and continuing to evaluate the other 7 cofactors we get

$$\operatorname{adj} \boldsymbol{A}_1 = \begin{bmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{bmatrix} = \begin{bmatrix} \alpha^2 & 0 & 1 \\ \alpha^8 & \alpha & \alpha^3 \\ \alpha^2 & \alpha^4 & \alpha^{12} \end{bmatrix}.$$

The inverse of $\boldsymbol{A}_1$, is therefore

$$\begin{aligned} \boldsymbol{A}_1^{-1} &= \operatorname{adj} \boldsymbol{A}_1/\det \boldsymbol{A}_1 \\ &= (1/\alpha^3)\begin{bmatrix} \alpha^2 & 0 & 1 \\ \alpha^8 & \alpha & \alpha^3 \\ \alpha^2 & \alpha^4 & \alpha^{12} \end{bmatrix} \\ &= \begin{bmatrix} \alpha^2/\alpha^3 & 0 & 1/\alpha^3 \\ \alpha^8/\alpha^3 & \alpha/\alpha^3 & \alpha^3/\alpha^3 \\ \alpha^2/\alpha^3 & \alpha^4/\alpha^3 & \alpha^{12}/\alpha^3 \end{bmatrix}. \end{aligned}$$

which gives

$$\boldsymbol{A}_1^{-1} = \begin{bmatrix} \alpha^{14} & 0 & \alpha^{12} \\ \alpha^5 & \alpha^{13} & 1 \\ \alpha^{14} & \alpha & \alpha^9 \end{bmatrix}.$$

The reader can check that $\boldsymbol{A}_1\boldsymbol{A}_1^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \boldsymbol{I}.$

Example 6.13
Determine the inverse of the matrix

$$\boldsymbol{A} = \begin{bmatrix} \alpha^3 & \alpha^5 \\ 1 & \alpha \end{bmatrix}$$

in $GF(2^3)$ and $GF(2^4)$.

In $GF(2^3)$ the determinant of $\boldsymbol{A}$ is

$$\det \boldsymbol{A} = \begin{vmatrix} \alpha^3 & \alpha^5 \\ 1 & \alpha \end{vmatrix} = \alpha^3\alpha + \alpha^5 1 = \alpha^4 + \alpha^5 = 1.$$

As $\det \boldsymbol{A} \neq 0$ the inverse therefore exists. The cofactors of $\boldsymbol{A}$ are $A_{11}=\alpha$, $A_{12}=1$, $A_{21}=\alpha^5$ and $A_{22}=\alpha^3$ and so the adjoint of $\boldsymbol{A}$ is

$$\operatorname{adj} \boldsymbol{A} = \begin{bmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{bmatrix} = \begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^3 \end{bmatrix}.$$

The inverse of $\boldsymbol{A}$ is therefore

$$\boldsymbol{A}^{-1} = (\operatorname{adj} \boldsymbol{A})/\det \boldsymbol{A} = \begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^3 \end{bmatrix}.$$

We can check that

$$AA^{-1} = \begin{bmatrix} \alpha^3 & \alpha^5 \\ 1 & \alpha \end{bmatrix} \begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^3 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^4 + \alpha^5 & \alpha^8 + \alpha^8 \\ \alpha + \alpha & \alpha^5 + \alpha^4 \end{bmatrix}$$

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

as required.

In $GF(2^4)$ we get

$$\det A = \alpha^8$$

$$\operatorname{adj} A = \begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^3 \end{bmatrix}$$

which gives

$$A^{-1} = \begin{bmatrix} \alpha^8 & \alpha^{12} \\ \alpha^7 & \alpha^{10} \end{bmatrix}.$$

□

Linear equations can be defined over finite fields and solved using standard methods. For example, take

$$\alpha x + \alpha^5 y = \alpha^3$$
$$x + \alpha^7 y = \alpha^{11}$$

defined over $GF(2^4)$. These can be solved in the normal manner of first multiplying one of the equations by a suitable number and then subtracting the equations, thus eliminating one variable. Here multiplying $x + \alpha^7 y = \alpha^{11}$ by α and then adding it to $\alpha x + \alpha^5 y = \alpha^3$ eliminates the x variable so leaving

$$(\alpha^5 + \alpha^8)y = \alpha^3 + \alpha^{12}$$

which is easily solved to give $y = \alpha^6$. Substituting this into either of the simultaneous equations gives $x = \alpha^4$.

Matrix inversion techniques can also be used to solve linear equations in finite fields, adopting this approach the above linear equations can be written as

$$\begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha^3 \\ \alpha^{11} \end{bmatrix}$$

with the solution given by

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^7 \end{bmatrix}^{-1} \begin{bmatrix} \alpha^3 \\ \alpha^{11} \end{bmatrix}.$$

Here we get

$$\operatorname{adj} \begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^7 \end{bmatrix} = \begin{bmatrix} \alpha^7 & \alpha^5 \\ 1 & \alpha \end{bmatrix}$$

and

$$\begin{vmatrix} \alpha & \alpha^5 \\ 1 & \alpha^7 \end{vmatrix} = \alpha\alpha^7 + 1\alpha^5 = \alpha^4$$

so that the required inverse matrix is

$$\begin{aligned} \begin{bmatrix} \alpha & \alpha^5 \\ 1 & \alpha^7 \end{bmatrix}^{-1} &= \frac{1}{\alpha^4}\begin{bmatrix} \alpha^7 & \alpha^5 \\ 1 & \alpha \end{bmatrix} \\ &= \begin{bmatrix} \alpha^7/\alpha^4 & \alpha^5/\alpha^4 \\ 1/\alpha^4 & \alpha/\alpha^4 \end{bmatrix} \\ &= \begin{bmatrix} \alpha^3 & \alpha \\ \alpha^{11} & \alpha^{12} \end{bmatrix}. \end{aligned}$$

