Some important ideas:

1. If you have a set that includes the rational numbers, and is a subset of the complex numbers then to prove it is a field you only have to prove that it is closed under multiplication and addition and that it has multiplicative and additive inverses.

Things to think about:

- Why don't you have to prove that the set includes identities?

Because 0 and 1 are elements of $\mathbb{Q}$ and $\mathbb{Q} \subseteq F$

- Why don't you have to prove addition and multiplication are associative and commutative?

Because addition and multiplication are associative and commutative for all complex numbers and $F \subseteq \mathbb{C}$

- What is the difference between being associative and being commutative?

This isn't a trick question: if you can write down the commutative properties and write down the associative properties then you know everything I want you to know. Look them up if you think you might be getting them confused.

2. If you have a field that includes another field (especially in the cases of fields F and G such that $\mathbb{Q} \subseteq F \subseteq G \subseteq \mathbb{C}$) then the larger field can be treated as a vector space where the scalars are the elements of the smaller field (we say G is a vector field over F). Sometimes these vector fields have a finite dimension and sometimes they have an infinite dimension. We have been focusing on vector fields that have a finite dimension. We write the dimension of the vector field [G:F].

3. Given a field (usually $\mathbb{Q}$, but I'm going to call it F in this description), and there is a number (α) that is not in F, but it is a solution of a polynomial with coefficients in F, then there is a vector field over F that has a finite number of basis vectors (one of which is α) that is also a field.

Things to think about:

- Is $\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ a vector field? Is it a field? What is its dimension over $\mathbb{Q}$?

Yes, it is a vector field, yes it is a field, and it is dimension 2 as a vector field (basis $\{1,\sqrt{2}\}$)

- Is $\{a+b\sqrt[3]{2} \mid a,b \in \mathbb{Q}\}$ a vector field? Is it a field? What is its dimension over $\mathbb{Q}$?

Yes it is a vector field, no it is not a field because $\sqrt[3]{2}\cdot\sqrt[3]{2}=\sqrt[3]{2}^2$ is not in the set. It is a 2 dimensional vector field (basis $\{1,\sqrt[3]{2}\}$

- Is $\{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2 \mid a,b,c \in \mathbb{Q}\}$ a vector field? Is it a field? What is its dimension over $\mathbb{Q}$?

Yes, it is a vector field, yes it is a field. It is dimension 3 (basis $\{1,\sqrt[3]{2},\sqrt[3]{2}^2\}$)

- Is $\{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2+d\sqrt[3]{2}^3 \mid a,b,c,d \in \mathbb{Q}\}$ a vector field? Is it a field? What is its dimension over $\mathbb{Q}$?
- Yes, it is a vector field, yes it is a field. It is dimension 3 (basis $\{1,\sqrt[3]{2},\sqrt[3]{2}^2\}$ or $\{\sqrt[3]{2},\sqrt[3]{2}^2,\sqrt[3]{2}^3\}$)

Things to be able to do:

- Prove that $\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ is a field

You all did practically perfect on this homework assignment, I'm not writing this up.

- Prove that $\{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2 \mid a,b,c \in \mathbb{Q}\}$ is a field : See last page.
- Write $\mathbb{Q}(\alpha)$ as a vector field given that α is the root of an irreducible polynomial $x^5+3x^4+6x^2-9x+12$

$\mathbb{Q}(\alpha)=\{a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4\}$

- Given that α is the root of the irreducible polynomial x^4+5x^3-10 prove that $\{a+b\,\alpha+c\,\alpha^2+d\,\alpha^3 \mid a,b,c,d \in \mathbb{Q}\}$ is closed under addition

Let $\{a+b\alpha+c\alpha^2+d\alpha^3 \mid a,b,c,d\in\mathbb{Q}\}=S$, and let $a+b\alpha+c\alpha^2+d\alpha^3,\ e+f\alpha+g\alpha^2+h\alpha^3\in S$
Then $(a+b\alpha+c\alpha^2+d\alpha^3)+(e+f\alpha+g\alpha^2+h\alpha^3)=(a+e)+(b+f)\alpha+(c+g)\alpha^2+(d+h)\alpha^3\in S$

