown value *x* (roots of the quadratic equation). There are several techniques to solve quadratic equations such as factorization; completing the square; the quadratic formula; and graphical techniques.

Example (**Quadratic Equations—Factorization**) Solve the quadratic equation $3x^2 - 11x - 4 = 0$ by factorization.

Solution
(**Quadratic Equations—Factorization**) The approach taken is to find the factors of the quadratic equation. Sometimes this is easy, but often other techniques will need to be employed. For the above quadratic equation we note immediately that its factors are $(3x + 1)(x - 4)$ since

$$\begin{aligned}&(3x+1)(x-4)\\&=3x^2-12x+x-4\\&=3x^2-11x-4\end{aligned}$$

Next, we note the property that if the product of two numbers A and B is 0 then either A is 0 or B is 0. Another words, $AB = 0 => A = 0$ or $B = 0$. We conclude from this property that as

$$\begin{aligned}&3x^2-11x-4=0\\ \Rightarrow\ &(3x+1)(x-4)=0\\ \Rightarrow\ &(3x+1)=0 \text{ or } (x-4)=0\\ \Rightarrow\ &3x=-1 \text{ or } x=4\\ \Rightarrow\ &x=-0.33 \text{ or } x=4\end{aligned}$$

Therefore, the solution (or roots) of the quadratic equation $3x^2 – 11x –4 = 0$ are $x = −0.33$ or $x = 4$.

Example (**Quadratic Equations—Completing the Square**) Solve the quadratic equation $2x^2 + 5x − 3 = 0$ by completing the square.

Solution
(**Quadratic Equations—Completing the Square**) First we convert the quadratic equation to an equivalent quadratic with a unary coefficient of x^2. This involves division by 2. Next, we examine the coefficient of x (in this case 5/2) and we add the square of half the coefficient of x to both sides. This allows us to complete the square, and we then to take the square root of both sides. Finally, we solve for x.

$$\begin{aligned}&2x^2+5x-3=0\\ \Rightarrow\ &x^2+5/2x-3/2=0\\ \Rightarrow\ &x^2+5/2x=3/2\\ \Rightarrow\ &x^2+5/2x+(5/4)^2=3/2+(5/4)^2\\ \Rightarrow\ &(x+5/4)^2=3/2+(25/16)\\ \Rightarrow\ &(x+5/4)^2=29/16+(25/16)\\ \Rightarrow\ &(x+5/4)^2=49/16\\ \Rightarrow\ &(x+5/4)=\pm 7/4\\ \Rightarrow\ &x=-5/4\pm 7/4\\ \Rightarrow\ &x=-5/4-7/4 \text{ or } x=-5/4+7/4\\ \Rightarrow\ &x=-12/4 \text{ or } x=2/4\\ \Rightarrow\ &x=-3 \text{ or } x=0.5\end{aligned}$$

Example 1 (**Quadratic Equations—Quadratic Formula**) Establish the quadratic formula for solving quadratic equations.

Solution

(**Quadratic Equations—Quadratic Formula**) We complete the square and the result will follow.

$$\begin{aligned}
&ax^2+bx+c = 0\\
&\Rightarrow x^2+b/ax+c/a = 0\\
&\Rightarrow x^2+b/ax = -c/a\\
&\Rightarrow x^2+b/ax+(b/2a)^2 = -c/a+(b/2a)^2\\
&\Rightarrow (x+b/2a)^2 = -c/a+(b/2a)^2\\
&\Rightarrow (x+b/2a)^2 = \frac{-4ac}{4a^2}+\frac{b^2}{4a^2}\\
&\Rightarrow (x+b/2a)^2 = \frac{b^2-4ac}{4a^2}\\
&\Rightarrow (x+b/2a) = \pm\frac{\sqrt{b^2-4ac}}{2a}\\
&\Rightarrow x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}
\end{aligned}$$

Example 2 (**Quadratic Equations—Quadratic Formula**) Solve the quadratic equation $2x^2 + 5x - 3 = 0$ using the quadratic formula.

