Exercise 1

Let V be the vector space of polynomials of degree at most 5, with coefficients in a field $\mathbb{F}$. Let U be the subspace of V consisting of polynomials of the form az^5+bz+c with $a, b, c \in \mathbb{F}$. Find a subspace W such that every element $v \in V$ can be written in one and only one way as the sum of an element in U and another element in W.

Let W be the subspace of V consisting of polynomials of the form $rz^4 + sz^3 + tz^2$ with $r, s, t \in \mathbb{F}$.

First we check that W is a subspace; note that setting $r = s = t = 0$ gives us $0 \in W$; furthermore if we have $\lambda \in F, r_1z^4+s_1z^3+t_1z^2, r_2z^4+s_2z^3+t_2z^2 \in W$ we see that $\lambda(r_1z^4 + s_1z^3 + t_1z^2) = \lambda r_1z^4 + \lambda s_1z^3 + \lambda t_1z^2 \in W$ and $(r_1z^4 + s_1z^3 + t_1z^2) + (r_2z^4 + s_2z^3 + t_2z^2) = (r_1 + r_2)z^4 + (s_1 + s_2)z^3 + (t_1 + t_2)z^2 \in W$. Hence W contains 0 and is closed under scalar multiplication and addition, so it is a subspace of V.

Now we wish to show that every element $v \in V$ can be written in exactly one way as $u + w$ for $u \in U, w \in W$.

Consider some $v = \lambda_5z^5 + \lambda_4z^4 + \lambda_3z^3 + \lambda_2z^2 + \lambda_1z + \lambda_0 \in V$. By the definitions of U and W, we see that $u = \lambda_5z^5 + \lambda_1z + \lambda_0 \in U$ and $w = \lambda_4z^4 + \lambda_3z^3 + \lambda_2z^2 \in W$, with $u + w = v$.

Hence we have shown that every element $v \in V$ can be written in at least one way as $u + w$ for $u \in U, w \in W$. Now we wish to show that this expression is unique.

First we will show that $U \cap W = 0$.

Consider some $x \in U \cap W$. By the definitions of U and W, there exist $a, b, c, r, s, t \in \mathbb{F}$ such that $x = az^5 + bz + c = rz^4 + sz^3 + tz^2$. Since two polynomials are equal if and only if all their coefficients are equal, it is immediate that $a = b = c = r = s = t = 0$. Hence $x = 0$, so $U \cap W = 0$.

Consider $u_1, u_2 \in U, w_1, w_2 \in W$ such that $u_1 + w_1 = u_2 + w_2$. Then $u_1 - u_2 = w_2 - w_1$.

Since $u_1, u_2 \in U$, we see that $u_1 - u_2 \in U$. SImilarly $w_2 - w_1 \in W$. Therefore $u_1 - u_2 = w_2 - w_1$ is in $U \cap W$; however, this implies by the above that $u_1 - u_2 = w_2 - w_1 = 0$. Hence $u_1 = u_2$ and $w_1 = w_2$. Therefore if $v \in V$ is equal to $u + w$ where $u \in U, w \in W$, this decomposition is necessarily unique since every such decomposition is equal.

Exercise 2

Prove that there exists a quadratic polynomial $ax^2 + bx + c$ whose graph passes through the points $(0, 1), (1, 0), (2, 3)$. Is such a polynomial unique?

If such a quadratic polynomial $ax^2 + bx + c$ existed, then necessarily we would have (because of the points it must pass through):

$$\begin{aligned} a(0)^2 + b(0) + c &= 1 \\ a(1)^2 + b(1) + c &= 0 \\ a(2)^2 + b(2) + c &= 3 \end{aligned}$$

or, simplifying:

$$\begin{aligned} c &= 1 \\ a + b + c &= 0 \\ 4a + 2b + c &= 3 \end{aligned}$$

If a, b, c solve the equations given above, that will imply that $ax^2 + bx + c$ is the desired quadratic polynomial (we check by setting $x = 0, 1, 2$). Conversely, if $ax^2 + bx + c$ is the desired quadratic polynomial, then it must satisfy the equations above.