- Given that α is the root of the irreducible polynomial x^4+5x^3-10 show that $3\alpha^6+2\alpha^5-\alpha^4+5\alpha^3\in\{a+b\alpha+c\alpha^2+d\alpha^3 \mid a,b,c,d\in\mathbb{Q}\}$

Because α is the root of x^4+5x^3-10, we know that $\alpha^4+5\alpha^3-10=0$, so $\alpha^4=-5\alpha^3+10$
So we can substitute in to get:

$$3\alpha^6+2\alpha^5-\alpha^4+5\alpha^3=3\alpha^2(-5\alpha^3+10)+2\alpha^5-\alpha^4+5\alpha^3=-13\alpha^5-\alpha^4+5\alpha^3+30\alpha^2$$

$$=-13\alpha(-5\alpha^3+10)-\alpha^4+5\alpha^3+30\alpha^2=64\alpha^4+5\alpha^3+30\alpha^2-130\alpha$$

$$=64(-5\alpha^3+10)+5\alpha^3+30\alpha^2-130\alpha=-315\alpha^3+30\alpha^2-130\alpha+640\in S$$

*note to self: try to find an example with smaller numbers next time.

- Given that α is the root of the irreducible polynomial x^4+5x^3-10 explain how to show that $\dfrac{1}{\alpha^2+3\alpha+2}$ is equal to a number in the set: $\{a+b\alpha+c\alpha^2+d\alpha^3 \mid a,b,c,d\in\mathbb{Q}\}$

It is possible to use Euclid's algorithm on the polynomials: x^4+5x^3-10 and x^2+3x+2 to find polynomials $f(x)$ and $g(x)$ with rational coefficients such that:
$\text{gcd}=(x^4+5x^3-10)\cdot f(x)+(x^2+3x+2)\cdot g(x)$
Because x^4+5x^3-10 is irreducible, the gcd of the polynomials must be a non-zero rational number, which I will call *n*.
Substituting in $x=\alpha$, the equation becomes:
$n=(\alpha^4+5\alpha^3-10)\cdot f(\alpha)+(\alpha^2+3\alpha+2)\cdot g(\alpha)$
Because α is the root of the x^4+5x^3-10, we know $\alpha^4+5\alpha^3-10=0$, so we can simplify to get:
$n=(\alpha^2+3\alpha+2)\cdot g(\alpha)$
Solving for $\dfrac{1}{\alpha^2+3\alpha+2}$ we get $\dfrac{1}{\alpha^2+3\alpha+2}=\dfrac{g(\alpha)}{n}$
If $g(\alpha)$ contains terms with powers of α that are greater than 3, then we can substitute: $\alpha^4=-5\alpha^3+10$ to simplify the form to get a polynomial with α substituted in where the highest power of α is α^3
Hence $\dfrac{1}{\alpha^2+3\alpha+2}=\dfrac{g(\alpha)}{n}\in S$

4. If you have polynomials with coefficients in the same field (think $\mathbb{Q}$), then you can add, subtract and multiply those polynomials, and you can do division with remainders. The coefficients always stay in the same field when you do that.

5. If you have two polynomials (p(x) and q(x)) with coefficients in the same field then you can use Euclid's algorithm to find the gcd of the two polynomials, and write an equation:
gcd = p(x)*f(x) +q(x)*g(x) where f(x) and g(x) are also polynomials with coefficients in the same field.
Things to think about:

- If p has degree n and it is irreducible, and q has degree m and m<n, is it possible for the gcd to have a degree greater than 0? Why not?

It is not possible because the gcd must evenly divide into p(x). If the gcd were a polynomial (and not just a constant) then we could divide p(x) by the gcd to get a factorization p(x)=gcd(x) quotient(x), and that contradicts the given that p is irreducible.

- If p is irreducible and α is a zero of p, can α be a zero of a polynomial that has a smaller degree than p? Why not?

