Trisection section assignments

A. Your goal is to find a degree 3 polynomial with coefficients in Z, one of whose solutions is $\cos(\pi/9)$. The following steps will probably be relevant:

1. Notice that $\pi/3 = 3\cdot(\pi/9)$. Notice that $\cos(\pi/3)$ is a nice number.
2. Use trigonometry to write $\cos(\pi/3)$ as polynomial of $\cos(\pi/9)$. You may find it less confusing to do this with $\cos(3\theta)$ as a polynomial function of $\cos(\theta)$.
3. Change $\cos(\pi/9)$ to x and $\cos(\pi/3)$ to a fraction, and turn it into a polynomial with integer coefficients.
4. Remark to yourself, that $\cos(\pi/3)$ must therefore be an algebraic number, and then go look up algebraic number to make sure you remembered it correctly. If you did, feel smug.

B. Take the polynomial you found in part A. Prove that it is irreducible over Q. Recall that irreducible is not the same thing as saying that it can't be completely factored: x^4-4 has no roots in Q, so it can't be completely factored with coefficients in Q, but $x^4-4=(x^2-2)(x^2+2)$, so it is not irreducible. You might want to look up various theorems about factorization and roots (especially rational roots, since you are only interested in factors over Q). If all else fails, you can look up Eisenstein's criterion, but then we'd have learn about it, so why don't you try some other things first. Double check your proof/argument to make sure you haven't left any big holes.

D. Extension fields
1. All of our fields are going to be sub-fields of C (complex numbers). Suppose you have a set S that is a subset of C. Look up the definition of a field, and write down in two columns: the conditions you will have to check to make sure S is a field, and the conditions you can skip checking because it is a subset of C.

2. We all know that $\mathbb{Q}$ is a field. The extension field $\mathbb{Q}(i)$ is the smallest set that contains $\mathbb{Q}$ and i and is a field. $\mathbb{Q}$ and i are both in $\mathbb{C}$, so obviously this will be a subset of $\mathbb{C}$. What does it look like? What do its elements look like? Write down your description and prove that your description is a field (and therefore describes all of $\mathbb{Q}(i)$)

3. Write down your best description of $\mathbb{Q}(\sqrt{2})$, and prove that it is a field.
What is the inverse of a typical element?

4. Write down your best description of $\mathbb{Q}(\sqrt{3})$. Don't bother to prove it's a field because it would be redoing your work from 2 and 3. Feel free to write a snobby sentence including the word "similarly" to explain why you're not bothering to prove it is a field.
What is the inverse of a typical element?

5. Write down your best description of $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})$. Prove that your description includes everything in the field.
Finding inverses is super messy here. Can you find a way to convince us that every element has an inverse without writing down a simplified form of the inverse?

6. Consider the field $Q(\sqrt{2}+\sqrt{3})$. Is it a subfield of the field in #5? Is it the same field as the field in #5? How do you know? This one is best done, I think, by a lot of playing around with the number

$\sqrt{2}+\sqrt{3}$: squaring it, cubing it, multiplying/adding/subtracting it with various rational numbers, finding its (multiplicative) inverse. Just do a lot of recreational arithmetic and you should be able to come up with something good.

E. Euclid's algorithm. You should look up Euclid's algorithm (perhaps in your abstract algebra book). You should practice on some numbers first, then try it with some polynomials, and finally do the same with square root and cube root things. Do not try to cut corners by doing #1 and 2 without Euclid's algorithm, because then you will be left with a mess you don't know how to handle in problems 3-5.

1. Use Euclid's algorithm on the numbers 16 and 42 to get $2 = a \cdot 16 + b \cdot 42$

2. Use Euclid's algorithm on the numbers 55 and 42 to get $1 = a \cdot 55 + b \cdot 42$

3. Use Euclid's algorithm on the polynomials $x^2 - 1$ and $x^3 - 1$ to get $x - 1 = a \cdot (x^2 - 1) + b \cdot (x^3 - 1)$. Note that *a* and *b* will be polynomials.