Therefore the solution is

$$\begin{aligned} \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} \alpha^3 & \alpha \\ \alpha^{11} & \alpha^{12} \end{bmatrix}\begin{bmatrix} \alpha^3 \\ \alpha^{11} \end{bmatrix} \\ &= \begin{bmatrix} \alpha^3\alpha^3 + \alpha\alpha^{11} \\ \alpha^{11}\alpha^3 + \alpha^{12}\alpha^{11} \end{bmatrix} \\ &= \begin{bmatrix} \alpha^4 \\ \alpha^6 \end{bmatrix} \end{aligned}$$

which gives $x = \alpha^4$, $y = \alpha^6$ as obtained previously. The next example considers a set of three linear equations.

Example 6.14
Using matrix inversion, determine the solution of the following set of linear equations over $GF(2^4)$:

$$\begin{aligned} \alpha^3 x_1 + \alpha x_2 + x_3 &= \alpha^5 \\ \alpha^2 x_1 + \alpha^6 x_2 + x_3 &= \alpha^6 \\ \alpha^{14} x_1 + \alpha^7 x_2 + \alpha^7 x_3 &= 1. \end{aligned}$$

Representing the equations in matrix form gives

$$\boldsymbol{A}\boldsymbol{x} = \boldsymbol{c}$$

where

$$\boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \quad \text{and} \quad \boldsymbol{c} = \begin{bmatrix} \alpha^5 \\ \alpha^6 \\ 1 \end{bmatrix}.$$

are column vectors, and A is the matrix

$$A = \begin{bmatrix} \alpha^3 & \alpha & 1 \\ \alpha^2 & \alpha^6 & 1 \\ \alpha^{14} & \alpha^7 & \alpha^7 \end{bmatrix}.$$

The determinant of $\boldsymbol{A}$ is

$$\begin{aligned}\det \boldsymbol{A} &= \alpha^3\begin{vmatrix}\alpha^6 & 1\\ \alpha^7 & \alpha^7\end{vmatrix} + \alpha\begin{vmatrix}\alpha^2 & 1\\ \alpha^{14} & \alpha^7\end{vmatrix} + 1\begin{vmatrix}\alpha^2 & \alpha^6\\ \alpha^{14} & \alpha^7\end{vmatrix}\\ &= \alpha^3(\alpha^{13}+\alpha^7)+\alpha(\alpha^9+\alpha^{14})+1(\alpha^9+\alpha^5)\\ &= \alpha^8+\alpha^5+\alpha^6=\alpha^{12}.\end{aligned}$$

The adjoint of $\boldsymbol{A}$ is

$$\operatorname{adj} \boldsymbol{A} = \begin{bmatrix}\alpha^5 & \alpha^{11} & \alpha^{11}\\ \alpha^4 & \alpha^{11} & \alpha^6\\ \alpha^6 & \alpha^5 & \alpha\end{bmatrix}$$

and using $\boldsymbol{A}^{-1} = \operatorname{adj} \boldsymbol{A}/\det \boldsymbol{A}$ gives

$$\boldsymbol{A}^{-1} = \begin{bmatrix}\alpha^8 & \alpha^{14} & \alpha^{14}\\ \alpha^7 & \alpha^{14} & \alpha^9\\ \alpha^9 & \alpha^8 & \alpha^4\end{bmatrix}.$$

Multiplying $\boldsymbol{Ax}=\boldsymbol{c}$ by $\boldsymbol{A}^{-1}$ gives $\boldsymbol{x}=\boldsymbol{A}^{-1}\boldsymbol{c}$ and therefore

$$\begin{aligned}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix} &= \begin{bmatrix}\alpha^8 & \alpha^{14} & \alpha^{14}\\ \alpha^7 & \alpha^{14} & \alpha^9\\ \alpha^9 & \alpha^8 & \alpha^4\end{bmatrix}\begin{bmatrix}\alpha^5\\ \alpha^6\\ 1\end{bmatrix}\\ &= \begin{bmatrix}\alpha^{13}+\alpha^5+\alpha^{14}\\ \alpha^{12}+\alpha^5+\alpha^9\\ \alpha^{14}+\alpha^{14}+\alpha^4\end{bmatrix}\\ &= \begin{bmatrix}\alpha\\ \alpha^4\\ \alpha^4\end{bmatrix}\end{aligned}$$

which gives $x_1=\alpha$, $x_2=\alpha^4$, and $x_3=\alpha^4$. □

Problems

6.1 Given that α is a field element of $GF(2^3)$ evaluate
(a) $(\alpha^2\alpha^{-5}+1)\ (\alpha^4+\alpha)$
(b) $\surd(\alpha^4\alpha^5+\surd\alpha)$.
Repeat when α is an element of $GF(2^4)$.

6.2 Determine whether the polynomials

$$\begin{aligned}p_1(x) &= x^4+x^3+x+1\\ p_2(x) &= x^2+x+1\\ p_3(x) &= x^3+x^2+1\end{aligned}$$

over $GF(2)$ are (a) irreducible and (b) primitive.