Since $c = 1$, the second equation $a + b + c = 0$ implies $a + b = -1$. Substituting $b = -1 - a$ and $c = 1$ into the third equation, we get:

$$4a + 2(-1 - a) + 1 = 4a - 2 - 2a + 1 = 2a - 1 = 3.$$

Then since $2a - 1 = 3$, we must have $a = 2$, which immediately implies $b = -3, c = 1$.

Since the steps we took to solve the equations for a, b, c were all reversible, the solution $a = 2, b = -3, c = 1$ is the only such solution; thus $2x^2 - 3x + 1$ is the desired polynomial, and it is also unique.

Exercise 3

Find a single homogeneous linear equation with unknowns x_1, x_2, x_3 such that the solution set is the span of the two vectors $(1,1,1), (1,-2,0)$.

We wish to find a, b, c so that the solution set of $ax_1 + bx_2 + cx_3 = 0$ is the span of the two vectors $(1,1,1), (1,-2,0)$.

This implies that we must have

$$a + b + c = 0, a - 2b = 0.$$

The second equation implies $a = 2b$; substituting into the first equation, we get $3b + c = 0$. Since we only wish to find a single homogeneous linear equation, we might try $b = 1$, which forces $a = 2, c = -3$.

Now we consider the equation we have found: $2x_1 + x_2 - 3x_3 = 0$. The span of the two vectors $(1,1,1), (1,-2,0)$ may be described as $W = \{r(1,1,1) + s(1,-2,0) = (r+s, r-2s, r) : r, s \in \mathbb{R}\}$.

For any $r, s \in \mathbb{R}$, we see that

$$2(r+s) + r - 2s - 3r = 2r + 2s + r - 2s - 3r = 0.$$

Hence any element in W satisfies the equation $2x_1 + x_2 - 3x_3 = 0$, so W is the solution set of $2x_1 + x_2 - 3x_3 = 0$.

Exercise 4

Let V be a vector space and suppose $S = \{v_1, \ldots, v_k\}$ is a finite set of linearly dependent vectors in V. Prove there is a proper subset of S whose span is equal to the span of S.

Now we fix $S = \{v_1, \ldots, v_k\}$ a finite set of linearly dependent vectors in V. By Simon Chapter 1 Section 3 Lemma 3.6, there must exist some $j \in \{1, \ldots, k\}$ and constants c_i for $i \neq j$ such that $v_j = \sum_{i=1, i\neq j}^{k} c_i v_i$.

Now we will show that $T = S \setminus \{v_j\}$ is the desired proper subset of S.

Consider some w in the span of T. Then by definition of span, $w = \sum_{i=1, i\neq j}^{k} a_i v_i$ for some a_i constants (for $i \neq j$). Setting $a_j = 0$, we see that $w = \sum_{i=1}^{k} a_i v_i$, so w must be in the span of S.

Now consider some u in the span of S; by definition of span, we have some constants b_i so that

$$\begin{aligned} u &= \sum_{i=1}^{k} b_i v_i \\ &= b_j v_j + \sum_{i=1, i\neq j}^{k} b_i v_i \\ &= b_j \left(\sum_{i=1, i\neq j}^{k} c_i v_i \right) + \sum_{i=1, i\neq j}^{k} b_i v_i \\ &= \sum_{i=1 i, i\neq j}^{k} (b_i + b_j c_i) v_i \end{aligned}$$

from which it is clear that u is in the span of T.

Since $v_j \in S$ but $v_j \notin T$, we see that T is a proper subset of S; then since the span of T is equal to the span of S, we have found our desired proper subset.

Exercise 5

Use Gaussian elimination in $\mathbb{R}$ to show that the solution set of the homogeneous system

$$\begin{aligned} x_1 + 2x_2 + 3x_3 + 4x_4 &= 0 \\ x_1 + 4x_2 + 3x_3 + 2x_4 &= 0 \\ 2x_1 + 5x_2 + 6x_3 + 7x_4 &= 0 \\ x_1 + 3x_3 + 6x_4 &= 0 \end{aligned}$$

is a plane through 0 (the span of two linearly independent vectors) and find 2 linearly independent vectors whose span is the solution space.

We follow the steps of Gaussian elimination in Chapter 1 Section 4 of Simon.

