1. What does it mean for a set $S$ of vectors in a vector space $V$ to be a spanning set? Show that if $S \subset T$, and $S$ is a spanning set, then $T$ is also a spanning set.

A set $S$ of elements in a vector space $V$ over a field $F$ is a spanning set for $V$ if and only if, whenever $v \in V$, we can find a finite subcollection $\{s_1, \ldots, s_k\}$ of elements of $S$, and elements $\alpha_1, \ldots, \alpha_k \in F$ such that $v = \alpha_1 s_1 + \cdots + \alpha_k s_k$.

Suppose $S$ is a spanning set and $S \subset T$. We will show that $T$ is a spanning set. To show this, we must imagine we are given a vector $w \in V$ and find vectors $t_1, \ldots, t_n \in T$ and coefficients $\alpha_1, \ldots, \alpha_n \in F$ in $T$ with $w = \alpha_1 t_1 + \cdots + \alpha_n t_n$. So suppose we are given such a $w$. Since $S$ is a spanning set, we can find a finite subcollection $\{s_1, \ldots, s_k\}$ of elements of $S$, and elements $\alpha_1, \ldots, \alpha_k \in F$ such that $w = \alpha_1 s_1 + \cdots + \alpha_k s_k$. Then take $t_i = s_i$, possible since $S \subset T$.

2. Suppose $F$ is a field. A vector space is a set $V$ together with operations $\cdot$ and $+$, where $+$ takes two elements of $V$ and produces another element of $V$, while $\cdot$ takes an element of $F$ and an element of $V$ and produces an element of $V$, satisfying certain axioms. For each of the following sets $V$ and proposed functions $\cdot$ and $+$, say whether the resulting structure satisfies the axioms. If not, say why not. If it does satisfy the axioms, do not give a proof of this, but do say what the dimension of the vector space is, and give an example of a basis, with brief justification.

(a) $F = \mathbb{R}$, $V$ is all triples of real numbers $(a, b, c)$ with sum $a+b+c = 0$. $+$ is addition element-by-element, and $\cdot$ is multiplication element-by-element.

This is a vector space; a basis is $(1, 0, -1), (0, 1, -1)$.

(b) $F = \mathbb{R}$, $V$ is all triples of real numbers $(a, b, c)$ with sum $a+b+c = 1$. $+$ is addition element-by-element, and $\cdot$ is multiplication element-by-element.

This is not a vector space. $(1, 0, 0)$ and $(0, 1, 0)$ are in $V$, but their sum is $(1, 1, 0)$ which is not.

(c) $F = \mathbb{Q}$, $V$ is all polynomials $p$ with coefficients in $\mathbb{Q}$ with degree less than 6 and $p(1) = p(2) = p(3) = 0$.

$+$ is addition of polynomials, and $\cdot$ is multiplication of polynomials by constants.

This is a vector space; a basis is $(x - 1)(x - 2)², (x - 1)(x - 2)x, (x - 1)(x - 2)²x²$.

(d) $F = \mathbb{C}$, $V$ is the set of all quadruples of real numbers $(x, y, z, w)$, $+$ is addition element by element and $\cdot$ is defined by

$$(a + bi) \cdot (x, y, z, w) = (ax - by, ay + bx, az - bw, aw + bz).$$

This is a vector space. A basis is $(1, 0, 0, 0)$ and $(0, 0, 1, 0)$, so the dimension is 2. (To see this is a spanning set, one sees that $(a, b, c, d)$ is $(a + ib) \cdot (1, 0, 0, 0) + (c + id) \cdot (0, 0, 1, 0)$.)

(e) $F = \mathbb{Z}/2\mathbb{Z}$, $V$ is the set of all subsets of $\{1, 2, \ldots, 10\}$, and we define for $S, T \in V$

$$S + T = \{i \in \{1, 2, \ldots, 10\} | i \text{ in } S \text{ or } T \text{ but not both}\}$$

$$[1]_2 \cdot S = S$$

$$[0]_2 \cdot S = \emptyset$$

This is a vector space. If we introduce vectors $v_1 = \{1\}, v_2 = \{2\}, v_3 = \{3\}, \ldots, v_{10} = \{10\}$ then these 10 vectors form a basis.

3. State and prove the Steinitz exchange lemma. You may assume that if $S$ is a spanning set, and that $v \in S$ can be expressed as a linear combination of other elements of $S$, then $S \{v\}$ is a spanning set too. See the online lecture notes.

4. State the Steinitz exchange lemma. For the rest of this problem, you may assume that the lemma is true without proof. Any other assertions you use, you should prove. See the online lecture notes for stating the Steinitz exchange lemma.

