SOLUTIONS TO ARTIN'S *ALGEBRA*, 2ND ED. CH. 3 – VECTOR SPACES

COLIN COMMANS

Contents

§1 - Fields

1.1

Prove that the numbers of the form $a+b\sqrt{2}$ where a and b are rational numbers form a subfield of $\mathbb{C}$.

Solution.

Proof.
Denote $\mathbb{Q}[\sqrt{2}] := \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$. We check the definition of subfield of $\mathbb{C}$ that Artin gives, i.e. closed under addition, subtraction, multiplication, and division as well as contains 1.

- For any $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, we have
$$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$
since $a+c \in \mathbb{Q}$ and $b+d \in \mathbb{Q}$ by closure of $\mathbb{Q}$.
- For any $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, we have
$$-(a+b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$
since $-a \in \mathbb{Q}$ and $-b \in \mathbb{Q}$ by closure of $\mathbb{Q}$.
- For any $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, we have
$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$
since $ac+2bd \in \mathbb{Q}$ and $ad+bc \in \mathbb{Q}$.
- For any $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, we have
$$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$
since $\frac{a}{a^2-2b^2} \in \mathbb{Q}$ and $\frac{-b}{a^2-2b^2} \in \mathbb{Q}$.
- Finally, we have $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

Therefore $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{C}$. □

1.2

Find the inverse of 5 modulo p, for $p = 7$, 11, 13, and 17.

Solution.
We solve $5x \equiv 1 \mod p$.

(i) $p = 7$: We have table

x	0	1	2	3	4	5	6
$5x \mod 7$	0	5	3	1	6	4	2

Hence $5^{-1} = 3$ in $\mathbb{F}_7$.

(ii) $p = 11$: We have table

x	0	1	2	3	4	5	6	7	8	9	10
$5x \mod 11$	0	5	10	4	9	3	8	2	7	1	6

Hence $5^{-1} = 9$ in $\mathbb{F}_{11}$.

(iii) $p = 13$: We have table

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$5x \mod 13$	0	5	10	2	7	12	4	9	1	6	11	3	8

Hence $5^{-1} = 8$ in $\mathbb{F}_{13}$.

(iv) $p = 17$: We have table

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$5x \mod 17$	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12

Hence $5^{-1} = 7$ in $\mathbb{F}_{17}$.

1.3

Compute the product polynomial $(x^3+3x^2+3x+1)(x^4+4x^3+6x^2+4x+1)$ when the coefficients are regarded as elements of the field $\mathbb{F}_7$. Explain your answer.

Solution.
We have by the binomial theorem that

$$(x^3+3x^2+3x+1)(x^4+4x^3+6x^2+4x+1) = (x+1)^3(x+1)^4 = (x+1)^7 = \sum_{i=0}^{7} \binom{7}{i} x^i$$

However, 7 divides $\binom{7}{i} = \frac{7!}{i!(7-i)!}$ for $i = 1, \ldots, 6$, so we have

$$\sum_{i=0}^{7} \binom{7}{i} x^i = x^7 + 1 + \sum_{i=1}^{6} \binom{7}{i} x^i \equiv x^7 + 1 + \sum_{i=1}^{6} 0x^i \equiv x^7 + 1$$

Thus the product is x^7+1. More generally, $(x+1)^p \equiv x^p + 1 \mod p$ for any prime p.

1.4

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

(a) Solve the system in $\mathbb{F}_p$ when $p = 5$, 11, and 17.

(b) Determine the number of solutions when $p = 7$.

Solution.
Denote $A = \begin{bmatrix} 6 & -3 \\ 2 & 6 \end{bmatrix}, X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, B = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$.

(a) We have $A^{-1} = 42^{-1} \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix}$ and so our solution is

$$X = A^{-1}B = 42^{-1} \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = 42^{-1} \begin{bmatrix} 21 \\ 0 \end{bmatrix}$$

Now we work modulo p for:

- $p = 5$: $42^{-1} \equiv 2^{-1} = 3$, so
$$X = 42^{-1} \begin{bmatrix} 21 \\ 0 \end{bmatrix} \equiv 3 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 0 \end{bmatrix}$$
- $p = 11$: $42^{-1} \equiv 9^{-1} = 5$, so
$$X = 42^{-1} \begin{bmatrix} 21 \\ 0 \end{bmatrix} \equiv 5 \begin{bmatrix} 10 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 6 \\ 0 \end{bmatrix}$$
- $p = 17$: $42^{-1} \equiv 8^{-1} = 15$, so
$$X = 42^{-1} \begin{bmatrix} 21 \\ 0 \end{bmatrix} \equiv 15 \begin{bmatrix} 4 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 0 \end{bmatrix}$$

(b) Note that $\det A = 42 \equiv 0 \mod 7$, so A is not invertible. However, we can write our system modulo 7:

$$AX \equiv \begin{bmatrix} -1 & -3 \\ 2 & 6 \end{bmatrix} X \equiv \begin{bmatrix} -(x_1 + 3x_2) \\ 2(x_1 + 3x_2) \end{bmatrix} \equiv \begin{bmatrix} 3 \\ -6 \end{bmatrix} \equiv B$$

So we have a solution iff $x_1 + 3x_2 \equiv -3 \equiv 4$. We can compute the table where each entry is $x_1 + 3x_2 \mod 7$ to find our solutions:

$x_1 \backslash x_2$	0	1	2	3	4	5	6
0	0	3	6	2	5	1	4
1	1	4	0	3	6	2	5
2	2	5	1	4	0	3	6
3	3	6	2	5	1	4	0
4	4	0	3	6	2	5	1
5	5	1	4	0	3	6	2
6	6	2	5	1	4	0	3

so we have solution set with 7 elements

$$\left\{ \begin{bmatrix} 0 \\ 6 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 5 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix}, \begin{bmatrix} 5 \\ 2 \end{bmatrix}, \begin{bmatrix} 6 \\ 4 \end{bmatrix} \right\}$$

1.5

Determine the 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 $\mathbb{F}_p$.

Solution.
We have A is invertible in $\mathbb{F}_p$ if and only if $\det A$ is not divisible mod p. Since $\det A = 10$, in this case A^{-1} exists if and only if $p \neq 2$ and $p \neq 5$.

1.6

Solve completely the system of linear equations $AX = 0$ and $AX = B$, where

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}, \quad \text{and} \quad B = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$$

(a) in $\mathbb{Q}$, (b) in $\mathbb{F}_2$, (c) in $\mathbb{F}_3$, (d) in $\mathbb{F}_7$.

Solution.
Note that $\det A = 3$. So if 3 is invertible in our field, then A is invertible and $X = 0$ is the only solution to $AX = 0$ and $X = A^{-1}B$ is the solution to $AX = B$. We can calculate

$$A^{-1}B = 3^{-1} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = 3^{-1} \begin{bmatrix} 1 \\ 2 \\ -4 \end{bmatrix}$$

Now we consider each field:

(a) In $\mathbb{Q}$, we have $3^{-1} = \frac{1}{3}$ and so $AX = 0$ has the unique solution $X = 0$ and $AX = B$ has the unique solution $X = \begin{bmatrix} \frac{1}{3} & \frac{2}{3} & -\frac{4}{3} \end{bmatrix}^t$.

(b) In $\mathbb{F}_2$, we have $3^{-1} \equiv 1^{-1} = 1$ and so $AX = 0$ has the unique solution $X = 0$ and $AX = B$ has the unique solution $X = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^t$.

(c) In $\mathbb{F}_3$, $3 \equiv 0$ is not invertible so we need to manually inspect our systems. Note that

$$AX = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 2 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ x_1 + x_3 \\ x_1 + 2x_2 + 2x_3 \end{bmatrix}$$

Hence the system $AX = 0$ is really the equations

$$\begin{cases} x_1 + x_2 \equiv 0 \\ x_1 + x_3 \equiv 0 \\ x_1 + 2x_2 + 2x_3 \equiv 0 \end{cases}$$

We consider cases:

- If $x_1 = 0$, equation 1 forces $x_2 = 0$ and equation 2 forces $x_3 = 0$. This satisfies equation 3, so we have a solution.
- If $x_1 = 1$, equation 1 forces $x_2 = 2$ and equation 2 forces $x_3 = 2$. This satisfies equation 3, so we have a solution.
- If $x_1 = 2$, equation 1 forces $x_2 = 1$ and equation 2 forces $x_3 = 1$. This satisfies equation 3, so we have a solution.

This exhausts all possible values of $x_1 \in \mathbb{F}_3$, so the system $AX = 0$ has three solutions $X = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}^t, \begin{bmatrix} 1 & 2 & 2 \end{bmatrix}^t, \begin{bmatrix} 2 & 1 & 1 \end{bmatrix}^t$.
Next, the system $AX = B$ is the equations

$$\begin{cases} x_1 + x_2 \equiv 1 \\ x_1 + x_3 \equiv 2 \\ x_1 + 2x_2 + 2x_3 \equiv 1 \end{cases}$$

We consider cases:

- If $x_1 = 0$, equation 1 forces $x_2 = 1$ and equation 2 forces $x_3 = 2$. This does not satisfy equation 3, so no solutions have $x_1 = 0$.
- If $x_1 = 1$, equation 1 forces $x_2 = 0$ and equation 2 forces $x_3 = 1$. This does not satisfy equation 3, so no solutions have $x_1 = 1$.
- If $x_1 = 2$, equation 1 forces $x_2 = 2$ and equation 2 forces $x_3 = 0$. This does not satisfy equation 3, so no solutions have $x_1 = 2$.

This exhausts all cases of x_1, so $AX = B$ has no solutions.

(d) In $\mathbb{F}_7$, we have $3^{-1} = 5$ and so $AX = 0$ has the unique solution $X = 0$ and $AX = B$ has the unique solution $X = \begin{bmatrix} 5 & 3 & 1 \end{bmatrix}^t$

1.7

By finding primitive elements, verify that the multiplicative group $\mathbb{F}_p^\times$ is cyclic for all primes $p < 20$.

Solution.
We need to check the cases $p = 2, 3, 5, 7, 11, 13, 17, 19$, i.e. find an element of order $p-1$ in $\mathbb{F}_p^\times$.