Our initial set of equations is:

$$\begin{aligned} x_1 + 2x_2 + 3x_3 + 4x_4 &= 0 \\ x_1 + 4x_2 + 3x_3 + 2x_4 &= 0 \\ 2x_1 + 5x_2 + 6x_3 + 7x_4 &= 0 \\ x_1 + 3x_3 + 6x_4 &= 0 \end{aligned}$$

We note that the first equation already has a coefficient of 1 for x_1. Therefore for our first step, we subtract the first equation from the second equation; subtract twice the first equation from the third equation; and subtract the first equation from the fourth equation. This gives us

$$\begin{aligned} x_1 + 2x_2 + 3x_3 + 4x_4 &= 0 \\ 2x_2 - 2x_4 &= 0 \\ x_2 - x_4 &= 0 \\ -2x_2 + 2x_4 &= 0 \end{aligned}$$

We now recognize that the second equation is twice the third and the fourth equation is negative two times the third equation. Then by subtracting twice the third equation from the second, and adding twice the third equation to the fourth, we get:

$$\begin{aligned} x_1 + 2x_2 + 3x_3 + 4x_4 &= 0 \\ 0 &= 0 \\ x_2 - x_4 &= 0 \\ 0 &= 0 \end{aligned}$$

The set of solutions to these equations is the same as for our four original equations. Ignoring equations $0 = 0$, we are left with the system:

$$\begin{aligned} x_1 + 2x_2 + 3x_3 + 4x_4 &= 0 \\ x_2 - x_4 &= 0 \end{aligned}$$

We now solve from the bottom up. The second equation implies that $x_2 = x_4$; therefore, we may substitute this in to the first equation to get $x_1 + 6x_2 + 3x_3 = 0$. Solving for x_3 in terms of the other two variables, we see that $x_3 = -2x_2 - \frac{1}{3}x_1$.

If we allow x_1, x_2 to be any $s, t \in \mathbb{R}$, we see that any solution to our original homogeneous system must take the form $(s, t, -2t - \frac{1}{3}s, t)$ for some s, t. To see that all vectors in this form are a solution of the homogeneous system, we may substitute in the appropriate values $x_1 = s, x_2 = t, x_3 = -2t - s/3, x_4 = t$.

$$\begin{aligned} s + 2t + 3(-2t - s/3) + 4t &= s + 2t - 6t - s + 4t \\ &= 0 \\ s + 4t + 3(-2t - s/3) + 2t &= s + 4t - 4t - s + 2t \\ &= 0 \\ 2s + 5t + 6(-2t - s/3) + 7t &= 2s + 5t - 12t - 2s + 7t \\ &= 0 \\ s + 3(-2t - s/3) + 6t &= s - 6t - s + 6t \\ &= 0 \end{aligned}$$

Therefore the solution set of our homogeneous system is $\{(s, t, -2t - \frac{1}{3}s, t) : s, t \in \mathbb{R}\}$.

Now we note that, as vectors,

$$(s, t, -2t - \frac{1}{3}s, t) = s(1, 0, -1/3, 0) + t(0, 1, -2, 1).$$

Therefore

$$\{(s, t, -2t - \frac{1}{3}s, t) : s, t \in \mathbb{R}\} = \{s(1, 0, -1/3, 0) + t(0, 1, -2, 1) : s, t \in \mathbb{R}\}$$

is just the span of the vectors $(1, 0, -1/3, 0), (0, 1, -2, 1)$, which are linearly independent by inspection.

Exercise 6

(a) Suppose $a \in \mathbb{Z}/p\mathbb{Z}, a \neq 0$. For any $x, y \in \mathbb{Z}/p\mathbb{Z}$ show that if $ax = ay$ then $x = y$.

(b) By considering the set $\{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$ over $\mathbb{Z}/p\mathbb{Z}$ or otherwise, show that there exists $b \in \mathbb{Z}/p\mathbb{Z}$ such that $ab = 1$.

(c) In the set of integers $\mathbb{Z}$, solve the system of equations $2x + y = 2 \mod 5, 3x - 2y = 0 \mod 5$ by using Gaussian elimination in $\mathbb{Z}/5\mathbb{Z}$.

(a) We have $a \in \mathbb{Z}/p\mathbb{Z}, a \neq 0$, and we wish to show that if $ax = ay$ then $x = y$ for any $x, y \in \mathbb{Z}/p\mathbb{Z}$.

