10. IMPOSSIBLE CONSTRUCTIONS

§10.1. Number Fields and Field Extensions

One of the classic non-constructibility problems is that of trisecting an angle. Ruler and compass constructions exist for certain angles, such as 60°, and constructions exist that approximately trisect any angle, but there are none that exactly trisect any angle. This is not an open question, waiting for some brilliant mathematician to solve it. It is a logical impossibility. One can be as sure that no such construction will be produced as one can be sure that no-one will ever find a solution to the equation 0.x = 1.

We'll demonstrate the impossibility of trisecting an angle by translating it into an algebraic problem, using the concept of a number field.

Definition: A number field is any subfield of the complex numbers.

Example 1: Q, R and C are number fields but Z isn’t a field. The field Z_p, that is the integers modulo the prime p, form a field but as Z_p is not a subfield of C (the operations are different) it isn’t a number field.

To prove that a given set, F, of complex numbers is a number field it’s sufficient to check that 0, 1 ∈ F and that x + y, −x and x⁻¹ (if x ≠ 0) all belong to F whenever x, y ∈ F. This is because all other field axioms (associative, commutative and distributive laws) hold automatically for subfields.

Example 2: {a + b√2 | a, b ∈ Q} is a number field.

The only axiom that’s not immediately obvious is the existence of multiplicative inverses. Suppose a + b√2 ≠ 0. Then a − b√2 ≠ 0 and so:

\[
\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}.
\]

If F, K are number fields with F ≤ K, we say that K is an extension of F and we denote the extension by the symbol K:F.

A simple extension of a field F is a field F[α] where this denotes the smallest number field containing F (as a subfield) and α (as an element). Such a smallest number field will always exist because it will be the intersection of all number fields containing F and α (and the intersection of any collection of fields is itself a field).

Suppose we start with a number field F. Then F[α] would have to contain such numbers as 1 + α and α² and, in fact, all polynomial expressions in α. In addition it must contain \(\frac{\alpha^2}{1 + \alpha}\) and, more generally, all expressions that have the form \(\frac{f(\alpha)}{g(\alpha)}\) where f(α) and g(α) are polynomial expressions in α with g(α) ≠ 0. But some of these may be equal to others.

Example 3: Q[√2] = {a + b√2 | a, b ∈ Q}. We showed above that K = {a + b√2 | a, b ∈ Q} is a field. Clearly any number field that contains Q and √2 must contain every element of K. So K must be the smallest number field containing Q and √2.
Example 4: \( \mathbb{R}[i] = \mathbb{C} \) since a field that contains every real number as well as the complex number i must contain every complex number.

Example 5: \( \mathbb{R}[\pi] = \mathbb{R} \). More generally \( F[\alpha] = F \) whenever \( \alpha \in F \).

Theorem 1: If \( \alpha = a + b\beta \) for some \( a, b \in F \), with \( b \neq 0 \), then \( F[\alpha] = F[\beta] \).

Proof: \( F[\beta] \) contains \( \alpha \) and \( F \) so \( F[\alpha] \leq F[\beta] \). But \( \beta = -(a/b) + (1/b)\alpha \), so \( F[\alpha] \) contains \( F \) and \( \beta \) and hence \( F[\beta] \leq F[\alpha] \). Thus \( F[\alpha] = F[\beta] \).

Example 6: \( \mathbb{Q}[e^{2\pi i/3}] = \mathbb{Q}[\sqrt{3}i] \) since \( e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2} \).

§10.2. Fields as Vector Spaces

We’re attempting to solve the geometric problem of angle trisection using the algebraic theory of fields. But there’s a slightly more basic structure that’s very useful here, and one that we know a lot more about – vector spaces. Every field extension can be viewed as a vector space.

In fact the field extension \( K:F \) (this just means one field \( F \) contained inside another field \( K \)) can be viewed as a vector space over \( F \). The “vectors” are the elements of \( K \) and the “scalars” are the elements of \( F \). Never mind that \( K \) contains \( F \) so that some of the vectors are also scalars. There’s nothing in the vector space axioms which prevents this. Of course we’ll have to abandon the convention of writing vectors with a ~ underneath or printing them in bold type.