- $p = 2$: Then $\mathbb{F}_2^\times = \{1\} = \langle 1 \rangle$ is clearly cyclic.
- $p = 3$: We have $\mathbb{F}_3^\times = \{1, 2\} = \langle 2 \rangle$ is cyclic.
- $p = 5$: Note that

$$\begin{aligned} 3 = 3^0 \times 3 \equiv 1 \times 3 \equiv 3 \mod 5 \\ 3^2 = 3^1 \times 3 \equiv 3 \times 3 \equiv 4 \mod 5 \\ 3^3 = 3^2 \times 3 \equiv 4 \times 3 \equiv 2 \mod 5 \\ 3^4 = 3^3 \times 3 \equiv 2 \times 3 \equiv 1 \mod 5 \end{aligned}$$

  Hence 3 has order 4 and so $\mathbb{F}_5^\times = \langle 3 \rangle$.

- $p = 7$: We have

$$\begin{aligned} 3 = 3^0 \times 3 \equiv 1 \times 3 \equiv 3 \mod 7 \\ 3^2 = 3^1 \times 3 \equiv 3 \times 3 \equiv 2 \mod 7 \\ 3^3 = 3^2 \times 3 \equiv 2 \times 3 \equiv 6 \mod 7 \\ 3^4 = 3^3 \times 3 \equiv 6 \times 3 \equiv 4 \mod 7 \\ 3^5 = 3^4 \times 3 \equiv 4 \times 3 \equiv 5 \mod 7 \\ 3^6 = 3^5 \times 3 \equiv 5 \times 3 \equiv 1 \mod 7 \end{aligned}$$

  Hence 3 has order 6 and so $\mathbb{F}_7^\times = \langle 3 \rangle$.

- $p = 11$: We have

$$\begin{aligned} 2 = 2^0 \times 2 \equiv 1 \times 2 \equiv 2 \mod 11 \\ 2^2 = 2^1 \times 2 \equiv 2 \times 2 \equiv 4 \mod 11 \\ 2^3 = 2^2 \times 2 \equiv 4 \times 2 \equiv 8 \mod 11 \\ 2^5 = 2^3 \times 2^2 \equiv 8 \times 4 \equiv 10 \mod 11 \\ 2^8 = 2^5 \times 2^3 \equiv 10 \times 8 \equiv 3 \mod 11 \\ 2^{10} = 2^8 \times 2^2 \equiv 3 \times 4 \equiv 1 \mod 11 \end{aligned}$$

  Note that by Lagrange, 2 can only have orders of 1, 2, 5, and 10, so the above shows 2 has order 10 and $\mathbb{F}_{11}^\times = \langle 2 \rangle$.

- $p = 13$: We have

$$\begin{aligned} 2 = 2^0 \times 2 \equiv 1 \times 2 \equiv 2 \mod 13 \\ 2^2 = 2^1 \times 2 \equiv 2 \times 2 \equiv 4 \mod 13 \\ 2^3 = 2^2 \times 2 \equiv 4 \times 2 \equiv 8 \mod 13 \\ 2^4 = 2^3 \times 2 \equiv 8 \times 2 \equiv 3 \mod 13 \\ 2^6 = 2^4 \times 2^2 \equiv 3 \times 4 \equiv 12 \mod 13 \\ 2^{12} = 2^3 \times 2^3 \times 2^3 \equiv 3 \times 3 \times 3 \equiv 1 \mod 13 \end{aligned}$$

  Hence 2 does not have order 1, 2, 3, 4, or 6, so by Lagrange 2 must have order 12 and $\mathbb{F}_{13}^{\times} = \langle 2 \rangle$.

- $p = 17$: We have

$$\begin{aligned} 3 = 3^0 \times 3 \equiv 1 \times 3 \equiv 3 \mod 17 \\ 3^2 = 3^1 \times 3 \equiv 3 \times 3 \equiv 9 \mod 17 \\ 3^3 = 3^2 \times 3 \equiv 9 \times 3 \equiv 10 \mod 17 \\ 3^4 = 3^3 \times 3 \equiv 10 \times 3 \equiv 13 \mod 17 \\ 3^5 = 3^4 \times 3 \equiv 13 \times 3 \equiv 5 \mod 17 \\ 3^8 = 3^5 \times 3^3 \equiv 5 \times 10 \equiv 16 \mod 17 \\ 3^{10} = 3^5 \times 3^5 \equiv 5 \times 5 \equiv 8 \mod 17 \\ 3^{11} = 3^{10} \times 3 \equiv 8 \times 3 \equiv 7 \mod 17 \\ 3^{16} = 3^{11} \times 3^5 \equiv 7 \times 5 \equiv 1 \mod 17 \end{aligned}$$

  Hence 3 does not have order 1, 2, 4, or 8, so by Lagrange 3 must have order 16 and $\mathbb{F}_{17}^{\times} = \langle 3 \rangle$.

- $p = 19$: We have

$$\begin{aligned} 2 = 2^0 \times 2 \equiv 1 \times 2 \equiv 2 \mod 19 \\ 2^2 = 2^1 \times 2 \equiv 2 \times 2 \equiv 4 \mod 19 \\ 2^3 = 2^2 \times 2 \equiv 4 \times 2 \equiv 8 \mod 19 \\ 2^5 = 2^3 \times 2^2 \equiv 8 \times 4 \equiv 13 \mod 19 \\ 2^6 = 2^5 \times 2 \equiv 13 \times 2 \equiv 7 \mod 19 \\ 2^8 = 2^6 \times 2^2 \equiv 7 \times 4 \equiv 9 \mod 19 \\ 2^9 = 2^8 \times 2 \equiv 9 \times 2 \equiv 18 \mod 19 \\ 2^{12} = 2^6 \times 2^6 \equiv 7 \times 7 \equiv 11 \mod 19 \\ 2^{13} = 2^{12} \times 2 \equiv 11 \times 2 \equiv 3 \mod 19 \\ 2^{18} = 2^{13} \times 2^5 \equiv 3 \times 13 \equiv 1 \mod 19 \end{aligned}$$

  Hence 2 does not have order 1, 2, 3, 6, or 9, so by Lagrange 2 must have order 18 and $\mathbb{F}_{19}^{\times} = \langle 2 \rangle$.

1.8

Let p be a prime integer.

(a) Prove *Fermat's Theorem*: For every integer a, $a^p \equiv a \mod p$.

(b) Prove *Wilson's Theorem*: $(p-1)! \equiv -1$ (modulo p).

Solution.

(a) *Proof.*
If $p \mid a$, then we also have $p \mid a^p$ and so $a^p \equiv a \equiv 0 \mod p$. Hence we may assume that $p \nmid a$, i.e. $\gcd(p, a) = 1$. Now note that p does not divide any element of $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$. Hence for every $b \in \mathbb{F}_p^\times$,

$$p \nmid a,\ p \nmid b \implies p \nmid ab$$

and so p does not divide any element of $a\,\mathbb{F}_p^\times = \{a, a2, \ldots, a(p-1)\}$. Then for any $ab \in a\,\mathbb{F}_p^\times$, its remainder modulo p is an element of $\mathbb{F}_p^\times$, and in fact $a\,\mathbb{F}_p^\times$ modulo p simply permutes the elements of $\mathbb{F}_p^\times$. To see this, note that

$$ab_1 \equiv ab_2 \implies a(b_1 - b_2) \equiv 0 \implies p \mid (b_1 - b_2)$$

But $b_1, b_2 \in \{1, \ldots, p-1\}$ means that $|b_1 - b_2| < p$, so the only multiple of p that $b_1 - b_2$ can be is zero and so $b_1 - b_2 = 0$ gives $b_1 = b_2$. Hence the map

$$f_a : \mathbb{F}_p^\times \to \mathbb{F}_p^\times \qquad b \mapsto ab \mod p$$

is injective, and as a map between the same finite set, must also be surjective. Now taking the product of all the elements in $a\,\mathbb{F}_p^\times$, we have modulo p that

$$a^{p-1}(p-1)! = \prod_{ab \in a\,\mathbb{F}_p^\times} ab \equiv \prod_{b \in \mathbb{F}_p^\times} b = (p-1)!$$

Therefore

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p \implies a^{p-1} \equiv 1 \mod p \implies a^p \equiv a \mod p$$

□

(b) *Proof.*
If $p = 2$, then we have $(2-1)! = 1 \equiv -1 \mod 2$. Hence we may assume $p > 2$ is odd.
Let $f_1(x) = x^{p-1} - 1$. Note that modulo p, we have for any $a \in \mathbb{F}_p^\times$ that

$$f_1(a) \equiv 0 \iff a^{p-1} \equiv 1 \iff a^p \equiv a$$

and the last is true by (a). Hence f_1 has roots $1, \ldots, p-1$ modulo p.
Next, let $f_2(x) = (x-1)\ldots(x-(p-1))$. This also has roots $1, \ldots, p-1$ modulo p, with leading term x^{p-1} and constant term $(-1)(-2)\ldots(-(p-1)) = (-1)^{p-1}(p-1)! = (p-1)!$ (since p is odd). However, now $g(x) = f_2(x) - f_1(x)$ has degree $p-2$ with $p-1$ roots, which forces g to be constantly zero (all of this modulo p). In particular its constant term $(p-1)! + 1$ is zero modulo p, and therefore

$$(p-1)! + 1 \equiv 0 \mod p \implies (p-1)! \equiv -1 \mod p$$

[NB: The above proof relies on Lagrange's Theorem (not the one about subgroup orders, but one about polynomials with coefficients in $\mathbb{F}_p$). One can more cleanly (i.e. without relying on other results) prove Wilson's theorem using a counting argument via pairing up elements of $\mathbb{F}_p$ with their inverses, but it does not use (a) unlike in the given proof.] □

1.9

Determine the orders of the matrices $\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 & \\ & 1 \end{bmatrix}$ in the group $GL_2(\mathbb{F}_7)$.

Solution.
We have that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 2^n & 0 \\ 0 & 1^n \end{bmatrix}$$

Hence $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has order 7 and $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ has order 3.

1.10

Interpreting matrix entries in the field $\mathbb{F}_2$, prove that the four matrices $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ form a field.
Hint: You can cut the work down by using the fact that various laws are known to hold for addition and multiplication of matrices.

Solution.