No: if α is a zero of p(x) (which is irreducible) and q(x) (which has a degree smaller than p), then this would contradict the property that p is irreducible and hence gcd(p,q) must be a non-zero constant (which I will call n). You can prove this makes a contradiction by thinking about the result of doing the (extended) Euclidean algorithm to get: n = p(x)*f(x) +q(x)*g(x)
When you plug in α, you get n=0+0 (which is a contradiction).

- If p is irreducible over field F, and α is a zero of p, you can write the multiplicative inverse of 3+2 α as a polynomial in α (this means there is a polynomial q(x) where q(α) is the multiplicative inverse of 3+2 α). How does Euclid's algorithm make that possible?

You use the extended Euclidean algorithm on the polynomials p(x) and 3+2x. You will get a gcd=n a non-zero rational number because p is irreducible, and you will get polynomials f(x) and g(x) such that
n = p(x)*f(x) +(3+2x)g(x)
Plugging in α, you get n = p(α)*f(α) +(3+2 α)g(α) which simplifies to n = (3+2 α)g(α), and you can do a little algebra to get that g(α)/n is the multiplicative inverse.

Things to be able to do:

- Use Euclid's algorithm to find the gcd of two not-too-large polynomial as a "linear" combination of the polynomials. For example, for $p(x)=4x^3+8x+3$ and $q(x)=x^2-3x+2$, find polynomials *f* and *g* such that gcd(p,q) = p(x)*f(x) +q(x)*g(x)

$$4x^3+8x+3=(x^2-3x+2)(4x+12)+(36x-21)$$

$$x^2-3x+2=(36x-21)(\frac{1}{36}x-\frac{29}{432})+(\frac{85}{144})$$

$$(36x-21)=(\frac{85}{144})(\frac{5184}{85}x-\frac{3024}{85})+0$$

so then

$$4x^3+8x+3-(x^2-3x+2)(4x+12)=(36x-21)$$

$$x^2-3x+2-(36x-21)(\frac{1}{36}x-\frac{29}{432})=(\frac{85}{144})$$

And substituting, we get

$$(x^2-3x+2)-((4x^3+8x+3)-(x^2-3x+2)(4x+12))(\frac{1}{36}x-\frac{29}{432})=(\frac{85}{144})$$

So :

$$(\frac{85}{144})=(x^2-3x+2)\left(1+(4x+12)(\frac{1}{36}x-\frac{29}{432})\right)-(4x^3+8x+3)(\frac{1}{36}x-\frac{29}{432})$$

$$=(x^2-3x+2)\left(\frac{1}{9}x^2+\frac{7}{108}x+\frac{7}{36}\right)-(4x^3+8x+3)(\frac{1}{36}x-\frac{29}{432})$$

**note to self: double check for nice numbers on problems like this too).

6. Given a field (usually $\mathbb{Q}$, but I'm going to call it F in this description), and there is a number (α) that is not in F, but it is a solution of an irreducible polynomial of degree *n* with coefficients in F, then the basis of $F(\alpha)$ as a vector field with scalars in F is $\{1,\alpha,\alpha^2,...,\alpha^{n-1}\}$

Things to think about:

- Why don't we need any more basis vectors (why is this set enough)?

If there are powers of n or higher (for instance after multiplying), we can solve for α^n in $P(\alpha)=0$ and use that to simplify any polynomial with α plugged in until there are only powers <n. We can also use Euclid's algorithm to find multiplicative inverses that are polynomials in α.

- Why do we need all of these basis vectors (why can't we get rid of any)?

If the set of vectors were linearly dependent, that would mean there was another polynomial (with degree less than n) where α was a solution, but that's impossible (see #5)

Things to be able to do:

- Write a basis for a vector field for $\mathbb{Q}(\alpha)$ with scalars in $\mathbb{Q}$, where α is a root of the irreducible polynomial x^4+5x^3-10

The basis is $\{1,\alpha,\alpha^2,\alpha^3\}$

- Tell the dimension $[\mathbb{Q}(\alpha):\mathbb{Q}]$ where α is a root of the irreducible polynomial x^4+5x^3-10

Dimension 4

7. Understand the vector field representations of $\mathbb{Q}(\alpha,\beta)$, and the vector field dimension equation: If $\mathbb{Q}\subseteq F\subseteq G\subseteq H\subseteq\mathbb{C}$ and F, G, H are fields then $[H:F]=[H:G][G:F]$.