To be a vector space we need to be able to add two vectors and to multiply a vector by a scalar. This we can do because all vectors and scalars live inside the field \( K \). In fact we can even multiply two vectors, something that’s not normally possible in a vector space.

We also need to check out the many vector space axioms. But these will just be the field axioms. For example the axioms \( \lambda(u + v) = \lambda u + \lambda v \) and \( (\lambda + \mu)v = \lambda v + \mu v \) are just two instances of the distributive law.

If \( V \) is a finite-dimensional vector space over the field \( F \) we denote its dimension by the symbol \( |V:F| \). If \( K \) is a field extension of \( F \) the degree of the extension is simply the dimension \( |K:F| \) of this vector space. If \( K = F \) then \( |K:F| = 1 \). It can in fact be infinite, but we’ll be mainly interested in the case of finite-dimensional extensions.

The degree of a complex number \( \alpha \) over a number field \( F \) is defined to be the degree of the corresponding simple extension, that is, \( |F[\alpha]:F| \).

Example 7: Find the degree of \( \sqrt{2} \) over \( \mathbb{Q} \).

Solution: We must find a basis for \( \mathbb{Q}[\sqrt{2}] \) over \( \mathbb{Q} \). We’ve shown that every element of \( \mathbb{Q}[\sqrt{2}] \) has the form \( a + b\sqrt{2} \) for \( a, b \in \mathbb{Q} \). Writing this as \( a.1 + b.\sqrt{2} \) we can view this as a linear combination of the “vectors” 1 and \( \sqrt{2} \), with the “scalar” coefficients being the rational numbers \( a, b \). So 1 and \( \sqrt{2} \) span \( \mathbb{Q}[\sqrt{2}] \) over \( \mathbb{Q} \). But are they linearly independent? Suppose \( a + b\sqrt{2} = 0 \) for rational \( a, b \). If \( b \neq 0 \) this gives \( \sqrt{2} = -\frac{a}{b} \) which is impossible since \( \sqrt{2} \) is irrational. So \( b = 0 \). But then this forces \( a = 0 \). So 1, \( \sqrt{2} \) are indeed linearly independent, and so they form a basis for this field extension. The fact that the basis consists of two elements shows that the degree of the extension is 2.
Example 8: What is the degree of $\sqrt{n}$ over $\mathbb{Q}$ (where $n$ is an integer)?

**Solution:** If $\sqrt{n}$ is irrational (as is the case for $n = 2$, $n = 3$, $n = 5$ etc) then $\mathbb{Q}[\sqrt{n}]$ has degree 2 over $\mathbb{Q}$. But if $\sqrt{n} \in \mathbb{Q}$ (eg if $n = 4$) then $\mathbb{Q}[\sqrt{n}] = \mathbb{Q}$ and so $\sqrt{n}$ has dimension 1 over $\mathbb{Q}$.

**Theorem 2:** If $\alpha$ is a zero of some quadratic equation $ax^2 + bx + c$, where $a, b, c \in F$, and $\alpha \not\in F$, then $\alpha$ has degree 2 over $F$.

**Proof:** $\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. If $\Delta = b^2 - 4ac$ then $\Delta \in F$, but $\sqrt{\Delta} \not\in F$ (otherwise $\alpha \in F$).

A basis for $F[\alpha] = F[\sqrt{\Delta}]$ over $F$ is 1, $\sqrt{\Delta}$ and so $|F[\alpha]:F| = 2$.

Example 9: What is the degree of $\pi i$ over $\mathbb{C}$ and what is its degree over $\mathbb{R}$?

**Solution:** $\mathbb{C}[\pi i] = \mathbb{C}$ so $\pi i$ has degree 1 over $\mathbb{C}$. $\mathbb{R}[\pi i] = \mathbb{C}$ which has degree 2 over $\mathbb{R}$ and so $\pi i$ has degree 2 over $\mathbb{R}$. (It can be shown that $\pi i$ has infinite degree over $\mathbb{Q}$.)