Proof.
We first denote our matrices

$$Z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

We have closure of both addition and multiplication via the tables

$+$	Z	I	A	B
Z	Z	I	A	B
I	I	Z	B	A
A	A	B	Z	I
B	B	A	I	Z

$\times$	Z	I	A	B
Z	Z	Z	Z	Z
I	Z	I	A	B
A	Z	A	B	I
B	Z	B	I	A

Furthermore, this also shows we have additive identity Z and multiplicative identity I, along with the existence of inverses. By nature of matrix addition and multiplication we have associativity of both operations and the distributive property holds. Finally, the tables show that both operations are commutative, so we indeed have a field. □

1.11

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. Will the same method work for $\mathbb{F}_5$? For $\mathbb{F}_7$? Explain.

Solution.
More generally, we discuss for what primes p does $\mathbb{C}_p := \{a + bi \mid a, b \in \mathbb{F}_p\}$ form a field. Addition is always fine (i.e. $\mathbb{C}_p^+$ is always abelian), so multiplication is where we need to focus. Indeed, since we are mimicking $\mathbb{C}$ we have

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Closure then follows from the closure of $\mathbb{F}_p$ as a field, and associativity and commutativity follow by construction. We have identity $1 + 0i$, so all we need is existence of multiplicative inverses. Recall that in $\mathbb{C}$ we have

$$(a + bi)(a - bi) = a^2 + b^2 \implies \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$$

and so in $\mathbb{C}_p$ we have/need $(a + bi)^{-1} = (a - bi)(a^2 + b^2)^{-1}$. Thus for any $a, b \neq 0$ we have

$$(a + bi)^{-1} \in \mathbb{C}_p \text{ exists} \iff (a^2 + b^2)^{-1} \in \mathbb{C}_p \text{ exists} \iff (a^2 + b^2) \neq 0 \in \mathbb{F}_p \iff p \nmid (a^2 + b^2)$$

and so $\mathbb{C}_p$ is a field if and only if $(a^2 + b^2) \equiv 0 \mod p \implies a = b = 0$.

With this characterization, we consider the cases originally given:

- $p = 3$: Consider the table where each entry is $a^2 + b^2$ modulo 3:

a \ b	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

  Hence $\mathbb{C}_3$ is a field.

- $p = 5$: We have table, now with each table modulo 5:

a \ b	0	1	2	3	4
0	0	1	4	4	1
1	1	2	0	0	2
2	4	0	3	3	0
3	4	0	3	3	0
4	1	2	0	0	2

  So $\mathbb{C}_5$ is not a field; from the table we can even state that, e.g., $1 + 2i$ has no inverse.

- $p = 7$: Again, we have the table:

a \ b	0	1	2	3	4	5	6
0	0	1	4	2	2	4	1
1	1	2	5	3	3	5	2
2	4	5	1	6	6	1	5
3	2	3	6	4	4	6	3
4	2	3	6	4	4	6	3
5	4	5	1	6	6	1	5
6	1	2	5	3	3	5	2

  Hence $\mathbb{C}_7$ is a field.

[NB: Rather than computing the entire table and looking for zeros, we really only need to compute the first row and then see if any two can be added to get 0 modulo p. In the case of $p = 7$, the only possible nonzero values are 1, 2, and 4, which cannot add to a multiple of 7 using only two of the numbers and so we have a field; in the case of $p = 5$, we had values of 1 and 4 which can be added together to get 5 and so we do not have a field.]

§2 - Vector Spaces

2.1

(a) Prove that the scalar product of a vector with the zero element of the field F is the zero vector.

(b) Prove that if w is an element of a subspace W, then $-w$ is in W too.

Solution.

(a) *Proof.*
Let $v \in V$ be a vector in a vector space over F and let $\vec{0} \in V$ be the zero vector, i.e. the additive inverse in V^+. Then note that by $0 \in F$ being the additive identity and distributivity in V we have

$$0v = (0+0)v = 0v + 0v$$

Hence by the cancellation law we have $0v = \vec{0}$. □

(b) *Proof.*
Let $W \subset V$ be a subspace and $w \in W$ a vector. By (a), we have $0w = \vec{0}$, and if -1 is the additive inverse of $1 \in F$, then we have

$$(-1)w + w = (-1)w + 1w = (-1+1)w = 0w = \vec{0}$$

which implies $(-1)w = -w$ by uniqueness of inverses. Hence $-w$ is a scalar multiple of w, and therefore $-w \in W$ by closure. □

2.2

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 ($A = A^t$), (b) invertible matrices, (c) upper triangular matrices

Solution.

(a) This is a subspace, since if A, B are two symmetric matrices then the identities

$$(A+B)^t = A^t + B^t = A + B$$

and

$$(cA)^t = c(A^t) = cA$$

show that the subset is closed under addition and scalar multiplication.

(b) This is not a subspace, since for any invertible matrix A, the zero matrix $0A$ has all entries zero, hence determinant zero, hence not invertible and so it is not closed under scalar multiplication.

(c) This is a subspace, as adding two upper triangular matrices keeps the matrix upper triangular, and multiplying every entry of an upper triangular matrix by a scalar also keeps the matrix upper triangular.

§3 - Bases and Dimension

3.1

Find a basis for the space of $n \times n$ symmetric matrices ($A^t = A$).

Solution.
Since symmetric matrices are, as the name suggests, symmetric along the diagonal, one such basis is the set

$$\{e_{ij} + e_{ji} \mid 1 \leq i \leq j \leq n\}$$

Every symmetric matrix can be written uniquely as a linear combination of these matrices, so by Prop 3.4.14 the set forms a basis.

3.2

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.

Solution.
We can row reduce A to A':

$$A = \begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 3 & 0 \\ 2 & 1 & 2 & 3 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 3 & 0 \\ 0 & -1 & -4 & 3 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -1 & 3 \\ 0 & 1 & 4 & -3 \end{bmatrix} = A'$$

so that $AX = 0$ if and only if $A'X = 0$. Hence we have system

$$A'X = 0 \iff \begin{cases} x_1 - x_3 + 3x_4 = 0 \\ x_2 + 4x_3 - 3x_4 = 0 \end{cases} \iff \begin{cases} x_1 = x_3 - 3x_4 \\ x_2 = -4x_3 + 3x_4 \end{cases}$$

$$\iff X = \begin{bmatrix} x_3 - 3x_4 \\ -4x_3 + 3x_4 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1 \\ -4 \\ 1 \\ 0 \end{bmatrix} x_3 + \begin{bmatrix} -3 \\ 3 \\ 0 \\ 1 \end{bmatrix} x_4$$

$$\iff X \in \operatorname{span} \left\{ \begin{bmatrix} 1 \\ -4 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 3 \\ 0 \\ 1 \end{bmatrix} \right\} =: \operatorname{span} \{b_1, b_2\}$$

Furthermore, b_1, b_2 are linearly independent since

$$0 = \alpha_1 b_1 + \alpha_2 b_2 = \begin{bmatrix} \alpha_1 - 3\alpha_2 \\ -4\alpha_1 + 3\alpha_2 \\ \alpha_1 \\ \alpha_2 \end{bmatrix} \implies \alpha_1 = \alpha_2 = 0$$

Hence $\{b_1, b_2\}$ is a basis of W.

3.3

Prove that the three functions $x^2, \cos x$, and e^x are linearly independent.

Solution.

Proof.
Suppose there exists $\alpha, \beta, \gamma \in \mathbb{R}$ such that $f(x) = \alpha x^2 + \beta \cos x + \gamma e^x$ is the zero function. Then we have

$$\begin{cases} 0 = f(0) = \beta + \gamma \\ 0 = f(\pi/2) = \alpha \frac{\pi^2}{4} + \gamma e^{\pi/2} \\ 0 = f(3\pi/2) = \alpha \frac{9\pi^2}{4} + \gamma e^{3\pi/2} \end{cases}$$

Multiplying the second equation by -9 and adding it to the third equation gives

$$0 = (\alpha \tfrac{9\pi^2}{4} + \gamma e^{3\pi/2}) - 9(\alpha \tfrac{\pi^2}{4} + \gamma e^{\pi/2}) = \gamma(\underbrace{e^{3\pi/2} - 9e^{\pi/2}}_{\neq\, 0}) \implies \gamma = 0$$

Hence substituting back into the first equation gives $\beta = 0$ and back into the second equation gives $\alpha = 0$. Therefore our original functions are linearly independent. □

3.4

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 space as the rows of A'.

Solution.

Proof.
By induction it suffices to show the case where $A' = EA$ is a single elementary row operation. We consider cases:

- If E swaps two rows, then clearly both matrices have the same row space.
- If E replaces row R_i with $R_i + \alpha R_j$, then we can rewrite any linear element in the row span of A as

$$\begin{aligned} &\beta_1 R_1 + \cdots + \beta_i R_i + \cdots + \beta_j R_j + \cdots + \beta_m R_m \\ &= \beta_1 R_1 + \cdots + \beta_i (R_i + \alpha R_j) + \cdots + (\beta_j - \alpha\beta_i) R_j + \cdots + \beta_m R_m \end{aligned}$$

  which is in the row span of A', and clearly vice versa, thus the two row spans are the same.
- If E scales row R_i by a nonzero α, then we can rewrite any element in the row span of A as

$$\beta_1 R_1 + \cdots + \beta_i R_i + \cdots + \beta_m R_m = \beta_1 R_1 + \cdots + \frac{\beta_i}{\alpha}(\alpha R_i) + \cdots + \beta_m R_m$$

  which is in the row span of A', and clearly vice versa, thus the two row spans are the same.

This is all possible cases of E, therefore the row space is unchanged under elementary row operations. □

3.5

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 $AX = 0$.

Solution.