Things to be able to do:

- Write $\mathbb{Q}(\sqrt{5})$ as a vector field over $\mathbb{Q}$ and write $F(\sqrt{3})$ as a vector field over $F=\mathbb{Q}(\sqrt{5})$. Show how to get the basis for $\mathbb{Q}(\sqrt{5},\sqrt{3})$ as a vector field over from the previous representations.

$\mathbb{Q}(\sqrt{5})=\{a+b\sqrt{5}\mid a,b\in\mathbb{Q}\}$; $F(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in F\}$

$\mathbb{Q}(\sqrt{5},\sqrt{3})=\{(a+b\sqrt{5})+(c+d\sqrt{5})\sqrt{3}\mid a,b,c,d\in\mathbb{Q}\}=\{a+b\sqrt{5}+c\sqrt{3}+d\sqrt{5}\sqrt{3}\mid a,b,c,d\in\mathbb{Q}\}$

The basis vectors of $\mathbb{Q}(\sqrt{5},\sqrt{3})$ are products of the basis vectors of $\mathbb{Q}(\sqrt{5})$ and $F(\sqrt{3})$.

- Given that c is a constructible number, explain why $[\mathbb{Q}(c):\mathbb{Q}]$ is a power of 2.

To construct a number using a compass and straight edge, you are doing a series of steps that involve intersecting circles with lines or other circles, and the numbers you get out of those constructions all come from solving quadratic equations, so every time you do a single construction step (getting a single new length), you're expanding your field of numbers with a square root type number, that gives you a vector field dimension of 2 over whatever number field you had before.

Numerically, you are starting with the rational numbers and extending it by one square root (or other root of a quadratic) at a time. For example, if your construction extended the number field 4 times by the quadratic solutions: a, b, c, d, then you can find the total dimension by looking at what happens at each step: $[\mathbb{Q}(a,b,c,d):\mathbb{Q}]=[\mathbb{Q}(a,b,c,d):\mathbb{Q}(a,b,c)][\mathbb{Q}(a,b,c):\mathbb{Q}(a,b)][\mathbb{Q}(a,b):\mathbb{Q}(a)][\mathbb{Q}(a):\mathbb{Q}]$

Each of those individual steps (that corresponds to just one intersection) gives you a vector space dimension of 2 or 1 (dimension 2 if you are solving a quadratic that doesn't factor using the numbers you already have; dimension 1 if you are solving a linear equation or a quadratic that does already factor).

When you multiply them all together, you are always multiplying factors of 1 or 2, and the total product (which is the total dimension) is a power of 2.

- Explain why $\cos(20°)$ is not constructible.

$[\mathbb{Q}(\cos 20°):\mathbb{Q}]=3$ because $\cos(20°)$ is a root of the irreducible degree 3 polynomial $8x^3-6x-1$.

The set of numbers you can get out of doing finitely many construction steps always has dimension 2^n, but if those construction steps resulted in $\cos(20°)$, then the dimension of that set of numbers would have to be a multiple of 3 because $[\mathbb{Q}(\cos 20°):\mathbb{Q}]=3$. Because 2^n is never divisible by 3, $\cos(20°)$ is not constructible.

- Explain why $\sqrt[3]{5}$ is not constructible.

$[\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}]=3$ because $\sqrt[3]{5}$ is a root of the irreducible degree polynomial x^3-5

If you do finitely many constructions, you get a field of numbers (F) that has dimension $[F:\mathbb{Q}]=2^n$ as a vector field over $\mathbb{Q}$. If that field (F) included $\sqrt[3]{5}$, it would have to include $\mathbb{Q}(\sqrt[3]{5})$, and so you would be able to write its dimension as a product: $[F:\mathbb{Q}]=[F:\mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}):\mathbb{Q}]=[F:\mathbb{Q}(\sqrt[3]{5})]\cdot 3$, so 3 would be a divisor of 2^n. Because 2^n is never divisible by 3, $\sqrt[3]{5}$ is not constructible.