We choose $\bar{a}, \bar{x}, \bar{y} \in \mathbb{Z}$ which represent a, x, y in $\mathbb{Z}/p\mathbb{Z}$ respectively.

If $ax = ay$ in $\mathbb{Z}/p\mathbb{Z}$, then $\bar{a}\bar{x} \equiv \bar{a}\bar{y} \mod p$. Therefore there exists some $n \in \mathbb{Z}$ with $\bar{a}\bar{x} = \bar{a}\bar{y} + np$. Then $np = \bar{a}(\bar{x} - \bar{y})$; since $n \in \mathbb{Z}$, we must have $p \mid \bar{a}(\bar{x} - \bar{y})$. Since p is prime, either $p \mid \bar{a}$ or $p \mid (\bar{x} - \bar{y})$.

If $p \mid \bar{a}$, then $\bar{a} \equiv 0 \mod p$, which would mean $a = 0$ in $\mathbb{Z}/p\mathbb{Z}$, contradicting our hypothesis.

Therefore we must have $p \mid (\bar{x} - \bar{y})$; then $\bar{x} - \bar{y} \equiv 0 \mod p$, meaning $x - y = 0$ in $\mathbb{Z}/p\mathbb{Z}$. This means that $ax = ay$ in $\mathbb{Z}/p\mathbb{Z}$ for $a \neq 0$ implies $x - y = 0$, or $x = y$.

(b) We consider the set $S = \{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$ in $\mathbb{Z}/p\mathbb{Z}$. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is a function defined by $f(x) = ax$, we see that S is the range of f.

Part (a) tells us that if for some $x, y \in \mathbb{Z}/p\mathbb{Z}$ we have $ax = ay$, then $x = y$. Therefore if $f(x) = f(y)$, then $x = y$, implying that f is injective.

Therefore f is an injective function from a finite set to itself; it is then necessarily surjective. Therefore there exists $b \in \mathbb{Z}/p\mathbb{Z}$ so that $f(b) = 1$.

Then $f(b) = 1$ means that $ab = 1$, so we have found the multiplicative inverse of a that we desired.

(c) We wish to solve in $\mathbb{Z}$ the system of equations $2x + y = 2 \mod 5, 3x - 2y = 0 \mod 5$ using Gaussian elimination in $\mathbb{Z}/5\mathbb{Z}$.

We start with the system of equations:

$$\begin{aligned} 2x + y &\equiv 2 \mod 5 \\ 3x - 2y &\equiv 0 \mod 5 \end{aligned}$$

We now perform the steps of Gaussian elimination; the first equation should have a coefficient of 1 for x. The multiplicative inverse of 2 modulo 5 is 3, since $2 \cdot 3 = 6 \equiv 1 \mod 5$. After multiplying the first equation by 3, we get:

$$\begin{aligned} x + 3y &\equiv 1 \mod 5 \\ 3x - 2y &\equiv 0 \mod 5 \end{aligned}$$

Now we subtract 3 times the first equation from the second equation, noting that $3 \cdot 3 = 9 \equiv 4 \mod 5$.

$$\begin{aligned} x + 3y &\equiv 1 \mod 5 \\ -6y &\equiv -3 \mod 5 \end{aligned}$$

Note that the second equation can be simplified to $4y \equiv 2 \mod 5$. Multiplying this equation by 4, with $4 \cdot 4 = 16 \equiv 1 \mod 5$ and $4 \cdot 2 = 8 \equiv 3 \mod 5$, we end up with the system:

$$\begin{aligned} x + 3y &\equiv 1 \mod 5 \\ y &\equiv 3 \mod 5 \end{aligned}$$

We may now solve from the bottom up. The second equation tells us that $y \equiv 3 \mod 5$, and $x \equiv 1 - 3y = -8 \equiv 2 \mod 5$.

Then $y = 3 + 5s$ for some $s \in \mathbb{Z}$, and $x = 2 + 5t$ for some $t \in \mathbb{Z}$.

Therefore the solutions to these equations in $\mathbb{Z}$ are $x = 2 + 5t, y = 3 + 5s$ for some $s, t \in \mathbb{Z}$.