Proof.
Let W be a subspace of F^n. Since F^n is finite-dimensional, we have W finite-dimensional (say $\dim W = m$) and so there exists a basis $w_1, \ldots, w_m$ of W. If $m = n$, then by Prop 3.4.23 we have $W = V$ and we can take A to be the zero matrix. Otherwise we may assume $m < n$ and since the vectors $w_1, \ldots, w_m$ are linearly independent in F^n, by Prop 3.4.16 we can add vectors $v_{m+1}, \ldots, v_n$ to our original basis to create a basis of F^n, and by Prop 3.4.14 we can correspond each $X \in F^n$ to its unique coefficients $\alpha_1, \ldots \alpha_n$ such that

$$X = \alpha_1 w_1 + \cdots + \alpha_m w_m + \alpha_{m+1} v_{m+1} + \cdots + \alpha_n v_n = \begin{bmatrix} w_1 & \ldots & w_m & v_{m+1} & \ldots & v_n \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} =: P\Lambda_X$$

Note that P is invertible by Exercise 3.8, so we in fact have a coefficient map $X \mapsto P^{-1}X$. We have again by Prop 3.4.14 that any $X \in W$ has a unique representation as a linear combination of $w_1, \ldots, w_m$, and by the uniqueness of Λ_X, this means that

$$X \in W \iff \alpha_{m+1} = \cdots = \alpha_n = 0$$

Hence if we construct the $(n-m) \times n$ matrix A to be the last $(n-m)$ rows of P^{-1} and B to be the first m rows (i.e. $P^{-1} = \begin{bmatrix} B \\ A \end{bmatrix}$), we have

$$AX = 0 \iff \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \Lambda_X = P^{-1}X = \begin{bmatrix} BX \\ 0 \end{bmatrix} \iff \alpha_{m+1} = \cdots = \alpha_n = 0 \iff X \in W$$

[NB: In the second line we implicitly use the fact that we can always find a basis of a finite-dimensional vector (sub)space, which is not a stated result by Artin at this point, but follows from the procedure in the proof of Prop 3.4.23 of iteratively pulling vectors not in the span of the previous. What we want is actually found in the appendix (Prop A.3.3), but it is the more general version that includes infinite-dimensional vector spaces and hence needs the Axiom of Choice, but in the finite case of F^n, no choice is needed in proving existence of a basis.] $\square$

3.6

Find a basis of the space of solutions in $\mathbb{R}^n$ of the equation

$$x_1 + 2x_2 + 3x_3 + \cdots + nx_n = 0$$

Solution.
Let $S \subset \mathbb{R}^n$ be the space of solutions of the above equation. Note that we have a system of one equation in n variables, which gives us $n-1$ degrees of freedom. We can write

$$x_1 = -2x_2 - 3x_3 - \cdots - nx_n$$

and so we have

$$X \in S \iff X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} -2x_2 - 3x_3 - \cdots - nx_n \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} -2 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} x_2 + \begin{bmatrix} -3 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} x_3 + \cdots + \begin{bmatrix} -n \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} x_n$$

Hence we have

$$S = \operatorname{span} \left\{ \begin{bmatrix} -2 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} -3 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} -n \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right\}$$

These vectors are also linearly independent since

$$0 = \alpha_1 \begin{bmatrix} -2 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_{n-1} \begin{bmatrix} -n \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} -2\alpha_1 - \cdots - n\alpha_{n-1} \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{bmatrix} \implies \alpha_1 = \cdots = \alpha_{n-1} = 0$$

Therefore these vectors are a basis of S.

3.7

Let $(X_1, \ldots, X_m)$ and $(Y_1, \ldots, Y_n)$ be bases for $\mathbb{R}^m$ and $\mathbb{R}^n$, respectively. Do the mn matrices $X_i Y_j^t$ form a basis for the vector space $\mathbb{R}^{m\times n}$ of all $m \times n$ matrices?

Solution.
We claim yes.

Proof.
Let A be an $m \times n$ matrix. Note that if we write row-wise

$$A = \begin{bmatrix} R_1^t \\ \vdots \\ R_m^t \end{bmatrix}$$

then each $R_k \in \mathbb{R}^n$ can be written uniquely as a linear combination of $(Y_1, \ldots, Y_n)$, say

$$R_k = \alpha_1^k Y_1 + \cdots + \alpha_n^k Y_n$$

Hence we have

$$\begin{aligned} A = \begin{bmatrix} \sum_{j=1}^n \alpha_j^1 Y_j^t \\ \sum_{j=1}^n \alpha_j^2 Y_j^t \\ \vdots \\ \sum_{j=1}^n \alpha_j^m Y_j^t \end{bmatrix} &= \begin{bmatrix} \sum_{j=1}^n \alpha_j^1 Y_j^t \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \sum_{j=1}^n \alpha_j^2 Y_j^t \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \sum_{j=1}^n \alpha_j^m Y_j^t \end{bmatrix} \\ &= \left(\sum_{j=1}^n \alpha_j^1 \begin{bmatrix} Y_j^t \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) + \left(\sum_{j=1}^n \alpha_j^2 \begin{bmatrix} 0 \\ Y_j^t \\ \vdots \\ 0 \end{bmatrix} \right) + \cdots + \left(\sum_{j=1}^n \alpha_j^m \begin{bmatrix} 0 \\ 0 \\ \vdots \\ Y_j^t \end{bmatrix} \right) \\ &= \left(\sum_{j=1}^n \alpha_j^1 e_1 Y_j^t \right) + \left(\sum_{j=1}^n \alpha_j^2 e_2 Y_j^t \right) + \cdots + \left(\sum_{j=1}^n \alpha_j^m e_m Y_j^t \right) \\ &= \sum_{k=1}^m \sum_{j=1}^n \alpha_j^k e_k Y_j^t \end{aligned}$$

since $e_k Y_j^t$ is the $m \times n$ matrix whose kth row is Y_j and zeros elsewhere. However, note each e_k is an element of $\mathbb{R}^m$, so it can be written uniquely as a linear combination of $(X_1, \ldots, X_m)$, say

$$e_k = \beta_1^k X_1 + \cdots + \beta_m^k X_m$$

Thus we have

$$A = \sum_{k=1}^m \sum_{j=1}^n \alpha_j^k e_k Y_j^t = \sum_{k=1}^m \sum_{j=1}^n \alpha_j^k \left(\sum_{i=1}^m \beta_i^k X_i \right) Y_j^t = \sum_{k=1}^m \sum_{j=1}^n \sum_{i=1}^m \alpha_j^k \beta_i^k X_i Y_j^t$$

We can rearrange this sum by fixing a value of i and j, in which case we vary k and have terms $\alpha_j^1 \beta_i^1 X_i Y_j^t + \cdots + \alpha_j^m \beta_i^m X_i Y_j^t$. Hence

$$A = \sum_{k=1}^m \sum_{j=1}^n \sum_{i=1}^m \alpha_j^k \beta_i^k X_i Y_j^t = \sum_{i=1}^m \sum_{j=1}^n \left(\sum_{k=1}^m \alpha_j^k \beta_i^k \right) X_i Y_j^t =: \sum_{i=1}^m \sum_{j=1}^n \gamma_{i,j} X_i Y_j^t$$

Therefore A is in the span of the $X_iY_j^t$ matrices.
To show linear independence, suppose that

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\delta_{i,j}X_iY_j^t$$

is equal to the zero matrix. Then for any vector $v \in \mathbb{R}^n$, we have

$$0 = \left(\sum_{i=1}^{m}\sum_{j=1}^{n}\delta_{i,j}X_iY_j^t\right)v = \sum_{i=1}^{m}\sum_{j=1}^{n}\delta_{i,j}X_i(Y_j^tv) = \sum_{i=1}^{m}\left(\sum_{j=1}^{n}\delta_{i,j}(Y_j^tv)\right)X_i$$

Since the basis $(X_1, \ldots, X_m)$ is linearly independent, this forces each $\sum_{j=1}^{n}\delta_{i,j}(Y_j^tv) = 0$. Setting

$$z_i = \sum_{j=1}^{n}\delta_{i,j}Y_j \in \mathbb{R}^n,$$

this means we have $z_i^tv = 0$ for every vector $v \in \mathbb{R}^n$. In particular, $\|z_i\|^2 = z_i^tz_i = 0$ for every i, but only the zero vector in $\mathbb{R}^n$ has length zero, so we have $z_i = 0$ for every i. Hence by linear independence of $(Y_1, \ldots, Y_n)$ we have

$$0 = z_i = \sum_{j=1}^{n}\delta_{i,j}Y_j \implies \delta_{i,1} = \cdots = \delta_{i,n} = 0$$

This is true for every i, so $\delta_{i,j} = 0$ for all i, j, thus the $X_iY_j^t$ matrices are linearly independent and therefore form a basis for $m \times n$ matrices. □

3.8

Prove that a set $(v_1, \ldots, v_n)$ of vectors in F^n is a basis if and only if the matrix obtained by assembling the coordinate vectors of v_i is invertible.

Solution.

Proof.
$\Longrightarrow$: Suppose that $(v_1, \ldots, v_n)$ is a basis of F^n. Write the $n \times n$ matrix

$$M = \begin{bmatrix} v_1 & \ldots & v_n \end{bmatrix}$$

By linear independence, the zero vector can be written as a linear combination of $(v_1, \ldots, v_n)$ in just one way. This implies that $MX = 0$ has only the solution $X = 0$, which by Theorem 1.2.21 implies M is invertible.

$\Longleftarrow$: Suppose that $M = [v_1 \ \ldots \ v_n]$ is invertible.
First note that we can reduce M to the identity $I = [e_1 \ \ldots \ e_n]$. By Exercise 3.4, M has the same span as I, and so $\operatorname{span}\{v_1, \ldots, v_n\} = \operatorname{span}\{e_1, \ldots, e_n\} = F^n$.
Next, for linear independence suppose that $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$. Note that we can rewrite this

$$0 = \alpha_1 v_1 + \cdots + \alpha_n v_n = \begin{bmatrix} v_1 & \ldots & v_n \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ v_n \end{bmatrix} = M\Lambda$$

and since M is invertible, we have $\Lambda = M^{-1}0 = 0$, thus $\alpha_1 = \cdots = \alpha_n = 0$ and the vectors $v_1, \ldots, v_n$ are linearly independent.
Therefore $(v_1, \ldots, v_n)$ is a basis of F^n. $\square$

§4 - Computing with Bases

4.1

(a) Prove that the set $\mathbf{B} = ((1,2,0)^t, (2,1,2)^t, (3,1,1)^t)$ is a basis of $\mathbb{R}^3$.

(b) Find the coordinate vector of the vector $v = (1,2,3)^t$ with respect to this basis.