4. Use Euclid's algorithm on the polynomials $x^2 - 2$ and $3x + 1$ to get $1 = a \cdot (x^2 - 2) + b \cdot (3x + 1)$

5. Use Euclid's algorithm on the polynomials $x^3 - 5$ and $x^2 + 2x$ to get $1 = a \cdot (x^3 - 5) + b \cdot (x^2 + 2x)$

6. Take *b* from #4 and plug in $x = \sqrt{2}$. Multiply that number by $3\sqrt{2} + 1$. You should get 1. Cool, huh?

7. Take *b* from #5 and plug in $x = \sqrt[3]{5}$. Multiply that number by $\sqrt[3]{5}^2 + 2\sqrt[3]{5}$. What do you get?

8. Look back at # 4-7. Where did $x = \sqrt{2}$ come from? Where did $x = \sqrt[3]{5}$ come from? Why do you get 1 in both cases (because the polynomials are ____).

9. Read a proof of Euclid's algorthm for integers. Rewrite it to be a theorem and proof of Euclid's algorithm for polynomials over a field. Be prepared to present/discuss your proof.

10. If you had the root $\sqrt[5]{2}$ of the polynomial $x^5 - 2$ that is irreducible over Q, and you wanted to know a multiplicative inverse of $\sqrt[5]{2}^3 + 4 \cdot \sqrt[5]{2}$, what would you do? You don't have to do the calculations on this one, just explain the process; your explanation of the process, however, should have a fair amount of detail--almost like a proof--and it should use your result from #9.

K. Read the definition of a vector space (perhaps in your linear algebra book).

1. The field Q is a subfield of the field R. Verify that R is a vector space over Q.

2. The field R is a subfield of the field C. Verify that C is a vector space over R.

3. Would $\{\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \ldots\}$ be a basis of R as a vector space of Q? Explain why or why not?

4. How many basis vectors would you need to span R as a vector space of Q? What is the dimension $[R:Q]$?

5. How many basis vectors would you need to span C as a vector space of R? What is the dimension $[C:R]$?

6. Give a basis for $Q(\sqrt{2})$ as a vector space over Q. What is the dimension $[Q(\sqrt{2}):Q]$?

K 7. Give a basis for $Q(\sqrt{2})(\sqrt{3})$ as a vector space over $Q(\sqrt{2})$. What is the dimension $[Q(\sqrt{2})(\sqrt{3}):Q(\sqrt{2})]$?

8. Give a basis for $Q(\sqrt{2})(\sqrt{3})$ as a vector space over Q. What is the dimension $[Q(\sqrt{2})(\sqrt{3}):Q]$?

9. Look back at D 2 and 3 and notice that your descriptions of *Q(i)* and $Q(\sqrt{2})$ are almost identical. Use this obvious similarity to write down a function $\phi : Q(i) \to Q(\sqrt{2})$. Look up the definition of a vector field isomorphism, and prove that your function is an isomorphism.
This is not a field isomorphism, only a vector field isomorphism.

10. Realize that this means that these sets (from #9) are the same as vector spaces. This is really weird, because if you think of them graphically in the complex plane, they don't look anything alike. Write down the inverse function $\phi^{-1} : Q(\sqrt{2}) \to Q(i)$ and try to get your brain to wrap around the idea that these two vector fields are the same.

M. Compass and straightedge constructions. I hope everyone knows a few of these. If you don't, ask your neighbor, google it, or check out a geometry book from the library.

1. Explain, in a very laborious, step-by-step way, with pictures, how, given a line *l* and a point *P*, to construct a line perpendicular to *l*, passing through point *P*. Identify every time you are creating a line, a circle, or finding an intersection.