Solution

(**Quadratic Equations—Quadratic Formula**) For this example $a = 2$; $b = 5$; and $c = -3$, and we put these values into the quadratic formula.

$$\begin{aligned}
&x = \frac{-5\pm\sqrt{5^2-4.2.(-3)}}{2.2} = \frac{-5\pm\sqrt{25+24}}{4}\\
&x = \frac{-5\pm\sqrt{49}}{4} = \frac{-5\pm 7}{4}\\
&x = 0.5 \text{ or } x = -3.
\end{aligned}$$

Example (**Quadratic Equations—Graphical Techniques**) Solve the quadratic equation $2x^2 - x - 6 = 0$ using graphical techniques given that the roots of the quadratic equation lie between $\boldsymbol{x} = -3$ and $x = 3$

Solution

(**Quadratic Equations—Graphical Techniques**) The approach is first to create a table of values (Table 6.1) for the curve $y = 2x^2 - x - 6$, and to draw the X and

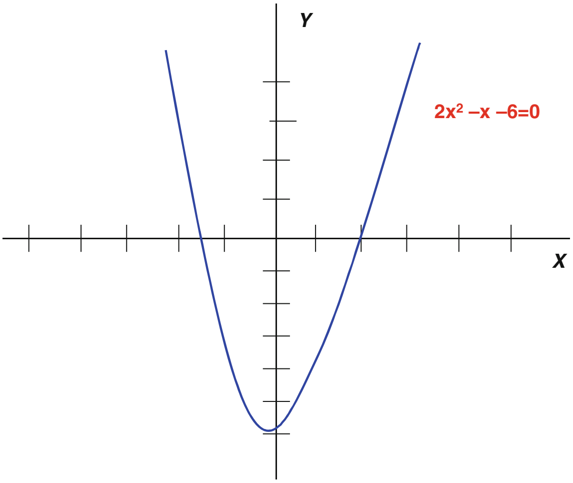

Fig. 6.2 Graphical solution to quadratic equation

Table 6.1 Table of values for quadratic equation

x	−3	−2	−1	0	1	2	3
$y = 2x^2 - x - 6$	15	4	−3	−6	−5	0	9

Y axis and scales, and then to plot the points from the table of values, and to join the points together to form the curve (Fig. 6.2).

The graphical solution is to the quadratic equation is then given by the points where the curve intersects the *X* axis (i.e. $y = 0$ on the *X* axis). There may be no solution (i.e. the curve does not intersect the *X* axis), one solution (a double root), or two solutions.

The graph for the curve $y = 2x^2 - x - 6$ is given below, and so the points where the curve intersects the *X* axis are determined. We note from the graph that the curve intersects the *X* axis at two distinct points, and we see from the graph that the roots of the quadratic equation are given by $x = -1.5$ and $x = 2$.

The solution to quadratic equations using graphical techniques requires care (as with the solution to simultaneous equations using graphical techniques), and graph paper is required for accuracy.

6.4 Indices and Logarithms

The product *a.a.a.a.....a* (*n* times) is denoted by a^n, and the number *n* is the index of *a*. The following are properties of indices:

$$
\begin{aligned}
&a^{\mathrm{o}} = 1\\
&a^{m+n} = a^m.a^n\\
&a^{mn} = (a^m)^n\\
&a^{-n} = \frac{1}{a^n}\\
&a^{\frac{1}{n}} = \sqrt[n]{a}
\end{aligned}
$$

Logarithms are closely related to indices, and if the number b can be written in the form $b = a^x$, then we say that log to the base a of b is x: i.e. $\log_a b = x \Leftrightarrow a^x = b$. Clearly, $\log_{10} 100 = 2$ since $10^2 = 100$. The following are properties of logarithms:

$$
\begin{aligned}
&\log_a AB = \log_a A + \log_a B\\
&\log_a A^n = n \log_a A\\
&\log \frac{A}{B} = \log A - \log B
\end{aligned}
$$

We will prove the first property of logarithms. Suppose $\log_a A = x$ and $\log_a B = y$. Then $A = a^x$ and $B = a^y$ and so $AB = a^x a^y = a^{x+y}$ and so $\log_a AB = x + y = \log_a A + \log_a B$.

The law of logarithms may be used to solve certain equations involving powers (called indicial equations). We illustrate this by an example

Example (**Indicial Equations**) Solve the equation $2^x = 3$, correct to 4 significant places.