(c) Let $\mathbf{B}' = ((0,1,0)^t, (1,0,1)^t, (2,1,0)^t)$. Determine the basechange matrix P from $\mathbf{B}$ to $\mathbf{B}'$.

Solution.

(a) *Proof.*
By Exercise 3.8 it suffices to show that B is invertible for

$$B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{bmatrix}$$

and indeed $\det B = 7 \neq 0$, so B^{-1} exists and $\mathbf{B}$ is a basis. □

(b) We want to find $\alpha_1, \alpha_2, \alpha_3$ such that

$$v = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \alpha_1 \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} + \alpha_3 \begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix}$$

Hence we have

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = B^{-1}v = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 2 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \frac{1}{7} \begin{bmatrix} -1 & 4 & -1 \\ -2 & 1 & 5 \\ 4 & -2 & -3 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 4/7 \\ 15/7 \\ -9/7 \end{bmatrix}$$

which is our new coordinate vector.

(c) By definition, we want to find a matrix P such that $\mathbf{B}' = \mathbf{B}P$. Hence we have

$$P = B^{-1}B' = \frac{1}{7} \begin{bmatrix} -1 & 4 & -1 \\ -2 & 1 & 5 \\ 4 & -2 & -3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \frac{1}{7} \begin{bmatrix} 4 & -2 & 2 \\ 1 & 3 & -3 \\ 2 & 1 & 6 \end{bmatrix}$$

4.2

(a) Determine the basechange matrix in $\mathbb{R}^2$, when the old basis is the standard basis $\mathbf{E} = (e_1, e_2)$ and the new basis is $\mathbf{B} = (e_1 + e_2, e_1 - e_2)$.

(b) Determine the basechange matrix in $\mathbb{R}^n$, when the old basis is the standard basis $\mathbf{E}$ and the new basis is $\mathbf{B} = (e_n, e_{n-1}, \ldots, e_1)$.

(c) Let $\mathbf{B}$ be the basis of $\mathbb{R}^2$ in which $v_1 = e_1$ and v_2 is a vector of unit length making an angle of 120° with v_1. Determine the basechange matrix that relates $\mathbf{E}$ to $\mathbf{B}$.

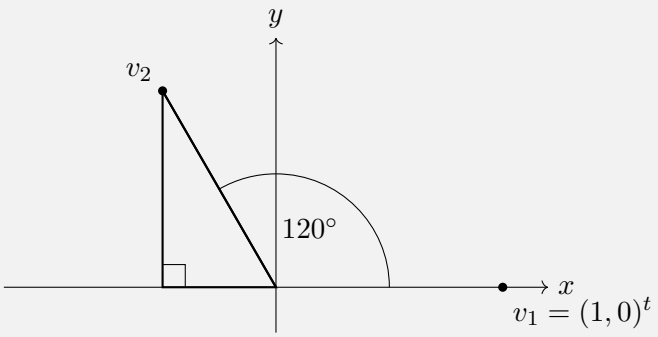
Solution.

(a) Since P satisfies $\mathbf{B} = \mathbf{E}P$ and the matrix representation of $\mathbf{E}$ is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$, we have $P = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

(b) Again, $\mathbf{E} = I$, so P is simply the matrix representation of $\mathbf{B}$:

$$P = \begin{bmatrix} 0 & 0 & \ldots & 1 \\ \vdots & \vdots & \iddots & 0 \\ 0 & 1 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{bmatrix}$$

(c) To find the matrix representation of $\mathbf{B}$, we have the following setup:



Hence using unit circle trigonometry we have $v_2 = (-\cos(\pi/3), \sin(\pi/3))^t = (-1/2, \sqrt{3}/2)^t$ and $P = [v_1\ v_2] = \begin{bmatrix} 1 & -1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix}$.

4.3

Let $\mathbf{B} = (v_1, \ldots, v_n)$ 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.

Solution.

Proof.
Let $B = [v_1 \ \ldots \ v_n]$ be the matrix representation of $\mathbf{B}$, and similarly B' for $\mathbf{B}'$. Then by Exercise 3.8, both B and B' are invertible, so we can perform column operations on both to reduce them to the identity:

$$I = BE_1 \ldots E_m = B'F_1 \ldots F_n \implies B' = B(E_1 \ldots E_m)(F_1 \ldots F_n)^{-1}$$

Note that $(F_1 \ldots F_n)^{-1} = F_n^{-1} \ldots F_1^{-1}$ are all still elementary matrices, so the column operations $B(E_1 \ldots E_m)(F_1 \ldots F_n)^{-1}$ each do one of (i), (ii), or (iii) depending on what elementary operation each matrix represents since each column is a vector in the basis. Hence we can get the vectors in $\mathbf{B}'$ from $\mathbf{B}$ in $m + n$ steps. □

4.4

Let $\mathbb{F}_p$ be a prime field, and let $V = \mathbb{F}_p^2$. Prove:

(a) The number of bases of V is equal to the order of the general linear group $GL_2(\mathbb{F}_p)$.

(b) The order of the general linear group $GL_2(\mathbb{F}_p)$ is $p(p+1)(p-1)^2$, and the order of the special linear group $SL_2(\mathbb{F}_p)$ is $p(p+1)(p-1)$.

Solution.

Proof.

(a) By Exercise 3.8, $\mathbf{B} = (v_1, v_2)$ is a basis if and only if $B = [v_1 \ v_2]$ is invertible. Hence there is a correspondence between a basis of V and an invertible matrix in $GL_2(\mathbb{F}_p)$, which implies the number of bases is the order of $GL_2(\mathbb{F}_p)$.

(b) By (a), it suffices to first find the number of bases of V. First, we need a nonzero vector $v = (v_1, v_2) \in \mathbb{F}_p^2$, which gives $p^2 - 1$ possibilities. Next, we need to choose another vector $w = (w_1, w_2)$ not in the span of v, i.e. $w \neq k \cdot v$ for $k = 0, 1, \ldots, p$, which gives $p^2 - p$ possibilities. Thus the number of bases is $(p^2-1)(p^2-p) = (p-1)(p+1)(p-1)p = p(p+1)(p-1)^2$.

Next, note the determinant map $\det : GL_2(\mathbb{F}_p) \to \mathbb{F}_p^\times$ is a surjective homomorphism (since $\det(AB) = (\det A)(\det B)$) with kernel $SL_2(\mathbb{F}_p)$, so by Corollary 2.8.13

$$|GL_2(\mathbb{F}_p)| = |SL_2(\mathbb{F}_p)| \cdot |\mathbb{F}_p^\times| \implies |SL_2(\mathbb{F}_p)| = \frac{|GL_2(\mathbb{F}_p)|}{|\mathbb{F}_p^\times|} = \frac{p(p+1)(p-1)^2}{p-1} = p(p+1)(p-1)$$

□

4.5

How many subspaces of each dimension are there in (a) $\mathbb{F}_p^3$, (b) $\mathbb{F}_p^4$?

Solution.
We more generally want to investigate the number of k-dimensional subspaces in $\mathbb{F}_p^n$, which we will denote $\#(k,n)$. The idea is to first find the number of linearly independent $(v_1,\dots,v_k)$ and divide that by the number of bases of $\mathbb{F}_p^k$ to account for different vector collections generating the same k-dimensional subspace (which are all isomorphic to $\mathbb{F}_p^k$ by Corollary 3.5.5).

By the same reasoning as Exercise 4.4(b), to generate k linearly independent $(v_1,\dots,v_k)$, we need to start with a nonzero vector $v_1 \in \mathbb{F}_p^n$, which has p^n-1 possibilities. Our next vector needs to not be in the span of v_1, i.e. $v_2 \neq k_1v_1$ for $k_1 \in \mathbb{F}_p$, which gives p^n-p possibilities. Similarly, $v_2 \neq k_1v_1+k_2v_2$ for $k_1,k_2 \in \mathbb{F}_p$, so we have p^n-p^2 possibilities. Thus there are $(p^n-1)(p^n-p)\dots(p^n-p^{k-1})$ many collections of k linearly independent vectors. Next, there are $(p^k-1)(p^k-p)\dots(p^k-p^{k-1})$ many bases of $\mathbb{F}_p^k$ by this same counting argument. Therefore the number of k-dimensional subspaces in $\mathbb{F}_p^n$ is

$$\#(k,n)=\frac{(p^n-1)(p^n-p)\dots(p^n-p^{k-1})}{(p^k-1)(p^k-p)\dots(p^k-p^{k-1})}$$

for $0<k<n$ and we set $\#(0,n)=\#(n,n)=1$.
We now consider our original cases:

(a) $n=3$: We have

- $k=0$: $\#(0,3)=1$
- $k=1$: $\#(1,3)=\dfrac{p^3-1}{p-1}=p^2+p+1$
- $k=2$: $\#(2,3)=\dfrac{(p^3-1)(p^3-p)}{(p^2-1)(p^2-p)}=\dfrac{(p-1)(p^2+p+1)p(p-1)(p+1)}{(p-1)(p+1)p(p-1)}=p^2+p+1$
- $k=3$: $\#(3,3)=1$

(b) $n=4$: We have

- $k=0$: $\#(0,4)=1$
- $k=1$: $\#(1,4)=\dfrac{p^4-1}{p-1}=p^3+p^2+p+1$
- $k=2$: $\#(2,4)=\dfrac{(p^4-1)(p^4-p)}{(p^2-1)(p^2-p)}=\dfrac{(p^2-1)(p^2+1)p(p^3-1)}{(p^2-1)p(p-1)}=(p^2+1)(p^2+p+1)$
- $k=3$: $\#(3,4)=\dfrac{(p^4-1)(p^4-p)(p^4-p^2)}{(p^3-1)(p^3-p)(p^3-p^2)}=p^3+p^2+p+1$
- $k=4$: $\#(4,4)=1$

§5 - Direct Sums

5.1

Prove that the space $\mathbb{R}^{n\times n}$ of all $n \times n$ real matrices is the direct sum of the space of symmetric matrices ($A^t = A$) and the space of skew-symmetric matrices ($A^t = -A$).

Solution.