2. Do the same thing as 1 for bisecting a given angle.

N. Do M #2 to find the angle bisector of the positive x-axis, and the positive y-axis, but do it with equations. Assume that the axes are given, as are the integer valued points on both axes. This means, where you said in M2: construct a circle, instead, I want you to write down the equation of a circle, and where you said, construct a line, instead I want you to write down the equation of a line. Any time you are finding an intersection between two circles or a circle and line, I want you to find the intersection algebraically.

O. 1. Find the intersection points between the circle with center (1,1) and radius 2, and the line through (1,0) and slope 2.

2. Find an intersection point between the circle with center (1,1) and radius 2 and the circle with center (3, 2) and radius 2.

3. Now write down equations for circles with center (a,b) and radius r, and center (c, d) and radius q. Pretend you are solving for x to find the intersections of these two circles, and do the simplifications to get it to a polynomial. Notice that it is a degree 2 polynomial, so that the solution could be found by the quadratic formula, and the solution would probably have square roots in it.

F. Look at K. Realize that you have already done most of this.

1. Give a basis for $Q(\sqrt[3]{2})$ as a vector space over Q. What is the dimension $[Q(\sqrt[3]{2}):Q]$? Prove that the set of elements you have described is a field.

2. Do the same thing for $Q(\sqrt[3]{7})$

3. Give a basis for $Q(\sqrt[5]{2})$ as a vector space over Q. What is the dimension $[Q(\sqrt[5]{2}):Q]$?

G. 1. B and F together are give you the basis of a 1-line proof of G. Write down the proof.

Notice that the important thing is that the vector space has dimension 3, which is not a power of 2. If you look at Q, when you do this for constructible numbers, you are going to get a power of 2.

L. This is mostly a vector space proof. It's probably in your book (the abstract algebra one), and it may be in your notes from class. I want you to reproduce it for a couple of specific examples:

1. $Q(\sqrt{2},\sqrt{3}) \supseteq Q(\sqrt{2}) \supseteq Q$, prove, using appropriate representations in terms of basis vectors, that $[Q(\sqrt{2},\sqrt{3}):Q] = [Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})]\cdot[Q(\sqrt{2}):Q]$

2. $Q(\sqrt{2},\sqrt[3]{7}) \supseteq Q(\sqrt{2}) \supseteq Q$. Prove, using appropriate representations in terms of basis vectors, that $[Q(\sqrt{2},\sqrt[3]{7}):Q] = [Q(\sqrt{2},\sqrt[3]{7}):Q(\sqrt{2})]\cdot[Q(\sqrt{2}):Q]$

Q. Fill in the missing steps:
In the following, a simple construction step means that two constructible objects have been intersected and a single x- or y-value has been found for an intersection points. Thus, intersecting two circles would probably consist of 4 simple constructions: finding the two x and two y values.

If you start with numbers/points in Q, and you do a simple construction step and get the value α, then α is either in ________ or it is of the form _______.
That means that $[Q(\alpha):Q]$=______ or ______.
At the next simple construction step, suppose you find the value β. Then β is either in the set _______ or it is of the form __________.
That means that $[Q(\alpha,\beta):Q(\alpha)]$=______ or ______.
So $[Q(\alpha,\beta):Q]$=______ or ______ or ______.
Our induction hypothesis will be, given $F = Q(\alpha_1,\alpha_2,...\alpha_n)$ a field that is attained after n simple construction steps, $[F:Q] = 2^m$ where $m \le n$
Prove that after n+1 simple constructions steps $[Q(\alpha_1,\alpha_2,...\alpha_n,\alpha_{n+1}):Q] = 2^j$ where $j \le n+1$.
Conclude that if F is any field obtained from Q by compass and straight-edge constructions, that $[F:Q] = 2^m$ for some m.

I. Is a proof by contradiction. Suppose that the angle is constructible. What goes wrong? Where do you use uniqueness of factorization in *Z*?

J. Write an overview of this proof. If you were going to explain to someone who was not in this class (but who is mathematically inclined—perhaps another HS math teacher) how you prove that you can't trisect every angle, what 10-15 minute summary would you give them?