Solution
(**Indicial Equations**)

$$
\begin{aligned}
&2^x = 3\\
&\Rightarrow \log_{10} 2^x = \log_{10} 3\\
&\Rightarrow x \log_{10} 2 = \log_{10} 3\\
&\Rightarrow x = \frac{\log_{10} 3}{\log_{10} 2}\\
&\quad = \frac{0.4771}{0.3010}\\
&\Rightarrow x = 1.585
\end{aligned}
$$

6.5 Horner's Method for Polynomials

Horner's Method is a computationally efficient way to evaluate a polynomial function. It is named after William Horner who was a nineteenth century British mathematician and schoolmaster. Chinese mathematicians were familiar with the method in the third century A.D.

The normal method for the evaluation of a polynomial involves computing exponentials, and this is computationally expensive. Horner's method has the advantage that fewer calculations are required, and it eliminates all exponentials using nested multiplication and addition. It also provides a computationally efficient way to determine the derivative of the polynomial.

Horner's Method and Algorithm

Consider a polynomial $P(x)$ of degree n defined by

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0$$

The Horner method to evaluate $P(x_0)$ essentially involves writing $P(x)$ as

$$P(x) = (((a_n x + a_{n-1})x + a_{n-2})x + \cdots + a_1)x + a_0$$

The computation of $P(x_0)$ involves defining a set of coefficients b_k such that

$$\begin{aligned}
b_n &= a_n \\
b_{n-1} &= a_{n-1} + b_n x_0 \\
&\ldots\ldots \\
b_k &= a_k + b_{k+1} x_0 \\
&\ldots\ldots \\
b_1 &= a_1 + b_2 x_0 \\
b_0 &= a_0 + b_1 x_0
\end{aligned}$$

Then the computation of $P(x_0)$ is given by

$$P(x_0) = b_0$$

Further, if $Q(x) = b_n x^{n-1} + b_{n-1} x^{n-2} + b_{n-2} x^{n-3} + \cdots + b_1$ then it is easy to verify that

$$P(x) = (x - x_0)\mathrm{Q}(x) + b_0$$

This also allows the derivative of $P(x)$ to be easily computed for x_0 since

$$P'(x) = Q(x) + (x - x_0)Q'(x)$$
$$P'(x_0) = Q(x_0)$$

Algorithm (*To evaluate polynomial and its derivative*)

(i) Initialize y to a_n and z to a_n (Compute b_n for P and b_{n-1} for Q)
(ii) For each j from $n - 1$, $n - 2$ to 1 compute b_j for P and b_{j-1} for Q by Set y to $x_0y + a_j$ (i.e. b_j for P) and z to $x_0z + y$ (i.e. b_{j-1} for Q)
(iii) Compute b_0 by setting y to $x_0y + a_0$

Then $P(x_0) = y$ and $P'(x_0) = z$.

6.6 Abstract Algebra

One of the important features of modern mathematics is the power of the abstract approach. This has opened up whole new areas of mathematics, and it has led to a large body of new results and problems. The term '*abstract*' is subjective, as what is abstract to one person may be quite concrete to another. We shall introduce some important algebraic structures in this section including monoids, groups, rings, fields, and vector spaces.

6.6.1 Monoids and Groups

A non-empty set M together with a binary operation '*' is called a *monoid* if for all elements $a, b, c \in M$ the following properties hold

(1) $a * b \in M$	(Closure property)
(2) $a * (b * c) = (a * b) * c$	(Associative property)
(3) $\exists u \in M$ such that: $a * u = u * a = a$ ($\forall a \in M$)	(Identity element)

A monoid is commutative if $a * b = b * a$ for all $a, b \in M$. A *semi-group* $(M, *)$ is a set with a binary operation '*' such that the closure and associativity properties hold (but it may not have an identity element).

Example 6.1 (**Monoids**)

(i) The set of sequences Σ* under concatenation with the empty sequence Λ the identity element.

(ii) The set of integers under addition forms an infinite monoid in which 0 is the identity element.

A non-empty set G together with a binary operation '*' is called a *group* if for all elements $a,b,c \in G$ the following properties hold

(1) $a * b \in G$	(Closure property)
(2) $a * (b * c) = (a * b) * c$	(Associative property)
(3) $\exists e \in G$ such that: $a * e = e * a = a$ $(\forall a \in G)$	(Identity element)
(4) For every $a \in G$, $\exists a^{-1} \in G$, such that: $a * a^{-1} - a^{-1} * a = e$	(Inverse element)

The identity element is unique, and the inverse a^{-1} of an element a is unique (see Exercise 5). A *commutative group* has the additional property that $a * b = b * a$ for all $a, b \in G$. The order of a group G is the number of elements in G, and is denoted by $o(G)$. If the order of G is finite then G is said to be a finite group.