Exercise 7

If $a, b \in \mathbb{R}$ with $a < b$, prove:

(a) There is a rational $r \in (a, b)$.

(b) There is an irrational $c \in (a, b)$.

(c) (a, b) contains infinitely many rationals and infinitely many irrationals.

(a) We wish to show that there is a rational number in the open interval (a, b).

Given any real number $x \in \mathbb{R}$, we can define the ceiling $\lceil x \rceil$ of x as the least integer $m \in \mathbb{Z}$ with $m \geq x$.

It is clear that for any x we must have $x \leq \lceil x \rceil$.

Furthermore, if we assume for sake of contradiction that $\lceil x \rceil - x \geq 1$, then $\lceil x \rceil - 1$ is an integer which is $\geq x$ and less than $\lceil x \rceil$; this conflicts with the definition of the ceiling function. Hence for any $x \in \mathbb{R}$ we have $\lceil x \rceil - x < 1$.

Now we consider the open interval (a, b). Let $N = \lceil \frac{2}{b-a} \rceil$. In particular, N is an integer strictly greater than $\frac{2}{b-a}$. Furthermore, $N > 0$ since $a < b$ implies that $\frac{2}{b-a} > 0$.

Since $N > \frac{2}{b-a}$, we see that $Nb > Na + 2$.

Now let $M = \lceil Na \rceil$. Then $M \geq Na, M \in \mathbb{Z}$. Furthermore we showed above that $M - Na < 1$, so $M + 1 < Na + 2$.

Therefore we have $Na \leq M < M + 1 < Na + 2 < Nb$, which means $Na < M + 1 < Nb$. Dividing by N, we see that $a < \frac{M+1}{N} < b$, so $\frac{M+1}{N} \in (a, b)$.

Since $N > 0$ and $M + 1 \in \mathbb{Z}$, we see that we have found a rational number in the open interval (a, b) as desired.

(b) We wish to show that there is a irrational number in the open interval (a, b).

Let $a' = \frac{a}{\sqrt{28}}, b' = \frac{b}{\sqrt{28}}$. Then by part (a), we see that there exists a rational number $r \in (a', b')$.

Therefore $a' < r < b'$; multiplying by $\sqrt{28}$, we see that $a < r\sqrt{28} < b$.

It remains only to show that $r\sqrt{28}$ is irrational. Recalling HW 1.2, we know $\sqrt{28}$ is irrational. If we assume for sake of contradiction that $c = r\sqrt{28}$ was rational, then since r is also rational, c/r would have to be rational. However, $c/r = \sqrt{28}$, yielding a contradiction. Therefore c is irrational, with $c \in (a, b)$.

(c) We wish to show that (a, b) contains infinitely many rationals and infinitely many irrationals.

Assume for sake of contradiction (a, b) contains only finitely many rational numbers. Let the set of rational numbers in the interval (a, b) be S. Since S is finite, it contains a smallest element s. By the definition of S, $a < s < b$.

We may apply part (a) to the interval (a, s) to find some rational $r \in (a, s)$. Then $a < r < s < b$, so necessarily $r \in S$, since it is a rational number in the interval (a, b). However, we took s to be the smallest element of S, but $r < s$, yielding a contradiction. Hence (a, b) contains infinitely many rationals.

The same argument may be applied to show that (a, b) contains infinitely many irrational numbers, using instead part (b).

Exercise 8

Let a_n denote the number of nonnegative integers less than 3^n that do not have two consecutive ones when written in base 3. Equivalently, a_n is the number of sequences of $0, 1, 2$ of length n which do not have two consecutive ones. Find a recurrence equation for a_n and then solve for a_n explicitly.

We may compute $a_1 = 3$ and $a_2 = 8$ by listing sequences.

Now we consider finding a recurrence relation for a_n. Consider any sequence of length n of $0, 1, 2$ fulfilling the condition: the last digit is either a $0, 1$, or a 2.

If the last digit is 0, then the other digits must be a sequence of length $n - 1$ fulfilling the condition. Then the number of sequences of length n with last digit 0 and no consecutive 1s is a_{n-1}.