§10.3. Dimensions of Field Extensions

**Theorem 3:** Suppose $V$ is a finite-dimensional vector space over the field $K$, which in turn is a finite-dimensional extension of the field $F$. Then $V$ can be viewed as a vector space over $F$ and $|V:F| = |V:K| \times |K:F|$.

**Proof:** Let $|V:K| = n$ and $|K:F| = m$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis for $V$ as a vector space over $K$ and let $\beta_1, \beta_2, \ldots, \beta_m$ be a basis for $K$ as a vector space over $F$. We’ll show that the $mn$ products $\alpha_i \beta_j$ form a basis for $V$ as a vector space over $F$. The theorem then follows.

The $\alpha_i \beta_j$ span $V$ over $F$. For, let $v \in V$. Then $v = k_1 \alpha_1 + \ldots + k_n \alpha_n$ for some “scalars” in $K$. But each of these is a “vector” in $K$, regarded as a vector space over $F$. Hence each $k_i$ can be expressed in the form $k_i = h_{ij} \beta_j$ where each $h_{ij} \in F$. Substituting into the previous equation we obtain $v = \sum_{i,j} h_{ij} \alpha_i \beta_j$ showing that the $\alpha_i \beta_j$ span $V$ over $F$.

On the other hand the $\alpha_i \beta_j$ are linearly independent over $F$. Suppose $\sum_{i,j} h_{ij} \alpha_i \beta_j = 0$ for $h_{ij}$’s $\in F$. Then $\sum_i \left( \sum_j h_{ij} \beta_j \right) \alpha_i = 0$ and since each $\sum_j h_{ij} \beta_j \in K$ and $\alpha_1, \ldots, \alpha_n$ is a basis for $V$ over $K$, each $\sum_j h_{ij} \beta_j = 0$. Now each $h_{ij} \in F$ and $\beta_1, \ldots, \beta_m$ is a basis for $V$ over $F$ and so each $h_{ij} = 0$. Thus the set of $mn$ products $\alpha_i \beta_j$ is linearly independent, and is therefore a basis for $V$ over $F$.

**Theorem 4:** If a point $(\alpha, \beta)$ is constructible by ruler and compass with rational coordinates then the degrees of $\alpha$ and $\beta$ over $\mathbb{Q}$ are powers of 2.

**Proof:** Suppose that at some stage in the ruler and compass construction the coordinates of all points generate some number field $F$. Then any point $(\alpha, \beta)$ that can be constructed from these points in one step is a point of intersection of two curves of the form $ax^2 + ay^2 + 2fx + 2gy + c = 0$.

(For $a \neq 0$ this represents a circle with centre $(-f/a, -g/a)$ with radius $\sqrt{\frac{f^2}{a^2} + \frac{g^2}{a^2} - c}$.)

For $a = 0$ it represents a straight line.)
The coefficients of the equations are expressible in terms of the coordinates of the points from which the circles/lines were constructed using only the operations of addition, subtraction, multiplication and division and so they belong to \( F \).

Eliminating \( y \) from these two equations we find that \( \alpha \) is a zero of some quadratic (or perhaps linear equation) with coefficients in \( F \). It follows that the degree of the minimum polynomial of \( \alpha \) over \( F \) is 1 or 2. Hence |\( F[\alpha]:F \)| = 1 or 2. Similarly |\( F[\beta]:F \)| = 1 or 2.

As the ruler and compass construction proceeds we build up a sequence of fields, each having degree 2 over the previous one. By Theorem 2, the degree of each of these fields over \( Q \) must be a power of 2. If \( \alpha \) is now a coordinate of any point that is constructible by ruler and compass (starting with points with rational coordinates) then \( \alpha \in K \) for some number field with |\( K:Q \)| = 2\( n \) for some \( n \). By Theorem 2, |\( F[\alpha]:Q[\alpha] \)| = |\( F:Q \)| = 2\( n \) and so |\( Q[\alpha]:Q \)| is a power of 2.