Proof.
Let SYM be the set of symmetric matrices and SKW be the set of skew-symmetric matrices. By Prop 3.6.6(c) it suffices to show $SYM \cap SKW = \{0\}$ and $SYM + SKW = \mathbb{R}^{n\times n}$.
First note

$$\begin{aligned} SYM \cap SKW &= \{A \in \mathbb{R}^{n\times n} \mid A = A^t = -A\} \\ &= \{A \in \mathbb{R}^{n\times n} \mid a_{ij} = -a_{ij} \ \ \forall i, j\} \\ &= \{A \in \mathbb{R}^{n\times n} \mid a_{ij} = 0 \ \ \forall i, j\} \\ &= \{0\} \end{aligned}$$

Thus we want to show every matrix $A \in \mathbb{R}^{n\times n}$ can be decomposed into a sum of symmetric and skew-symmetric matrices. Consider the matrices B and C where

$$b_{ij} = \tfrac{1}{2}(a_{ij} + a_{ji}) \qquad \text{and} \qquad c_{ij} = \tfrac{1}{2}(a_{ij} - a_{ji})$$

Then note that

$$\begin{cases} b_{ji} = \frac{1}{2}(a_{ji} + a_{ij}) = \frac{1}{2}(a_{ij} + a_{ji}) = b_{ij} & \implies B \in SYM \\ c_{ji} = \frac{1}{2}(a_{ji} - a_{ij}) = -\frac{1}{2}(a_{ij} - a_{ji}) = -c_{ij} & \implies C \in SKW \\ b_{ij} + c_{ij} = \frac{1}{2}((a_{ij} + a_{ji}) + (a_{ij} - a_{ji})) = a_{ij} & \implies B + C = A \end{cases}$$

Thus $A \in SYM + SKW$, and therefore $SYM \oplus SKW = \mathbb{R}^{n\times n}$. □

5.2

The trace of a square matrix is the sum of its diagonal entries. Let W_1 be the space of $n \times n$ matrices whose trace is zero. Find a subspace W_2 so that $\mathbb{R}^{n\times n} = W_1 \oplus W_2$.

Solution.
We claim $W_2 = \mathbb{Z}I = \{kI \mid k \in \mathbb{Z}\}$.

Proof.
The only scalar multiple of I with trace zero is the zero matrix, so we have $W_1 \cap \mathbb{Z}I = \{0\}$. Thus by Prop 3.6.6(c) it suffices to show $W_1 + \mathbb{Z}I = \mathbb{R}^{n\times n}$. Let A be an $n \times n$ matrix and consider the matrices kI and B where

$$k = \frac{1}{n}\sum_{i=1}^{n} a_{ii} = \frac{1}{n}\operatorname{tr}(A) \qquad \text{and} \qquad b_{ij} = \begin{cases} a_{ij} & \text{if } i \neq j \\ a_{ij} - k & \text{if } i = j \end{cases}$$

Then clearly $kI \in \mathbb{Z}I$ and

$$\operatorname{tr}(B) = \sum_{i=1}^{n} b_{ii} = \sum_{i=1}^{n}(a_{ii} - k) = \left(\sum_{i=1}^{n} a_{ii}\right) - nk = \operatorname{tr}(A) - n(\tfrac{1}{n}\operatorname{tr}(A)) = 0 \implies B \in W_1$$

Furthermore,

$$[kI + B]_{ij} = \begin{cases} 0 + a_{ij} = a_{ij} & \text{if } i \neq j \\ k + (a_{ij} - k) = a_{ij} & \text{if } i = j \end{cases} \implies kI + B = A$$

Therefore $A \in W_1 + \mathbb{Z}I$ and $\mathbb{R}^{n\times n} = W_1 \oplus \mathbb{Z}I$. □

5.3

Let $W_1, \ldots, W_k$ be subspaces of a vector space V, such that $V = \sum W_i$. Assume that $W_1 \cap W_2 = 0$, $(W_1 + W_2) \cap W_3 = 0, \ldots, (W_1 + W_2 + \cdots + W_{k-1}) \cap W_k = 0$. Prove that V is the direct sum of the subspaces $W_1, \ldots, W_k$.

Solution.

Proof.
Since we are given that $V = W_1 + \cdots + W_k$, all we have to show is that $W_1, \ldots, W_k$ are independent. We induct on k.
The base case is $k = 2$ and follows from Prop 3.6.6(b) since we are given $W_1 \cap W_2 = \{0\}$. Now assume that $W_1, \ldots, W_{k-1}$ are independent and suppose that $w_1 + \cdots + w_k = 0$ for $w_i \in W_i$. Note that

$$\begin{aligned} -w_k = w_1 + \cdots + w_{k-1} \in W_1 + \cdots + W_k &\implies -w_k \in (W_1 + \cdots + W_{k-1}) \cap W_k = \{0\} \\ &\implies -w_k = 0 \\ &\implies w_k = 0 \end{aligned}$$

Hence we have $w_1 + \cdots + w_{k-1} = 0$. But by IH we have $W_1, \ldots, W_{k-1}$ independent and so $w_1 = \cdots = w_{k-1} = 0$. Therefore every w_i is zero and $W_1, \ldots, W_k$ are independent. □

6.1

Let $\mathbf{E}$ be the set of vectors $(e_1, e_2, \dots)$ in $\mathbb{R}^\infty$, and let $w = (1, 1, 1, \dots)$. Describe the span of the set $(w, e_1, e_2, \dots)$.

Solution.
We claim that

$$\operatorname{span}\{w, e_1, e_2, \dots\} = Z_{\mathbb{R}} := \bigcup_{x \in \mathbb{R}} Z_x$$

where $Z_x := \{(a) \in \mathbb{R}^\infty \mid a_n = x \text{ for all but finitely many } n\}$.

Proof.
First choose $(a) \in \operatorname{span}\{w, e_1, e_2, \dots\}$. Then there exists a finite index set J such that

$$(a) = bw + \sum_{j \in J} c_j e_j$$

Then by construction of w, we have that $a_n = b$ for all but finitely many n, namely for all $n \notin J$. Thus $(a) \in Z_b \subset Z_{\mathbb{R}}$.
Next, choose $(b) \in Z_{\mathbb{R}}$. Then there exists $x \in \mathbb{R}$ such that $b_n = x$ for all but finitely many n. Let $J = \{n \in \mathbb{N} \mid b_n \neq x\}$ and define $c_j = b_j - x$ for all $j \in J$. Now $x \cdot w_j + c_j = x \cdot 1 + (b_j - x) = b_j$ for all $j \in J$ and so

$$(b) = xw + \sum_{j \in J} c_j e_j \in \operatorname{span}\{w, e_1, e_2, \dots\}$$

Therefore we have both inclusions and $\operatorname{span}\{w, e_1, e_2, \dots\} = Z_{\mathbb{R}}$. □

6.2

The doubly infinite row vectors $(a) = (\dots, a_{-1}, a_0, a_1, \dots)$, with a_i real form a vector space. Prove that this space is isomorphic to $\mathbb{R}^\infty$.

Solution.

Proof.
The very useful set-theoretic fact we need is that $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality. Indeed, consider the bijection

$$f : \mathbb{N} \to \mathbb{Z}, \qquad f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

If we denote the set of doubly infinite row vectors by $\mathbb{R}^{\pm\infty}$, then consider the map

$$\varphi : \mathbb{R}^\infty \to \mathbb{R}^{\pm\infty}$$

where given $(a) \in \mathbb{R}^\infty$, we define $\varphi(a)_n = a_{g(n)}$, where $g = f^{-1}$. This map is bijective, namely with inverse $\psi(b)_n = b_{f(n)}$. Furthermore, note that for all n we have

$$\varphi(a+b)_n = (a+b)_{g(n)} = a_{g(n)} + b_{g(n)} = \varphi(a)_n + \varphi(b)_n \implies \varphi(a+b) = \varphi(a) + \varphi(b)$$

and

$$\varphi(c \cdot (a))_n = (c \cdot (a))_{g(n)} = c \cdot a_{g(n)} = c \cdot \varphi(a)_n \implies \varphi(c \cdot (a)) = c \cdot \varphi(a)$$

Thus φ is a vector space isomorphism. □

6.3

For every positive integer, we can define the space ℓ^p to be the space of sequences such that $\sum |a_i|^p < \infty$. Prove that ℓ^p is a proper subspace of ℓ^{p+1}.

Solution.

Proof.
This is really a question in analysis more than anything, but note that if we have a sequence $(a) \in \ell^p$, then

$$\sum_{n=1}^{\infty} |a_n|^p < \infty \implies \lim_{n\to\infty} |a_n|^p = 0$$

In particular, this means that there exists $N > 0$ such that $|a_m|^p < 1$ for all $m \geq N$ and $\sum_{m=N}^{\infty} |a_m|^p < \infty$. Furthermore, $|a_m|^p < 1 \implies |a_m| < 1$ and so

$$\sum_{m=N}^{\infty} |a_m|^{p+1} = \sum_{m=N}^{\infty} |a_m|^p |a_m| < \sum_{m=N}^{\infty} |a_m|^p < \infty$$

and clearly $\sum_{n=1}^{N-1} |a_n|^{p+1}$ is finite, so we have $\sum_{n=1}^{\infty} |a_n|^{p+1} < \infty$ and $(a) \in \ell^{p+1}$, or in short, $\ell^p \subset \ell^{p+1}$, and since both are vector spaces it is a subspace. Finally, to show it is proper we need to find a sequence $(a) \in \ell^{p+1}$ such that $(a) \notin \ell^p$. Consider the sequence

$$a_n = \frac{1}{\sqrt[p]{n}}$$

Then

$$\sum_{n=1}^{\infty} |a_n|^p = \sum_{n=1}^{\infty} \frac{1}{n} \not< \infty \qquad \text{and} \qquad \sum_{n=1}^{\infty} |a_n|^{p+1} = \sum_{n=1}^{\infty} \frac{1}{n^{1+1/p}} < \infty$$

by the p-series test. Therefore ℓ^p is a proper subspace of ℓ^{p+1}. □

6.4

Let V be a vector space that is spanned by a countably infinite set. Prove that every independent subset of V is finite or countably infinite.

Solution.