If the last digit is 1, then the other digits must be a sequence of length $n-2$ fulfilling the condition, followed by a digit which is not 1. Then the number of sequences of length n with last digit 1 and no consecutive 1s is $2a_{n-2}$.

If the last digit is 2, then the other digits must be a sequence of length $n-1$ fulfilling the condition. Then the number of sequences of length n with last digit 2 and no consecutive 1s is a_{n-1}.

Then it is clear that the total number of sequences of length n of $0, 1, 2$ with no two consecutive 1s is $a_n = 2a_{n-1} + 2a_{n-2}$.

We now have a recurrence equation: $a_1 = 3, a_2 = 8, a_n = 2a_{n-1} + 2a_{n-2}$.

As in Matousek Miniature 2, we are "inspired" to look for sequences satisfying the recurrence relation $u_n = 2u_{n-1} + 2u_{n-2}$ of the form $u_n = \tau^n$ for suitable τ. For such a sequence to exist, we must have $\tau^2 = 2\tau + 2$, or $\tau = 1 \pm \sqrt{3}$.

The vector space W of all sequences satisfying the condition $u_n = 2u_{n-1} + 2u_{n-2}$ has dimension 2, since each such sequence is determined by the choice of the first two values u_1, u_2. The two sequences we have found $u'_n = (1+\sqrt{3})^n$ and $u''_n = (1-\sqrt{3}^n$ can be checked to be linearly independent by considering the first two terms. Therefore they form a basis of W.

Our desired sequence a_n should be in W. Therefore it should be a linear combination of u'_n, u''_n.

Therefore we must find $x, y \in \mathbb{R}$ so that

$$(1+\sqrt{3})x + (1-\sqrt{3})y = a_1 = 3 \quad (1+\sqrt{3})^2 x + (1-\sqrt{3})^2 y = a_2 = 8.$$

We may solve these equations using Gaussian elimination or substitution to find $x = \frac{3+2\sqrt{3}}{6}, y = \frac{3-2\sqrt{3}}{6}$.

This gives us $a_n = \frac{3+2\sqrt{3}}{6}\left(1+\sqrt{3}\right)^n + \frac{3-2\sqrt{3}}{6}\left(1-\sqrt{3}\right)^n$ our explicit formula.

Exercise 9

How many positive integers up to 2018 are not divisible by 2, 3, 6, or 11?

For positive integers d, we let $A_d = \{n \in \mathbb{Z} : 1 \leq n \leq 2018, d \mid n\}$. We will count the size of $A_2 \cup A_3 \cup A_6 \cup A_{11}$.

In fact $A_6 = A_2 \cap A_3$, so we will count the size of $A_2 \cup A_3 \cup A_{11}$.

By the Principle of Inclusion-Exclusion,

$$|A_2 \cup A_3 \cup A_{11}| = |A_2| + |A_3| + |A_{11}| - |A_2 \cap A_3| - |A_2 \cap A_{11}| - |A_3 \cap A_{11}| + |A_2 \cap A_3 \cap A_{11}|.$$

Simplifying, we see that $A_2 \cap A_3 = A_6$, $A_2 \cap A_{11} = A_{22}$, $A_3 \cap A_{11} = A_{33}$, and $A_2 \cap A_3 \cap A_{11} = A_{66}$.

Hence what we wish to calculate is

$$|A_2 \cup A_3 \cup A_{11}| = |A_2| + |A_3| + |A_{11}| - |A_6| - |A_{22}| - |A_{33}| + |A_{66}|.$$

Now for any positive integer d, $|A_d|$ counts the number of multiples of d which are less than or equal to 2018. This is just $2018/d$ rounded down to the nearest integer. We may calculate:

$$|A_2| = 1014 \quad |A_3| = 672 \quad |A_{11}| = 183$$
$$|A_6| = 336 \quad |A_{22}| = 91 \quad |A_{33}| = 61 \quad |A_{66}| = 30$$

Therefore

$$|A_2 \cup A_3 \cup A_{11}| = 1014 + 672 + 183 - 336 - 91 - 61 + 30 = 1411.$$

This counts the number of positive integers up to 2018 which are divisible by at least one of $2, 3, 6$, and 11.

Then the number of positive integers up to 2018 which are **not** divisible by $2, 3, 6$, or 11 is $2018 - 1411 = 607$.