Proposition 9. Suppose \( P_1, \ldots, P_k, \Gamma_1, \ldots, \Gamma_l, s_1, \ldots, s_m, \) and \( \ell_1, \ldots, \ell_n \) 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 \([K^* : K] = 2^a\) for some integer \( a \), such that \( X \) is defined over \( K^* \).

Proof. We write \( K_0 = K \), and imagine writing down the construction line by line. In each line, we construct a new point defined over \( K \). 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 \( 2 \).
* 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 \( K_i = K' \).

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, since each factor on the RHS is either 2 or 1. Thus we take \( K^* = K_n \) and we are done.

Theorem 10. Given a segment \( AB \) of unit length, it is impossible (using Euclidean methods) to construct another segment of length \( \sqrt{2} \) times the length of the original segment.

Proof. Suppose for contradiction that it was possible. Let’s 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 proposition, 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 \([K' : \mathbb{Q}] \) a power of two. We then have a tower of fields \( K'/\mathbb{Q}[\sqrt{2}]_{CR}/\mathbb{Q} \), so

\[
[K' : \mathbb{Q}] = [K' : \mathbb{Q}[\sqrt{2}]_{CR}][\mathbb{Q}[\sqrt{2}]_{CR} : \mathbb{Q}]
\]

and so \([\mathbb{Q}[\sqrt{2}]_{CR} : \mathbb{Q}] \) is also a power of two. But we saw (§5, ex 25) that \([\mathbb{Q}[\sqrt{2}]_{CR} : \mathbb{Q}] = 3 \). Contradiction.

It follows that it is certainly not the case that, given segments \( AB \) and \( CD \), you can always construct segments \( XY \) and \( VW \) s.t. \( AB : XY = XY : VW = VW : CD \) by Euclidean methods.

Onwards! Before we tackle our next problem of antiquity, we will need a little lemma.
Lemma 11. Suppose \( P(x) = a_n x^n + \cdots + a_1 x + a_0 \) is a polynomial over \( \mathbb{Q} \) with integer coefficients, and the rational number \( r/s \) is a root of \( P \) (so \( P(r/s) = 0 \)). Assume that \( r/s \) is in lowest terms: that is, \( r, s \) are coprime. (Any fraction can be expressed in this form by dividing numerator and denominator by their \( \text{hcf} \).) Then \( r|a_0 \) and \( s|a_n \).

Proof. We know that \( P(r/s) = 0 \), so that \( a_n(r/s)^n + \cdots + a_1(r/s) + a_0 = 0 \) or, clearing denominators
\[
a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0.
\]
Thus \( a_n r^n = -s(a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-2} + a_0 s^{n-1}) \), so \( s|a_n r^n \). But \( (s, r) = 1 \) so \( (s, r^n) = 1 \), so it follows that \( s|a_n \). (To see this formally, put \( xs + r^ny = 1 \); then \( s|a_n r^ny \), so \( s|a_n(1 - xs) \) so \( s|a_n \).

A similar argument shows \( r|a_0 \).