Proof.
Let $V = \operatorname{span}\{v_1, v_2, \dots\}$ and let $S \subset V$ be an independent subset. Note that for every $w \in S$ and by definition of span, there exists a positive integer k such that $w \in \operatorname{span}\{v_1, v_2, \dots, v_k\}$. Hence for every $w \in S$, define

$$k_w := \min\{k \in \mathbb{N} \mid w \in \operatorname{span}\{v_1, v_2, \dots, v_k\}\}$$

We claim that for every $K \in \mathbb{N}$, there are only finitely many $w \in S$ such that $k_w = K$.

> To see this, choose $K \in \mathbb{N}$ and let $S_K = \{w \in S \mid k_w = K\}$. Note that $S_K \subset S$ is the subset of an independent set, so it must also be independent. However, we also have that $S \subset \operatorname{span}\{v_1, \dots, v_K\}$ is the subset of a finite-dimensional subspace, so by Corollary 3.7.7, S_K is finite.

Again since $S \subset V = \operatorname{span}\{v_1, v_2, \dots\}$, we then have

$$S = \bigcup_{K \in \mathbb{N}} \{w \in S \mid k_w = K\}$$

which is a countable union of finite sets, therefore S is countable (finite or countably infinite). □

[NB: For those worried about Axiom of Choice when defining k_w, this definition only needs the well-orderedness of $\mathbb{N}$; it *would* be an issue if we were to choose a finite linear combination for each $x \in S$, since the whole point is that we do not know a priori that S is countable.]

M.1

Consider the determinant function $\det : F^{2\times 2} \to F$, where $F = \mathbb{F}_p$ is the prime field of order p and $F^{2\times 2}$ is the space of 2×2 matrices. Show that this map is surjective, that all nonzero values of the determinant are taken on the same number of times, but that there are more matrices with determinant 0 than with determinant 1.

Solution.
First, for sujectivity note for any $k \in F$ that

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

Next, note that if we restrict our determinant to $\varphi : GL_2(F) \to F^\times$, we have a surjective homomorphism (as $\det(AB) = (\det A)(\det B)$) with kernel $SL_2(F)$, and so by Prop 2.7.15 we have the inverse image $\varphi^{-1}(k)$ is the coset $kSL_2(F)$. In particular, every coset has the same number of elements and thus for every $k \in F^\times$,

$$\big|\{\det A = k\}\big| = \big|\varphi^{-1}(k)\big| = \big|kSL_2(F)\big| = \big|SL_2(F)\big| = \big|\{\det A = 1\}\big|$$

and so every nonzero value of the determinant is taken on the same number of times.

Finally, we have from Exercise 4.4(b) that the order of $GL_2(\mathbb{F}_p)$ is $p(p+1)(p-1)^2$ and clearly the order of $F^{2\times 2}$ is p^4, so the number of matrices with determinant 0 is

$$\big|\{\det A = 0\}\big| = p^4 - |GL_2(F)| = p^4 - (p^4 - p^3 - p^2 + p) = p^3 + p^2 - p$$

But we also have from Exercise 4.4(b) that the order of $SL_2(\mathbb{F}_p)$ is $p(p+1)(p-1)$ and so

$$\big|\{\det A = 1\}\big| = |SL_2(F)| = p^3 - p < p^3 - p + p^2 = \big|\{\det A = 0\}\big|$$

M.2

Let A be a real $n \times n$ matrix. Prove that there is an integer N such that A satisfies a nontrivial polynomial relation $A^N + c_{N-1}A^{N-1} + \cdots + c_1 A + c_0 = 0$.

Solution.

Proof.
Note that we can consider the $n \times n$ matrix A as a vector in $\mathbb{R}^{n^2}$, and so define the vector a_k to correspond to A^k. Then by Theorem 3.4.18 (more specifically, its contrapositive) we have that any set of n^2+1 vectors in $\mathbb{R}^{n^2}$ must be linearly dependent, i.e. there exists a nontrivial relation

$$b_{n^2+1}a_{n^2+1} + \cdots + b_1 a_1 = 0$$

and let N be the largest index such that $b_N \neq 0$. Then we have

$$b_N a_N + \cdots + b_1 a_1 = 0$$

Finally set $c_0 = 0$ and $c_i = \frac{b_i}{b_N}$ for $i = 1, \ldots, N$ to get

$$\begin{aligned} 0 &= b_N a_N + b_{N-1}a_{N-1} + \cdots + b_1 a_1 \\ &= \frac{b_N}{b_N}a_N + \frac{b_{N-1}}{b_N}a_{N-1} + \cdots + \frac{b_1}{b_N}a_1 + 0 \\ &= a_N + c_{N-1}a_{N-1} + \cdots + c_1 a_1 + c_0 \end{aligned}$$

And since the zero vector corresponds to the zero matrix, this gives

$$A^N + c_{N-1}A^{N-1} + \cdots + c_1 A + c_0 = 0$$

□

M.3

(a) Let $x(t)$ and $y(t)$ be quadratic polynomials with real coefficients. Prove that the image of the path $(x(t), y(t))$ is contained in a conic, i.e., that there is a real quadratic polynomial $f(x, y)$ such that $f(x(t), y(t))$ is identically zero.

(b) Let $x(t) = t^2 - 1$ and $y(t) = t^3 - t$. Find a nonzero real polynomial $f(x, y)$ such that $f(x(t), y(t))$ is identically zero. Sketch the locus $\{f(x, y) = 0\}$ and the path $(x(t), y(t))$ in $\mathbb{R}^2$.

(c) Prove that every pair $x(t), y(t)$ of real polynomials satisfies some real polynomial relation $f(x, y) = 0$.

Solution.

(a) *Proof.*
Note that any quadratic polynomial $F(x, y)$ is of the form

$$F(x, y) = a + bx + cy + dx^2 + ey^2 + fxy$$

and our path components are of the form

$$x(t) = \alpha_1 + \alpha_2 t + \alpha_3 t^2 \quad \text{and} \quad y(t) = \beta_1 + \beta_2 t + \beta_3 t^2$$

Hence when we plug these into F we get (as a polynomial in t)

$$\begin{aligned}
F(x(t), y(t)) &= a + b(x(t)) + c(y(t)) + d(x(t))^2 + e(y(t))^2 + f((x(t)y(t)) \\
&= a + b(\alpha_1 + \alpha_2 t + \alpha_3 t^2) + c(\beta_1 + \beta_2 t + \beta_3 t^2) + d(\alpha_1 + \alpha_2 t + \alpha_3 t^2)^2 \\
&\quad + e(\beta_1 + \beta_2 t + \beta_3 t^2)^2 + f([\alpha_1 + \alpha_2 t + \alpha_3 t^2][\beta_1 + \beta_2 t + \beta_3 t^2]) \\
&= (a + b\alpha_1 + c\beta_1 + d\alpha_1^2 + e\beta_1^2 + f\alpha_1\beta_1) \\
&\quad + t(b\alpha_2 + c\beta_2 + 2d\alpha_1\alpha_2 + 2e\beta_1\beta_2 + f[\alpha_1\beta_2 + \alpha_2\beta_1]) \\
&\quad + t^2(b\alpha_3 + c\beta_3 + d[2\alpha_1\alpha_3 + \alpha_2^2] + e[2\beta_1\beta_3 + \beta_2^2] + f[\alpha_1\beta_3 + \alpha_2\beta_2 + \alpha_3\beta_1]) \\
&\quad + t^3(2d\alpha_2\alpha_3 + 2e\beta_2\beta_3 + f[\alpha_2\beta_3 + \alpha_3\beta_2]) \\
&\quad + t^4(d\alpha_3^2 + e\alpha_3^2 + f\alpha_3\beta_3)
\end{aligned}$$

Hence to get $F(x(t), y(t))$ to be identically zero, we need to solve the system

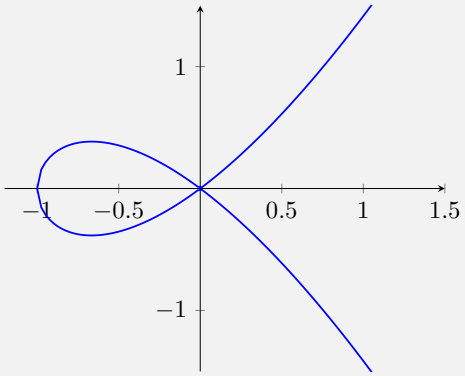
$$\begin{cases}
a + b\alpha_1 + c\beta_1 + d\alpha_1^2 + e\beta_1^2 + f\alpha_1\beta_1 = 0 \\
b\alpha_2 + c\beta_2 + 2d\alpha_1\alpha_2 + 2e\beta_1\beta_2 + f[\alpha_1\beta_2 + \alpha_2\beta_1] = 0 \\
b\alpha_3 + c\beta_3 + d[2\alpha_1\alpha_3 + \alpha_2^2] + e[2\beta_1\beta_3 + \beta_2^2] + f[\alpha_1\beta_3 + \alpha_2\beta_2 + \alpha_3\beta_1] = 0 \\
2d\alpha_2\alpha_3 + 2e\beta_2\beta_3 + f[\alpha_2\beta_3 + \alpha_3\beta_2] = 0 \\
d\alpha_3^2 + e\alpha_3^2 + f\alpha_3\beta_3 = 0
\end{cases}$$

which is five equations in six unknowns (a, b, c, d, e, f), which will always have a solution and thus such an F will always exist. □

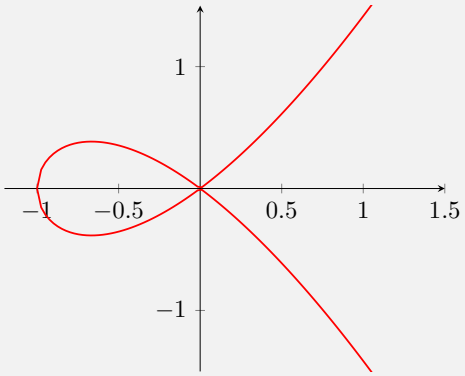
(b) Note that $y(t) = t(t^2-1) = tx(t)$, so $y^2 = t^2x^2 = (x+1)x^2$. Thus the polynomial $F(x,y) = y^2 - (x+1)x^2$ should work. Indeed,

$$\begin{aligned} F(x(t),y(t)) &= (t^3-t)^2 - ((t^2-1)+1)(t^2-1)^2 \\ &= (t^6 - 2t^4 + t^2) - t^2(t^4 - 2t^2 + 1) \\ &= 0 \end{aligned}$$

We now graph:



$\{F(x,y) = 0\}$



$(x(t), y(t))$

And note the two are the exact same.

