2.1 *Prove that the numbers of the form $a+\sqrt{2}b$, where a and b are rational numbers, form a subfield of $\mathbb{C}$.*
Let our alleged subfield be denoted $\mathbb{Q}[\sqrt{2}]$

(a) *If a and b are in $\mathbb{Q}[\sqrt{2}]$, then $a+b$ is in $\mathbb{Q}[\sqrt{2}]$.*
Suppose $a+\sqrt{2}b, c+\sqrt{2}d \in \mathbb{Q}[\sqrt{2}]$. Therefore

$$a+\sqrt{2}b+c+\sqrt{2}d = (a+c)+\sqrt{2}(b+d) \in \mathbb{Q}[\sqrt{2}].$$

(b) *If a is in $\mathbb{Q}[\sqrt{2}]$, then $-a$ is in $\mathbb{Q}[\sqrt{2}]$*
Suppose $a+\sqrt{2}b \in \mathbb{Q}[\sqrt{2}]$. Since $a, b \in \mathbb{Q}$ then $-a, -b \in \mathbb{Q}$. Therefore $-a-\sqrt{2}b = -(a+\sqrt{2}b) \in \mathbb{Q}[\sqrt{2}]$.

(c) *If a and b are in $\mathbb{Q}[\sqrt{2}]$, then ab is in $\mathbb{Q}[\sqrt{2}]$.*
Suppose $a+\sqrt{2}b, c+\sqrt{2}d \in \mathbb{Q}[\sqrt{2}]$. Therefore

$$\begin{aligned}(a+\sqrt{2}b)(c+\sqrt{2}d) &= ac+\sqrt{2}ad+\sqrt{2}bc+2bd \\ &= (ac+2bd)+\sqrt{2}(ad+bc) \in \mathbb{Q}[\sqrt{2}].\end{aligned}$$

(d) *If a is in $\mathbb{Q}[\sqrt{2}]$ and $a \neq 0$, then a^{-1} is in $\mathbb{Q}[\sqrt{2}]$.*
Suppose $a+\sqrt{2}b \in \mathbb{Q}[\sqrt{2}], a+\sqrt{2}b \neq 0$. Note that since $a+\sqrt{2}b \neq 0$ then $a-\sqrt{2}b \neq 0$, because if $a-\sqrt{2}b = 0$ then $a+\sqrt{2}b = 2\sqrt{2}b$, contradicting a being an arbitrary rational number. Since $a+\sqrt{2}b, a-\sqrt{2}b$ are non-zero then their product, a^2+2b^2, is non-zero. Therefore,

$$(a+\sqrt{2}b)\frac{a-\sqrt{2}b}{a^2+2b^2} = \frac{a^2+2b^2}{a^2+2b^2} = 1,$$

thus $\frac{a-\sqrt{2}b}{a^2+2b^2}$ is an inverse for $a+\sqrt{2}b$.

(e) *1 is in $\mathbb{Q}[\sqrt{2}]$.*
Since $1, 0 \in \mathbb{Q}$, then $1 = 1+\sqrt{2}*0 \in \mathbb{Q}[\sqrt{2}]$. Therefore $1 \in \mathbb{Q}[\sqrt{2}]$.

2.3 *Compute the product of the polynomial $(x^3+3x^2+3x+1)(x^4+4x^3+6x^2+4x+1)$ when the coefficents are elements in $\mathbb{F}_7$. Explain your answer.*

$$\begin{aligned}(x^3+3x^2+3x+1)(x^4+4x^3+6x^2+4x+1) &= x^3(x^4+4x^3+6x^2+4x+1)\\ &+ 3x^2(x^4+4x^3+6x^2+4x+1)\\ &+ 3x(x^4+4x^3+6x^2+4x+1)\\ &+ (x^4+4x^3+6x^2+4x+1)\\ &= (x^7+4x^6+6x^5+4x^4+x^3)\\ &+ (3x^6+12x^5+18x^4+12x^3+3x^2)\\ &+ (3x^5+12x^4+18x^3+12x^2+3x)\\ &+ (x^4+4x^3+6x^2+4x+1)\\ &= x^7+(3+4)x^6\\ &+ (6+12+3)x^5+(4+18+12+1)x^4\\ &+ (1+12+18+4)x^3+(3+12+6)x^2+(3+4)x+1\\ &= x^7+(7*1+0)+(7*3+0)x^5+(7*5+0)x^4\\ &+ (7*5+0)x^3+(7*3+0)x^2+(7*1+0)x+1\\ &= x^7+1\end{aligned}$$

Explanation: If you look at the right hand side, the first two equal signs is just multiplying out the polynomial then regrouping the terms. After the third equals sign I employ the fact that $\mathbb{F}_7$ has characteristic 7 and further reduce the coefficients of the polynomial.