Example 6.1 (**Groups**)

(i) The set of integers under addition $(\mathbb{Z}, +)$ forms an infinite group in which 0 is the identity element.

(ii) The set of integer 2 × 2 matrices under addition, where the identity element is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(iii) The set of integers under multiplication $(\mathbb{Z}, \times)$ forms an infinite monoid with 1 as the identity element.

A *cyclic group* is a group where all elements $g \in \mathrm{G}$ are obtained from the powers a^i of one element $a \in \mathrm{G}$, with $a^0 = e$. The element 'a' is termed the generator of the cyclic group G. A finite cyclic group with n elements is of the form $\{a^0, a^1, a^2, \ldots.., a^{n-1}\}$.

A non-empty subset H of a group G is said to be a *subgroup* of G if for all $a, b \in H$ then $a * b \in H$, and for any $a \in H$ then $a^{-1} \in H$. A subgroup N is termed a *normal subgroup* of G if $gng^{-1} \in G$ for all $g \in G$ and all $n \in N$. Further, if G is a group and N is a normal subgroup of G, then the *quotient group* G/N may be formed.

Lagrange's theorem states the relationship between the order of a subgroup H of G, and the order of G. The theorem states that if G is a finite group, and H is a subgroup of G, then $o(H)$ is a divisor of $o(G)$.

We may also define mapping between similar algebraic structures termed *homomorphism*, and these mapping preserve structure. If the homomorphism is one to one and onto it is termed an *isomorphism*, which means that the two structures are identical in some sense (apart from a relabelling of elements).

6.6.2 Rings

A *ring* is a non-empty set R together with two binary operations '+' and '×' where (R, +) is a commutative group; (R, ×) is a semi-group; and the left and right distributive laws hold. Specifically, for all elements $a, b, c \in$ R the following properties hold:

(1) $a + b \in R$	(Closure property)
(2) $a + (b + c) = (a + b) + c$	(Associative property)
(3) $\exists 0 \in R$ such that $\forall a \in R$: $a + 0 = 0 + a = a$	(Identity element)
(4) $\forall a \in R$: $\exists(-a) \in R$: $a + (-a) = (-a) + a = 0$	(Inverse element)
(5) $a + b = b + a$	(Commutativity)
(6) $a \times b \in R$	(Closure property)
(7) $a \times (b \times c) = (a \times b) \times c$	(Associative property)
(8) $a \times (b + c) = a \times b + a \times c$	(Distributive law)
(9) $(b + c) \times a = b \times a + c \times a$	(Distributive law)

The element 0 is the identity element under addition, and the additive inverse of an element a is given by $-a$. If a ring (R, ×, +) has a multiplicative identity 1 where $a \times 1 = 1 \times a = a$ for all $a \in R$ then R is termed a ring with a unit element. If $a \times b = b \times a$ for all a, $b \in R$ then R is termed a *commutative ring*.

An element $a \neq 0$ in a ring R is said to be a *zero divisor* if there exists $b \in R$, with $b \neq 0$ such that $ab = 0$. A commutative ring is an *integral domain* if it has no zero divisors. A ring is said to be a *division ring* if its non-zero elements form a group under multiplication.

Example 6.2 (**Rings**)

(i) The set of integers ($\mathbb{Z}$, +, ×) forms an infinite commutative ring with multiplicative unit element 1. Further, since it has no zero divisors it is an integral domain.

(ii) The set of integers mod 4 (i.e. $\mathbb{Z}_4$ where addition and multiplication is performed modulo 4)[1] is a finite commutative ring with unit element $[1]_4$. Its elements are $\{[0]_4, [1]_4, [2]_4, [3]_4\}$. It has zero divisors since $[2]_4[2]_4 = [0]_4$ and so it is not an integral domain.

[1] Recall from Chap. 3 that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{[a]_n\text{: } 0 \leq a \leq n - 1\} = \{[0]_n, [1]_n, \ldots., [n - 1]_n\}$.

(iii) The Quaternions (discussed in [1]) are an example of a non-commutative ring (they form a division ring).

(iv) The set of integers mod 5 (i.e. $\mathbb{Z}_5$ where addition and multiplication is performed modulo 5) is a finite commutative division ring[2] and it has no zero divisors.