(a) Show that $V$ is a vector space and $B_1$ and $B_2$ are two finite bases for $V$ then $B_1$ and $B_2$ have the same number of elements. See the online lecture notes.
5. (a) **What does it mean to say ‘let L/K be a field extension’?**

   It means ‘let L be a field and let K be a subfield of L—that is, a subset of the elements of L which is closed under addition and multiplication and contains 1.’

   (b) **Let L/K be a field extension. What do we mean when we call an element of L transcendental over K.**

   We say that \( \alpha \in L \) is algebraic over K if there is some polynomial \( p(t) \in K[T] \) such that \( p(\alpha) = 0 \). We say that \( \alpha \) is transcendental over K otherwise.

   (c) **What is meant by by saying the extension L/K is finite? In the case where L/K is finite, what is the degree of the extension?**

   Given a field extension \( L/K \), we can consider L as a vector space over K. We say that \( L/K \) is finite if L, considered as a vector space over K, is a finite dimensional vector space. In this case, the degree of the extension is the dimension of \( L \) considered as a vector space over K.

   (d) **Show that in a finite extension L/K, any element of L is algebraic.** Since \( L \) is finite over K, it must have some dimension \( [L : K] \); let \( n = [L : K] \). Let \( x \in L \). We wish to show that \( x \) is the root of some polynomial over K. Thinking of \( L \) as a field in its own right (not just a vector space) we can form the powers of \( x \) up to the \( n \)th power: \( 1, x, x^2, \ldots, x^n \). Now we’ll think of \( L \) as a vector space over K, and think of these elements of \( L \) as vectors

   \[(1), (x), (x^2), \ldots, (x^n)\]

   Since these are \( n+1 \) different vectors in an \( n \) dimensional vector space, they must be linearly dependent. Thus we can find elements \( a_0, \ldots, a_n \in K \), not all 0, such that

   \[a_0(1) + a_1(x) + a_2(x^2) + \cdots + a_n(x^n) = 0\]

   Now consider the following polynomial in \( K[T] \)

   \[p(T) = a_0 + a_1T + a_2T^2 + \cdots + a_nT^n\]

   if we plug in \( x \), we get

   \[p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\]

   which is 0 by the calculation above. So \( x \) is a root of \( p(T) \)

6. **Suppose L/K is a field extension, and \( \alpha \in L \). What is meant by a minimal polynomial of \( \alpha \)? Prove that any minimal polynomial for \( \alpha \) is irreducible, and that any irreducible polynomial \( p \) with coefficients in \( K \) such that \( p(\alpha) = 0 \) is a minimal polynomial for \( \alpha \).**

   The minimal polynomial is only defined if and \( \alpha \in L \) is algebraic. The algebraic degree of \( L/K \) is then degree of the smallest (lowest degree) nonzero polynomial \( p(T) \in K[T] \) such that \( p(\alpha) = 0 \). A minimal polynomial is some polynomial \( p(T) \in K[T] \) of that degree with \( p(\alpha) = 0 \).

   Proof that the minimal polynomial is irreducible: Suppose that \( \alpha \in L \) has minimal polynomial \( p(T) \), and \( p(T) = f(T)g(T) \) for two other polynomials, neither of which is a constant polynomial. (Remember that ‘being a constant polynomial’ is the same as ‘being a unit in \( K[T] \).’) Then \( f(\alpha)g(\alpha) = p(\alpha) = 0 \), and so either \( f(\alpha) = 0 \), or \( g(\alpha) = 0 \), since \( L \) is a field and so an integral domain. But then \( \alpha \) satisfies a polynomial (either \( f \) or \( g \)) which is of lower degree than \( p \), a contradiction.

   Proof that any irreducible polynomial \( p \) with coefficients in \( K \) such that \( p(\alpha) = 0 \) is a minimal polynomial for \( \alpha \) (we assume the fact that if \( p(X) \in K[X] \) is a polynomial with \( p(\alpha) = 0 \), then \( m(X)p(X) \)): Suppose
8. (a) What does it mean for a polynomial to be irreducible? Prove that the polynomial \(X^2 + X + 1\) over \(\mathbb{Z}/2\mathbb{Z}\) is irreducible.

A polynomial over a field \(K\) is irreducible over \(K\) if whenever we factor it as \(fg\) where \(f\) and \(g\) are also polynomials over \(K\), then one of \(f\) or \(g\) is a constant polynomial.