2.4 *Consider the system of linear equations* $\begin{bmatrix}6 & -3\\ 2 & 6\end{bmatrix}\begin{bmatrix}x_1\\ x_2\end{bmatrix} = \begin{bmatrix}3\\ 1\end{bmatrix}$

Note: the inverse of $\begin{bmatrix}6 & -3\\ 2 & 6\end{bmatrix}$ in $\mathbb{R}$ is $\frac{1}{42}\begin{bmatrix}6 & 3\\ -2 & 6\end{bmatrix}$.

$p=5$ Note that 42 reduces to 2 mod 5, therefore having inverse is 3. Thus our inverted matrix is

$$3\begin{bmatrix}6 & 3\\ -2 & 6\end{bmatrix} = \begin{bmatrix}18 & 9\\ -6 & 18\end{bmatrix} \equiv \begin{bmatrix}3 & 4\\ 4 & 3\end{bmatrix} \mod 5.$$

Therefore the solution to our equation is

$$\begin{bmatrix}3 & 4\\ 4 & 3\end{bmatrix}\begin{bmatrix}3\\ 1\end{bmatrix} = \begin{bmatrix}9+4\\ 12+3\end{bmatrix} \equiv \begin{bmatrix}3\\ 0\end{bmatrix} \mod 5.$$

$p=7$ Since the determinate above is a multiple of 7, the matrix is not invertable. Therefore

$$\begin{bmatrix}6 & -3 & 3\\ 2 & 6 & 1\end{bmatrix} \xrightarrow{R_1\leftrightarrow R_2} \begin{bmatrix}2 & 6 & 1\\ 6 & -3 & 3\end{bmatrix} \xrightarrow[R_1*4]{R_2*4} \begin{bmatrix}1 & 3 & 4\\ 3 & 2 & 5\end{bmatrix}$$
$$\xrightarrow{R_2-3*R_1} \begin{bmatrix}1 & 3 & 4\\ 0 & 0 & 0\end{bmatrix}$$

Since we have a row of 0s, then we can have $x_1 = 4 - 3x_2 = 4 + 4x_2$. Therefore our solution is $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 4+4a \\ a \end{bmatrix} = \begin{bmatrix} 4 \\ 0 \end{bmatrix} + \begin{bmatrix} 4 \\ 1 \end{bmatrix} a, a \in \mathbb{F}_7$

3.2 *Which of the following subsets is a subspace of the vector space $F^{n\times n}$ of $n \times n$ matrices with coefficients in F?*

(a) *Symmetric Matrices*
Symmetric matrices form a subspace as the transpose operation satisfies the following:

i. Suppose A, B are symmetric matrices, therefore

$$(A + B)^T = A^T + B^T = A + B.$$

Thus their sum is symmetric.

ii. Suppose A is a symmetric matrix, $c \in F$, therefore

$$(cA)^T = cA^T.$$

Thus scalar multiples of symmetric matrices are symmetric.

iii. The $n \times n$ matrix of all 0s is trivially symmetric

Therefore the set of symmetric matrices forms a subspace.

(b) *Invertible Matrices*
These do not form a subspace as the 0 matrix has determinate 0, and is thus not invertible.

(c) *Upper Triangular Matrices*
Upper triangular matrices form a subspace as they satisfy the following:

i. Suppose A, B are upper triangular matrices. If we consider $A + B$ element wise, then if $i > j$ then $a_{ij} = b_{ij} = 0$, thus $(A + B)_{ij} = a_{ij} + b_{ij} = 0 + 0 = 0$. Therefore their sum is upper triangular.

ii. Suppose A is upper triangular, $c \in F$. Therefore if $i > j$ then $(cA)_{ij} = ca_{ij} = c * 0 = 0$. Thus cA is upper triangular.

iii. The 0 matrix clearly ensures for all entries a_{ij} where $i > j$ that $a_{ij} = 0$. Thus the 0 matrix is upper triangular.