6.6.3 Fields

A *field* is a non-empty set F together with two binary operation '+' and '×' where (F, +) is a commutative group; $(F\backslash\{0\}, \times)$ is a commutative group; and the distributive properties hold. The properties of a field are

(1) $a + b \in F$	(Closure property)
(2) $a + (b + c) = (a + b) + c$	(Associative property)
(3) $\exists 0 \in F$ such that $\forall a \in F\ a + 0 = 0 + a = a$	(Identity Element)
(4) $\forall a \in F\ \exists(-a) \in F\ a + (-a) = (-a) + a = 0$	(Inverse Element)
(5) $a + b = b + a$	(Commutativity)
(6) $a \times b \in F$	(Closure property)
(7) $a \times (b \times c) = (a \times b) \times c$	(Associative property)
(8) $\exists 1 \in F$ such that $\forall a \in F\ a \times 1 = 1 \times a = a$	(Identity Element)
(10) $\forall a \in F\backslash\ \{0\}\ \exists a^{-1} \in F\ a \times a^{-1} = a^{-1} \times a = 1$	(Inverse Element)
(11) $a \times b = b \times a$	(Commutativity)
(12) $a \times (b + c) = a \times b + a \times c$	(Distributive Law)
(13) $(b + c) \times a = b \times a + c \times a$	(Distributive Law)

The following are examples of fields:

Example 6.3 (**Fields**)

(i) The set of rational numbers $(\mathbb{Q}, +, \times)$ forms an infinite commutative field. The additive identity is 0, and the multiplicative identity is 1.

(ii) The set of real numbers $(\mathbb{R}, +, \times)$ forms an infinite commutative field. The additive identity is 0, and the multiplicative identity is 1.

(iii) The set of complex numbers $(\mathbb{C}, +, \times)$ forms an infinite commutative field. The additive identity is 0, and the multiplicative identity is 1.

(iv) The set of integers mod 7 (i.e. $\mathbb{Z}_7$ where addition and multiplication is performed mod 7) is a finite field.

[2] A finite division ring is actually a field (i.e. it is commutative under multiplication), and this classic result was proved by Wedderburn.

(v) The set of integers mod p where p is a prime (i.e. $\mathbb{Z}_p$ where addition and multiplication is performed mod p) is a finite field with p elements. The additive identity is [0] and the multiplicative identity is [1].

A field is a commutative division ring but not every division ring is a field. For example, the quaternions (discovered by Hamilton) are an example of a division ring, which is not a field. If the number of elements in the field F is finite then F is called a finite field, and F is written as F_q where q is the number of elements in F. In fact, every finite field has $q = p^k$ elements for some prime p, and some $k \in \mathbb{N}$ and $k > 0$.

6.6.4 Vector Spaces

A non-empty set V is said to be a *vector space* over a field F if V is a commutative group under vector addition +, and if for every $\alpha \in F$, $v \in V$ there is an element αv in V such that the following properties hold for $v, w \in V$ and $\alpha, \beta \in F$:

1. $u + v \in V$
2. $u + (v + w) = (u + v) + w$
3. $\exists 0 \in V$ such that $\forall v \in V\ v + 0 = 0 + v = v$
4. $\forall v \in V\ \exists(-v) \in V$ such that $v + (-v) = (-v) + v = 0$
5. $v + w = w + v$
6. $\alpha(v + w) = \alpha v + \alpha w$
7. $(\alpha + \beta)v = \alpha v + \beta v$
8. $\alpha(\beta v) = (\alpha\beta)v$
9. $1v = v$

The elements in V are referred to as *vectors* and the elements in F are referred to as *scalars*. The element 1 refers to the identity element of the field F under multiplication.

Application of Vector Spaces to Coding Theory

The representation of codewords in coding theory (which is discussed in Chap. 11), is by n-dimensional vectors over the finite field F_q. A codeword vector v is represented as the n-tuple

$$v = (a_0, a_1, \ldots .a_{n-1})$$

where each $a_i \in F_q$. The set of all n-dimensional vectors is the n-dimensional vector space $\boldsymbol{F}_q^n$ with q^n elements. The addition of two vectors v and w, where $v = (a_0, a_1, \ldots.\ a_{n-1})$ and $w = (b_0, b_1, \ldots.\ b_{n-1})$ is given by