To show that an angle of 60° cannot be trisected by ruler and compass we need to show that an angle of 20° is not constructible and to do this we merely need to show that the degree of \( \cos(2\pi/9) \) over \( Q \) is not a power of 2. But how do we compute this degree?

We use the trigonometric identity:

\[
\cos(3\theta) = 4\cos^3\theta - 3\cos\theta.
\]

If \( \theta = 2\pi/9 \) (corresponding to the 20° angle that would result from a trisection of 60°) then

\[
3\theta = 2\pi/3 \text{ and } \cos(3\theta) = -\frac{1}{2}.
\]

So, if \( \alpha = \cos(2\pi/9) \) then \( 4\alpha^3 - 3\alpha = -\frac{1}{2} \) and so \( \alpha \) is a zero of the polynomial \( 8\alpha^3 - 6\alpha + 1 \).

This polynomial has in fact three zeros: \( \cos(2\pi/9), \cos(8\pi/9), \cos(14\pi/9) \). If any of these are rational then the cubic would factorise over \( Q \).

Using a calculator we find that:

\[
\cos(2\pi/9) \approx 0.7660444431, \quad \cos(8\pi/9) \approx -0.9396926208 \quad \text{and} \quad \cos(14\pi/9) \approx 0.1736481777.
\]

These don’t look rational, but that’s not very convincing. In actual fact these approximate values are rational (because they have finitely many decimal places) but then they’re only very good approximations and not the exact values. What then?

Suppose \( a/b \) (where \( a, b \) are coprime integers and \( a > 0 \)) is a zero of this cubic. Then:

\[
8 \frac{a^3}{b^3} - 6 \frac{a}{b} + 1 = 0 \quad \text{and so} \quad 8a^3 - 6ab^2 + b^3 = 0.
\]

Suppose \( a \neq 1 \) and let \( p \) be a prime divisor of \( a \). Then \( p \) divides \( a^3 \) and hence divides \( b^3 \) and so divides \( b \). This contradicts the coprimeness of \( a, b \). Hence \( a = 1 \).

This gives us \( 8 - 6b^2 + b^3 = 0 \) for some integer \( b \). Clearly \( b \) is even and divides 8 so \( b = \pm2, \pm4 \) or \( \pm8 \). Checking each of these we get a contradiction.

So \( 8x^3 - 6x + 1 \) has no rational zeros and so is a prime cubic over \( Q \).

**Theorem 5:** If \( p(x) = px^3 + qx^2 + rx + s \) is a prime cubic over \( Q \) and \( p(\alpha) = 0 \) then |\( Q[\alpha]:Q \)| = 3.

**Proof:** Let \( K = \{a\alpha^2 + b\alpha + c \mid a, b, c \in Q\} \). By the closure properties \( K \) must be a subset of \( Q[\alpha] \). In fact \( K \) is a field. It’s clearly closed under addition and subtraction.

The fact that \( p\alpha^3 + q\alpha^2 + r\alpha + s = 0 \) means that \( \alpha^3 \) can be expressed as a rational linear combination of 1, \( \alpha \) and \( \alpha^2 \). So, multiplying two elements of \( K \) we get an expression involving powers of \( \alpha \) up to \( \alpha^4 \), but then \( \alpha^5 \), and hence \( \alpha^4 \), can be expressed in terms of 1, \( \alpha \) and \( \alpha^2 \). The only thing left to check is closure under inverses.
Is \( \frac{1}{a\alpha^2 + bx + c} \in K \) if the denominator is non-zero?

Suppose the denominator is non-zero and let \( h(x) \) be the polynomial \( ax^2 + bx + c \).

If \( p(x) \) divides \( h(x) \) then the denominator is \( h(\alpha) = 0 \).

So \( p(x) \) doesn’t divide \( h(x) \) and hence they’re coprime. It follows that there exist polynomials \( e(x), f(x) \in \mathbb{Q}[x] \) such that

\[
e(x)p(x) + f(x)h(x) = 1.
\]

Now substituting \( x = \alpha \) we get

\[
e(\alpha)p(\alpha) + f(\alpha)h(\alpha) = f(\alpha)h(\alpha) = 1.
\]

Hence \( \frac{1}{h(\alpha)} = f(\alpha) \in K \).