If the polynomial \(X^2 + X + 1\) factorized, it would have to factor as a linear times a linear. Thus, if it weren’t irreducible, it would have a linear factor, which means it would have a root. That is, we would be able to plug something in to the polynomial and get \([0]\). But there are only two possible things we could plug into the polynomial, \([0]\) and \([1]\). Plugging either of them in gives \([1]\). Thus \(X^2 + X + 1\) is irreducible.

(b) It is a fact that there is a field (which happens to be called \(\bar{\mathbb{F}}_2\)) which contains \(\mathbb{Z}/2\mathbb{Z}\) and over which the polynomial \(X^2 + X + 1\) has a root. We will call this root \(\alpha\). Let \(K = \mathbb{Z}/2\mathbb{Z}\) and let \(L = K[\alpha] \subset \bar{\mathbb{F}}_2\). As a vector space over \(K\), what is the dimension of \(L\)?
We know that the degree \( [K[\alpha] \subset \bar{\mathbb{F}}_2, K] \) will be the degree of a minimal polynomial. But \( X^2 + X + 1 \) is an irreducible polynomial which \( \alpha \) satisfies. So it is the minimal polynomial for \( \alpha \). Thus the degree of the minimal polynomial (and hence \( [K[\alpha] \subset \bar{\mathbb{F}}_2, K] \)) is 2.

(c) Using this result, and an appropriate homework problem, write down the number of elements that \( L \) must have.

\( K[\alpha] \subset \bar{\mathbb{F}}_2 \) is a vector space over \( K \), a 2-dimensional vector space. We saw in homework that a \( k \)-dimensional vector space over \( \mathbb{Z}/p \) has \( p^k \) elements. Thus a 2-dimensional vector space over \( \mathbb{Z}/2 \) has 4 elements. Thus \( K[\alpha] \subset \bar{\mathbb{F}}_2 \) has 4 elements.

(d) List all the elements of \( L \). (It may help to first write down a basis for \( L \) as a vector space over \( K \).)

We know that 1, \( \alpha \) are a basis for \( K[\alpha] \subset \bar{\mathbb{F}}_2 \) over \( K \). (See lecture 23). Thus the elements of \( L \) are \([0]_2 + [0]_2 \alpha, [1]_2 + [0]_2 \alpha, [0]_2 + [1]_2 \alpha \) and \([1]_2 + [1]_2 \alpha \) (or \([0]_2, [1]_2, \alpha \) and \([1]_2 + \alpha \)).

(e) Give explicit multiplication and addition tables for \( L \).

<table>
<thead>
<tr>
<th></th>
<th>( [0]_2 )</th>
<th>( [1]_2 )</th>
<th>( \alpha )</th>
<th>( [1]_2 + \alpha )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( [0]_2 )</td>
<td>( [0]_2 )</td>
<td>( [1]_2 )</td>
<td>( \alpha )</td>
<td>( [1]_2 + \alpha )</td>
</tr>
<tr>
<td>( [1]_2 )</td>
<td>( [1]_2 )</td>
<td>( [0]_2 )</td>
<td>( [1]_2 + \alpha )</td>
<td>( \alpha )</td>
</tr>
<tr>
<td>( [1]_2 + \alpha )</td>
<td>( [1]_2 + \alpha )</td>
<td>( [0]_2 )</td>
<td>( [1]_2 )</td>
<td>( \alpha )</td>
</tr>
</tbody>
</table>

(To see that the multiplication table is correct, first fill in the first two rows and the first two columns, which are easy. Then see that \( \alpha \times \alpha = \alpha^2 = -\alpha - [1]_2 \), where we use the fact that \( \alpha \) is a root of \( X^2 + X + 1 \). Then we see that \( -\alpha - [1]_2 = \alpha + [1]_2 \) since \( [-1]_2 = [1]_2 \). The remainder can be filled in using ‘sudoku’.)

9. The real number \( \beta \) satisfies the polynomial \( (x^2 + 7x + 1)(3x^3 + 5x - 9) \). Give two different polynomials such that one of them must be a minimal polynomial for \( \beta \). What are the possible values for \( [\mathbb{Q}(\beta) \subset \mathbb{R} : \mathbb{Q}] \)?