Prove that $S = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mid a,b,c \in \mathbb{Q}\}$ is a field

Additive closure:

Let $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2,\ d+e\sqrt[3]{2}+f\sqrt[3]{2}^2 \in S$

Then $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2 +\ d+e\sqrt[3]{2}+f\sqrt[3]{2}^2 = (a+d)+(b+e)\sqrt[3]{2}+(c+f)\sqrt[3]{2}^2 \in S$

Additive inverse:

$a+b\sqrt[3]{2}+c\sqrt[3]{2}^2 \in S$

Then $-(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2) = (-a)+(-b)\sqrt[3]{2}+(-c)\sqrt[3]{2}^2 \in S$

Multiplicative closure:

Let $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2,\ d+e\sqrt[3]{2}+f\sqrt[3]{2}^2 \in S$

Then when we expand out and simplify the product $(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2)(\ d+e\sqrt[3]{2}+f\sqrt[3]{2}^2)$ we will get a polynomial form with $\sqrt[3]{2}$ in the place of the variable, and where the highest power of $\sqrt[3]{2}$ will be a fourth power, so:

$(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2)(\ d+e\sqrt[3]{2}+f\sqrt[3]{2}^2) = A+B\sqrt[3]{2}+C\sqrt[3]{2}^2+D\sqrt[3]{2}^3+E\sqrt[3]{2}^4$ where $A,B,C,D,E \in \mathbb{Q}$

Now, $\sqrt[3]{2}^3 = 2$ so we can substitute and simplify to get:

$A+B\sqrt[3]{2}+C\sqrt[3]{2}^2+D\cdot 2+E\cdot 2\sqrt[3]{2} = (A+2D)+(B+2E)\sqrt[3]{2}+C\sqrt[3]{2}^2 \in S$

Multiplicative inverses:

Let $c+b\sqrt[3]{2}+a\sqrt[3]{2}^2 \in S$

If we use the extended Euclidean algorithm on the polynomials $p(x) = x^3-2$ and $q(x) = ax^2+bx+c$ where $q(x) \neq 0$, then we will find that the greatest common divisor is a constant $n \neq 0$ because $p(x)$ is irreducible. We will also get polynomials $f(x), g(x) \in \mathbb{Q}[x]$ such that

$n = f(x)p(x)+g(x)q(x)$

Substituting in $\sqrt[3]{2}$ and simplifying we get:

$n = f(\sqrt[3]{2})p(\sqrt[3]{2})+g(\sqrt[3]{2})q(\sqrt[3]{2})$

$n = f(\sqrt[3]{2})(\sqrt[3]{2}^3-2)+g(\sqrt[3]{2})(a\sqrt[3]{2}^2+b\sqrt[3]{2}+c)$

$n = 0+g(\sqrt[3]{2})(a\sqrt[3]{2}^2+b\sqrt[3]{2}+c)$

$$\frac{1}{(a\sqrt[3]{2}^2+b\sqrt[3]{2}+c)} = \frac{g(\sqrt[3]{2})}{n}$$

So we get that $\frac{g(\sqrt[3]{2})}{n}$ is the multiplicative inverse of $c+b\sqrt[3]{2}+a\sqrt[3]{2}^2$

$\frac{g(\sqrt[3]{2})}{n}$ is a polynomial with $\sqrt[3]{2}$ in the place of the variable with rational coefficients.

If there are powers of $\sqrt[3]{2}$ that are higher than 2, we can simplify $\frac{g(\sqrt[3]{2})}{n}$ by substituting $\sqrt[3]{2}^3 = 2$ until it is in a form with only $\sqrt[3]{2}$ and $\sqrt[3]{2}^2$, so that $\frac{g(\sqrt[3]{2})}{n} \in S$