$$v + w = (a_0 + b_0, a_1 + b_1, \ldots .a_{n-1} + b_{n-1})$$

The scalar multiplication of a vector $v = (a_0, a_1, \ldots .a_{n-1}) \in \boldsymbol{F}_q^n$ by a scalar $\beta \in F_q$ is given by

$$\beta v = (\beta a_0, \beta a_1, \ldots .\beta a_{n-1})$$

The set $\boldsymbol{F}_q^n$ is called the vector space over the finite field F_q, if the vector space properties above hold. A finite set of vectors v_1, v_2, … v_k is said to be *linearly independent* if

$$\beta_1 v_1 + \beta_2 v_2 + \ldots + \beta_k v_k = 0 \Rightarrow \beta_1 = \beta_2 = \ldots \beta_k = 0$$

Otherwise, the set of vectors v_1, v_2, … v_k is said to be *linearly dependent*.

A non-empty subset W of a vector space $V(W \subseteq V)$ is said to be a *subspace* of V, if W forms a vector space over F under the operations of V. This is equivalent to W being closed under vector addition and scalar multiplication: i.e. w_1, $w_2 \in W$, α, $\beta \in F$ then $\alpha w_1 + \beta w_2 \in W$.

The *dimension* (dim W) of a subspace $W \subseteq V$ is k if there are k linearly independent vectors in W but every $k + 1$ vectors are linearly dependent. A subset of a vector space is a *basis* for V if it consists of linearly independent vectors, and its linear span is V (i.e. the basis generates V). We shall employ the basis of the vector space of codewords (see Chap. 11) to create the generator matrix to simplify the encoding of the information words. The linear span of a set of vectors v_1, v_2, …, v_k is defined as $\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k$.

Example 6.4 (**Vector Spaces**)

(i) The Real coordinate space $\mathbb{R}^n$ forms an n-dimensional vector space over $\mathbb{R}$. The elements of $\mathbb{R}^n$ are the set of all n tuples of elements of $\mathbb{R}$, where an element x in $\mathbb{R}^n$ is written as

$$x = (x_1, x_2, \ldots x_n)$$

where each $x_i \in \mathbb{R}$ and vector addition and scalar multiplication are given by

$$\begin{aligned} \alpha x &= (\alpha x_1, \alpha x_2, \ldots \alpha x_n) \\ x + y &= (x_1 + y_1, x_2 + y_2 \ldots x_n + y_n) \end{aligned}$$

(ii) The set of $m \times n$ matrices over the real numbers forms a vector space, with vector addition given by matrix addition, and the multiplication of a matrix by a scalar given by the multiplication of each entry in the matrix by the scalar.

6.7 Review Questions

1. Solve the simple equation: $4(3x + 1) = 7(x + 4) - 2(x + 5)$

2. Solve the following simultaneous equations by

$$x + 2y = -1$$
$$4x - 3y = 18$$

   (a) Graphical techniques
   (b) Method of substitution
   (c) Method of Elimination

3. Solve the quadratic equation $3x^2 + 5x - 2 = 0$ given that the solution is between $x = -3$ and $x = 3$ by:

   (a) Graphical techniques
   (b) Factorization
   (c) Quadratic Formula

4. Solve the following indicial equation using logarithms

$$2^{x=1} = 3^{2x-1}$$

5. Explain the differences between semigroups, monoids and groups.
6. Show that the following properties are true for groups.

   (i) The identity element is unique in a group.
   (ii) The inverse of an element is unique in a group.

7. Explain the differences between rings, commutative rings, integral domains, division rings and fields.
8. What is a vector space?
9. Explain how vector spaces may be applied to coding theory (see Chap. 11 for more details).

6.8 Summary

This chapter provided a brief introduction to algebra, which is the branch of mathematics that studies mathematical symbols and the rules for manipulating them. Algebra is a powerful tool for problem solving in science and engineering.

Elementary algebra includes the study of simultaneous equations (i.e. two or more equations with two or more unknowns); the solution of quadratic equations $ax^2 + bx + c = 0$; and the study of polynomials, indices and logarithms. Linear algebra is concerned with the solution of a set of linear equations, and the study of matrices and vector spaces.

Abstract algebra is concerned with the study of abstract algebraic structures such as monoids, groups, rings, integral domains, fields and vector spaces. The abstract approach in modern mathematics has opened up whole new areas of mathematics as well as applications in areas such as coding theory in the computing field.

Reference

1. Mathematics in Computing. Second Edition, Gerard O' Regan. Springer. 2012.