We know that the minimal polynomial a) is irreducible and b) goes into \( (x^2 + 7x + 1)(3x^3 + 5x - 9) \). So the possibilities for the minimal polynomial are narrowed down to the list of irreducible factors of \( (x^2 + 7x + 1)(3x^3 + 5x - 9) \). It is natural to hope that \( (x^2 + 7x + 1) \) and \( (3x^3 + 5x - 9) \) are both irreducible, since then the list of irreducible factors of \( (x^2 + 7x + 1)(3x^3 + 5x - 9) \) would be \( (x^2 + 7x + 1) \) and \( (3x^3 + 5x - 9) \), and that would give us a list of two possibilities for the minimal polynomial of \( \beta \), as the question seeks. So we try to prove that \( (x^2 + 7x + 1) \) and \( (3x^3 + 5x - 9) \) are irreducible. Since they’re quadratic and cubic, if either factorized it would have at least one linear factor, and hence, at least one root. But by the rational roots test, the only possible roots of \( (x^2 + 7x + 1) \) are 1 and \( -1 \), and (plugging in) neither actually is a root. Similarly, the only possible roots of \( (3x^3 + 5x - 9) \) are \( 1/3, 1, 3, 9, -1/3, -1, -3, -9 \), and none of these is a root. Thus they are both irreducible, and we know the minimal polynomial for \( \beta \) is either \( (x^2 + 7x + 1) \) or \( (3x^3 + 5x - 9) \).

The possible values for \( [\mathbb{Q}(\beta) \subset \mathbb{R} : \mathbb{Q}] \) are the degrees of these two possible minimal polynomials: 2 or 3.

10. (a) Calculate the degree of the extension \( [\mathbb{Q}(\sqrt{5}) \subset \mathbb{R}, \mathbb{Q}] \). Give an explicit basis for \( \mathbb{Q}(\sqrt{5}) \subset \mathbb{R} \) as a vector space over \( \mathbb{Q} \).

The minimal polynomial of \( \sqrt{5} \) is \( X^2 - 5 \). Thus \( [\mathbb{Q}(\sqrt{5}) \subset \mathbb{R}, \mathbb{Q}] = 2 \). An explicit basis is easily seen to be \( 1, \sqrt{5} \).

(b) Show that it is impossible to find \( a, b \in \mathbb{Q} \) with \((a + \sqrt{5}b)^2 = 7\).

If we could, then we would have \((a^2 + 5b^2 - 7) + 2ab\sqrt{5} = 0\). That is, we would have \((a^2 + 5b^2 - 7)(1/\mathbb{Q}) + 2ab(\sqrt{5})/\mathbb{Q} = (0)/\mathbb{Q}\).

Since \( 1, \sqrt{5} \) form a basis for \( \mathbb{Q}(\sqrt{5}) \subset \mathbb{R} \) over \( \mathbb{Q} \), they are linearly independent, and we must have \( a^2 + 5b^2 - 7 = 0 \) and \( 2ab = 0 \). Using the second of these, either \( a = 0 \) or \( b = 0 \).
11. Euclid was, of course, the most famous mathematics textbook author of all time. Not so many people have heard of Euclid (pronounced New-clid), a crackpot. He proposed that as well as the five standard constructions of Euclidean geometry, a sixth construction be allowed:

- given two line segments \( AB \) and \( AC \), it is given to construct a circle \( \Gamma \) center \( A \) with radius \( \sqrt{AC \cdot AC - AB} \).

In this problem we will consider how one might show that in euclidean geometry it is not possible, given a line segment of length 1, to construct a line segment of length \( \sqrt{2} \). There are two parts, and you may choose to do either one or the other.

(a) Prove that if \( AB \) and \( AC \) were defined over a field \( K \), then \( \Gamma \) would be defined over a field \( K' \) with \( [K' : K] = 1, 2 \) or 3. Explain how to modify the proof of Prop 9 in the notes to prove the following fact about neucldidean geometry.

- Suppose \( P_1, \ldots, P_k, \Gamma_1, \ldots, \Gamma_l, s_1, \ldots, s_m, \ell_1, \ldots, \ell_n \) are a collection of points, circles, segments and lines, all defined over a field \( K \). Suppose that we apply a series of Euclidean constructions to these objects, eventually constructing some further object \( X \). (\( X \) might be a point, a circle, a segment or a line.) Then we can find a field \( K^* \) with \( [K^* : K] = 2^a 3^b \) for some integers \( a, b \), such that \( X \) is defined over \( K^* \).

Let us suppose that \( AB \) and \( AC \) are defined over \( K \), so that \( AC^2 \cdot AC^2 \cdot AB^2 \) (which we will call \( t \)) is also defined over \( K \). (Here \( AC^2 \) refers to the length squared of \( AC \), which is defined over \( K \) by using the length formula.) We write \( \alpha \) for \( \sqrt{t} \). Since \( \alpha \) satisfies \( X^3 - t \), the minimal polynomial of \( \alpha \) goes into \( X^3 - t \) and has degree 1,2 or 3. Thus \( [K[\alpha] : K] \) is 1, 2 or 3.