(c) *Proof.*
Let $x(t)$ and $y(t)$ be polynomials in t of degree n. Note that any polynomial $F(x,y)$ of degree m is a linear combination of

$$\{1, x, y, x^2, y^2, xy, \ldots, x^m, x^{m-1}y, \ldots, xy^{m-1}, y^m\} = \{x^iy^j \mid 0 \le i+j \le m\}$$

and hence $F(x(t),y(t))$ will be a polynomial in t of degree $\le mn$. Furthermore, we have

$$\left|\{x^iy^j \mid 0 \le i+j \le m\}\right| = \left|\{(i,j) \mid i+j = k \text{ for } k = 0,\ldots,m\}\right| = \sum_{k=0}^{m}(k+1) = \frac{1}{2}[(m+1)(m+2)]$$

So we want the case, as in the proof of (a), of the polynomial $F(x(t),y(t))$ with $\le mn+1$ terms being less than the $\frac{1}{2}[(m+1)(m+2)]$ coefficients we get in $F(x,y)$. In other words, given a fixed n, we want to find an m such that $\frac{1}{2}[(m+1)(m+2)] > mn+1$. Indeed, note

$$\frac{(m+1)(m+2)}{2} > mn+1 \iff m^2+3m+2 > 2mn+2 \iff m^2+(3-2n)m > 0$$

which holds for any $m > 2n-3$, say $m = 2n-2$. Therefore every pair $x(t), y(t)$ of degree-n polynomials satisfy a nonzero degree-$(2n-2)$ polynomial relation $F(x,y) = 0$. □

M.4

Let V be a vector space over an infinite field F. Prove that V is not the union of finitely many proper subspaces.

Solution.

Proof.
Suppose otherwise, i.e. there exists proper subspaces $W_1, \dots, W_n$ such that $V = W_1 \cup \cdots \cup W_n$. Without loss of generality, let n be the smallest number of proper subspaces needed. Now choose $v_1 \in W_1$ such that $v_1 \notin W_2 \cup \cdots \cup W_n$. Note that v_1 must exist since otherwise

$$W_1 \subset W_2 \cup \cdots \cup W_n \implies V = W_1 \cup W_2 \cup \cdots \cup W_n = W_2 \cup \cdots \cup W_n$$

which contradicts the minimality of n. Next choose $v_2 \in V \setminus W_1$ (which is nonempty since W_1 is proper) and consider elements on the "line" $L := \{v_1 + \alpha v_2 \mid \alpha \in F\}$. Since this is a subset of V, it must intersect some W_i. We consider cases:

- $i = 1$: Note that if there exists a nonzero $\alpha \in F$ such that $v_1 + \alpha v_2 \in W_1$, then

  $$\alpha v_2 = (v_1 + \alpha v_2) - v_1 \in W_1 \implies v_2 = \alpha^{-1}(\alpha v_2) \in W_1$$

  which is impossible. Thus $L \cap W_1 = \{v_1\}$ (as $v_1 \in L$ when we take $\alpha = 0$).

- $i \geq 2$: Note that if $L \cap W_i$ has at least two elements, then there exists distinct elements $\alpha, \beta \in F$ such that

  $$v_1 + \alpha v_2, v_1 + \beta v_2 \in W_i \implies (\alpha - \beta)v_2 = (v_1 + \alpha v_2) - (v_1 + \beta v_2) \in W_i \implies v_2 \in W_i$$

  and

  $$v_2 \in W_i \implies \alpha v_2 \in W_i \implies v_1 = (v_1 + \alpha v_2) - (\alpha v_2) \in W_i$$

  Hence $v_1 \in W_i$ for some $i \geq 2$, which is impossible. Therefore $L \cap W_i$ can have at most one element for all $i \geq 2$.

Thus we have

$$L = L \cap V = \bigcup_{i=1}^{n} L \cap W_i$$

which is a finite union of finite (specifically of order ≤ 1) sets, so L is finite. However, note that since F is infinite, L must be infinite. Therefore we have a contradiction and so V is not a finite union of proper subspaces. □

M.5

Let α be the real cube root of 2.

(a) Prove that $(1, \alpha, \alpha^2)$ is an independent set over $\mathbb{Q}$, i.e., that there is no relation of the form $a + b\alpha + c\alpha^2 = 0$ with integers a, b, c.
Hint: Divide $x^3 - 2$ by $cx^2 + bx + a$.

(b) Prove that the real numbers $a + b\alpha + c\alpha^2$ with a, b, c in $\mathbb{Q}$ form a field.

Solution.

(a) *Proof.*
Suppose otherwise, i.e. we can find rational numbers $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}$ (not all zero) such that $\frac{p_1}{q_1} + \frac{p_2}{q_2}\alpha + \frac{p_3}{q_3}\alpha^2 = 0$. Since we can simply clear out all the denominators by multiplying by $q_1q_2q_3$, without loss of generality we may assume $a + b\alpha + c\alpha^2 = 0$ for integers a, b, c not all zero. Furthermore, note that if $c = 0$, then we have

$$b\alpha + a = 0 \implies \alpha = -\frac{a}{b} \in \mathbb{Q}$$

which is impossible and so $c \neq 0$.
Thus we have α as a root of the polynomial $f(x) = cx^2 + bx + a$, along with $g(x) = x^3 - 2$ by construction. We now perform polynomial division, i.e. write $g(x) = q(x)f(x) + r(x)$ for polynomials q and r. In particular we get

$$q(x) = \frac{1}{c}x - \frac{b}{c^2} \quad \text{and} \quad r(x) = \left(\frac{b^2}{c^2} - \frac{a}{c}\right)x + \left(\frac{ab}{c^2} - 2\right) =: Ax + B$$

Note that if we plug in $x = \alpha$ we get

$$0 = g(\alpha) = q(\alpha) \cdot f(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha)$$

But

$$r(\alpha) = 0 \implies A\alpha + B = 0 \implies \alpha = -\frac{B}{A} \in \mathbb{Q} \text{ or } A = 0$$

and since $\alpha \in \mathbb{Q}$ is impossible, this forces $A = 0$ and so $B = 0$ also. Then

$$A = 0 \implies \frac{b^2}{c^2} - \frac{a}{c} = 0 \implies b^2 - ac = 0 \implies a = \frac{b^2}{c}$$

Now

$$B = 0 \implies a\frac{b}{c^2} - 2 = 0 \implies \frac{b^3}{c^3} = 2 \implies \alpha = \frac{b}{c} \in \mathbb{Q}$$

which is a contradiction, so our assumption is false and therefore $(1, \alpha, \alpha^2)$ is independent. $\square$

(b) *Proof.*
First note that with addition

$$(a+b\alpha+c\alpha^2)+(x+y\alpha+z\alpha^2)=(a+x)+(b+y)\alpha+(c+z)\alpha^2$$

clearly we have closure, associativity, commutativity, identity $0+0\alpha+0\alpha^2$, and inverses $(-a)+(-b)\alpha+(-c)\alpha^2$. Next we turn to multiplication.
We have product

$$\begin{aligned}(a+b\alpha+c\alpha^2)(x+y\alpha+z\alpha^2) &= ax+ay\alpha+ax\alpha^2+bx\alpha+by\alpha^2+bz\alpha^3+cx\alpha^2+cy\alpha^3+cz\alpha^4\\ &= (ax+2bz+2cy)+(ay+bx+2cz)\alpha+(az+by+cx)\alpha^2\end{aligned}$$

From this we have closure, associativity, commutativity, and identity $1+0\alpha+0\alpha^2$. So all we need to show is that we have multiplicative inverses. Given $a+b\alpha+c\alpha^2\neq 0$, we want to find $x,y,z\in\mathbb{Q}$ such that the above product is $1+0\alpha+0\alpha^2$, i.e. we have the system

$$\begin{cases} ax+2bz+2cy &= 1\\ ay+bx+2cz &= 0\\ az+by+cx &= 0\end{cases} \quad\leftrightsquigarrow\quad \begin{bmatrix}a & 2c & 2b\\ b & a & 2c\\ c & b & a\end{bmatrix}\begin{bmatrix}x\\y\\z\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix} \tag{$\star$}$$

Theorem 1.2.21 implies that ($\star$) has a unique solution in $\mathbb{Q}$ if and only if

$$\begin{bmatrix}a & 2c & 2b\\ b & a & 2c\\ c & b & a\end{bmatrix}\begin{bmatrix}x\\y\\z\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix} \tag{$\dagger$}$$

only has the trivial solution in $\mathbb{Q}$. Thus if ($\dagger$) has a nontrivial solution, we have

$$\begin{bmatrix}a & 2c & 2b\\ b & a & 2c\\ c & b & a\end{bmatrix}\begin{bmatrix}x\\y\\z\end{bmatrix}=\begin{bmatrix}0\\0\\0\end{bmatrix} \implies (a+b\alpha+c\alpha^2)(x+y\alpha+z\alpha^2)=0+0\alpha+0\alpha^2$$

and since we have $a+b\alpha+c\alpha^2\neq 0$, this forces $x+y\alpha+z\alpha^2=0$ for $(x,y,z)\neq(0,0,0)$, which contradicts (a). Thus ($\star$) will always have a solution in $\mathbb{Q}$, and so $(a+b\alpha+c\alpha^2)^{-1}$ exists and therefore $\{a+b\alpha+c\alpha^2 \mid a,b,c\in\mathbb{Q}\}$ is a field. □

M.6

My cousin Phil collects hot sauce. He has about a hundred different bottles on the shelf, and many of them, Tabasco for instance, have only three ingredients other than water: chilis, vinegar, and salt. What is the smallest number of bottles of hot sauce that Phil would need to keep on hand so that he could obtain any recipe that uses only these three ingredients by mixing the ones he had?

Solution.
If we treat each recipe as a vector in $\mathbb{R}^3$ where each component is the amount of chilis, vinegar, and salt respectively, then we are simply looking for a basis of $\mathbb{R}^3$, which will have 3 vectors. Hence 3 bottles of hot sauce is the smallest number needed.