This means that \( \mathbb{Q}[\alpha] = \{a\alpha^2 + bx + c \mid a, b, c \in \mathbb{Q}\} \) and so \( 1, \alpha \) and \( \alpha^2 \) span \( \mathbb{Q}[\alpha] \).

Are they linearly independent?

Suppose there exist rational numbers \( a, b \) and \( c \) such that \( a\alpha^2 + bx + c = 0 \).

Let \( u(x) \) be the polynomial \( ax^2 + bx + c \). Dividing \( p(x) \) by the quadratic \( u(x) \) we get

\[
p(x) = u(x)q(x) + (rx + s),
\]

where \( rx + s \) is the remainder.

Substituting \( x = \alpha \) we get \( \alpha r + s = 0 \). If \( r \neq 0 \) we get \( \alpha = -s/r \in \mathbb{Q} \), a contradiction.

Hence \( r = 0 \) and so \( s = 0 \). But then \( p(x) = u(x)q(x) \), contradicting the assumption that \( p(x) \) is prime. It follows that \( \{1, \alpha, \alpha^2\} \) is a basis for \( \mathbb{Q}[\alpha] \) over \( \mathbb{Q} \) and so \( \alpha \) has degree 3 over \( \mathbb{Q} \).

The theorem can be easily generalised to any field, and any prime polynomial.

**Theorem 6:** If \( \alpha \) is a zero of a prime polynomial of degree \( n \) over a field \( F \) then \( |F[\alpha]:F| = n \) and \( 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \) is a basis.

To wrap things up, it’s impossible to have a ruler and compass construction for trisecting any given angle, because it would have to be able to trisect \( 60^\circ \) in particular. But this would involve constructing a point having \( \cos(2\pi/9) \). Since ruler and compass constructions involve intersecting lines with lines and lines with circles and circles, the coordinates of newly constructed points would have degree 1 or 2 over the field generated by the coordinates of the existing points. No matter how many steps were involved in the construction the degree of the coordinates of any point so constructed, over \( \mathbb{Q} \), would have to be a power of 2. But the degree of \( \cos(2\pi/9) \) over \( \mathbb{Q} \) is 3, which is not a power of 2. Therefore no such trisection construction is possible.

**EXERCISES FOR CHAPTER 10**

**Exercise 1:** Determine which of the following are TRUE and which are FALSE

1. Every angle can be trisected by ruler and compass.
2. A regular polygon with 18 sides can be constructed by ruler and compass.
3. \( \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \) is a number field.
4. \( \mathbb{Q}[\sqrt{8}] = \mathbb{Q}[\sqrt{2}] \).
5. If \( F \) is a number field then so is \( \{f(\alpha) \mid f(x) \in F[x]\} \).
6. \( 1, \omega, \omega^2 \) are linearly independent over \( \mathbb{Q} \).
7. \( \mathbb{Q}[1 + \sqrt{2}] = \mathbb{Q}[\sqrt{4}] \).
8. If \( H, K \) are number fields then \( H \cap K \) a number field.
9. \( \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \) is a vector space over \( \mathbb{Q} \).
10. \( |\mathbb{Q}[(\sqrt{2}/11)] : \mathbb{Q}| = 11 \).
Exercise 2: Prove that there is no number field $F$ such that $\mathbb{R} < F < \mathbb{C}$.

Exercise 3: Prove that all the zeros of $x^8 + x^4 + 1$ are constructible.  
[HINT: $x^8 + x^4 + 1$ is a quadratic in $x^4$.]

Exercise 4: Prove that $\{a + b^{1/4} + c\sqrt{2} + d^{3/4} \mid a, b, c, d \in \mathbb{Q}\}$ is a number field.  
[HINT: Of course you could check it directly, but would Theorem 6 help?]