Then we see that the coordinates of \( A \) (\( x_A \) and \( y_A \) say) are in \( K \), since \( A \) is defined over \( K \), and that the circle \( \Gamma \) has equation \( (x - x_A)^2 + (y - y_A)^2 = \alpha \). All the coefficients lie in \( K[\alpha] \), and so \( \Gamma \) is defined over \( K[\alpha] \). But we saw this field had degree 1,2 or 3 over \( K \), so we may take \( K' \) to be \( K[\alpha] \).

Here is the proof of the modified version of Prop 9:

We write \( K_0 = K \), and imagine writing down the construction line by line. In each line, we construct a new point, line or circle. We will construct a sequence of fields \( K_1, K_2, \ldots \) with the following properties:

- Each \( K_i \) is an extension of the last: \( K_0 \subset K_1 \subset K_2 \subset \ldots \).
- For each \( i \geq 1 \), \( [K_i : K_{i-1}] = 1 \) or 2 or 3.
- All the points, circles, segments and lines introduced up to the \( i \)th line of the proof are defined over \( K_i \).

We do this one step at a time. At each step, we look at the new object constructed in the \( i \)th line, and see how it was constructed. If we used point+point→segment, we take \( K_i = K_{i-1} \). Since the input points were defined over \( K_{i-1} \), so the resulting segment will be defined over \( K_{i-1} \). A similar argument works for segment→line, line+line→point or line+segment→circle. If we used circle+circle→point or...
line + circle → point, then our Lemmas above let us construct a field $K'$ with $[K' : K_{i-1}] = 1$ or $2$ and the new point defined over $K'$. So we take $K_1 = K'$. Finally if we used the additional construction allowed by euclid’s rule, the earlier part of this problem let us construct a field $K'$ with $[K' : K_{i-1}] = 1$ or $2$ or $3$. So we take $K_1 = K'$.

At the final step of the proof (number $n$), say, we see that the final thing constructed is defined over $K_n$, and that

$$[K_n : K] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \ldots [K_1 : K_0]$$

which is a power of 2 times a power of 3, since each factor on the RHS is either 3 or 2 or 1. Thus we take $K^* = K_n$ and we are done.

(b) Use the fact in the bullet point above to prove that in euclidean geometry it is not possible, given a line segment of length 1, to construct a line segment of length $\sqrt{2}$. You may assume that the polynomial $X^5 - 2$ is irreducible over $\mathbb{Q}$.

Suppose for contradiction that it were possible. Let’s call our original line segment of length 1 $AB$, and take our coordinate system so that $A$ is the origin, and $B$ is the point $(1, 0)$. If we could construct (anywhere in the plane) a segment $CD$ of length $\sqrt{2}$, then we could construct the point $(\sqrt{2}, 0)$ (by intersecting the circle, center $A$ radius $CD$ with the line $AB$ produced. Thus it suffices to imagine we have started with just $AB$ and constructed $(\sqrt{2}, 0)$ and deduce a contradiction. So let us imagine this.

By the bullet point, since $AB$ is defined over $\mathbb{Q}$, it follows that there is some subfield $K'$ of $\mathbb{R}$ containing $\mathbb{Q}$, with $(\sqrt{2}, 0)$ defined over $\mathbb{Q}$ and $[K' : \mathbb{Q}]$ of the form $2^a3^b$. We then have a tower of fields $K'/\mathbb{Q}[\sqrt{2}]_{\subset \mathbb{R}}/\mathbb{Q}$, so

$$[K' : \mathbb{Q}] = [K' : \mathbb{Q}[\sqrt{2}]_{\subset \mathbb{R}}][\mathbb{Q}[\sqrt{2}]_{\subset \mathbb{R}} : \mathbb{Q}]$$

and so $[\mathbb{Q}[\sqrt{2}]_{\subset \mathbb{R}} : \mathbb{Q}]$ is also of the form $2^a3^b$.

But on the other hand, we are told that the the polynomial $X^5 - 2$ is irreducible over $\mathbb{Q}$, so since $\sqrt{2}$ clearly satisfies this polynomial, it must be the minimal polynomial of $\sqrt{2}$. Thus $[\mathbb{Q}[\sqrt{2}]_{\subset \mathbb{R}} : \mathbb{Q}] = \deg X^5 - 2 = 5$. This is not of the form $2^a3^b$. Contradiction.