Exercise 5: Prove that the volume of a cube cannot be doubled by a ruler and compass construction.  That is, show that $\sqrt[3]{2}$ is not constructible.

Exercise 6:
Show that the following construction, attributed to Archimedes, will exactly trisect any given angle and explain why this doesn’t contradict the theorem that angles can’t be trisected by ruler and compass.

To trisect the angle $\angle AOB$, with $A, B$ on a circle of radius $r$ with centre $O$, construct $C'$ so that $C'OB$ is a diameter of the circle and construct $L'$ on this diameter so that $L'C' = r$.  Having a straight edge lying along the diameter $C'OB$, with points $L'$ and $C'$ marked on them, move it so that $C'$ slides around the circle, and $L'$ slides along the diameter.  Being a rigid straight edge, the distance between $L'$ and $C'$ will always be equal to $r$.  Continue sliding until the straight edge passes through $A$ and let $L, C$ be the respective positions of $L'$ and $C'$ when this occurs.  Then $\angle ALO$ will be exactly one third of $\angle AOB$.

Exercise 7: Prove that the regular pentagon can be constructed by ruler and compass.  
[HINT: Find a polynomial with integer coefficients that has $\cos(2\pi/5)$ as a root.]

Exercise 8: Prove that the regular heptagon (seven equal sides) is not constructible by ruler and compass.
SOLUTIONS FOR CHAPTER 10

Exercise 1:
(1) FALSE; (2) FALSE That would make 20° constructible; (3) FALSE $4^{1/3}$ is not in the set; (4) TRUE; (5) FALSE Only true if $\alpha$ is algebraic; (6) FALSE $1 + \alpha + \omega^2 = 0$; (7) TRUE; (8) TRUE; (9) TRUE; (10) FALSE (the minimum polynomial has degree $\leq 10$ since $x - 1$ is a factor of $x^{11} - 1$).

Exercise 2: $|C: R| = 2$. If $R < F < C$, $|C:F| = |C:R||F:R|$ but each of these factors is at least 2, a contradiction.

Exercise 3: If $\alpha$ is a zero of $x^8 + x^4 + 1$ then $\alpha^4 = -\frac{1 + \sqrt{3}}{2}$. So $|Q[\alpha^4]:Q| = 2$. Clearly $|Q[\alpha]:Q[\alpha^2]| = |Q[\alpha^2]:Q[\alpha^4]| = 2$ so $|Q[\alpha]:Q[\alpha^4]| = 4$ and $Q[\alpha]:Q| = 8$. Since this is a power of 2, $\alpha$ is constructible.

Exercise 4: Let $\alpha = \sqrt[4]{2}$. Then $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \alpha)(x + \alpha)(x - i\alpha)(x + i\alpha)$. None of these factors has rational coefficients, and no pair of factors can multiply to give a polynomial with rational coefficients. So $x^4 - 2$ is prime over $Q$. Hence, by Theorem 6, \{1, $\alpha$, $\alpha^2$, $\alpha^3$\} is a basis for $Q[\alpha]$ over $Q$. Hence \{ $a + b\sqrt{2} + c\sqrt[4]{4} + d\sqrt[8]{8}$ $|$ $a, b, c, d \in Q$ \} is a field.

Exercise 5: Let $\alpha = \sqrt[3]{2}$. The roots of $x^3 - 2$ are $\alpha, \alpha\omega, \alpha\omega^2$ where $\omega = e^{2\pi i/3}$. Since none of these is rational (we’d prove that $\sqrt[3]{2}$ is irrational in a similar way to $\sqrt{2}$) this polynomial has no rational roots and hence no linear factors and hence is prime over $Q$. Therefore, by Theorem 5, $|Q[\alpha]:Q| = 3$. Since this is not a power of 2, $\sqrt[3]{2}$ is not constructible.

Exercise 6:

If $\angle CLO = \alpha$ then $\angle COL = \alpha$ as $\Delta CLO$ is isosceles. Hence $\angle ACO = 2\alpha$, being the exterior angle of $\Delta OCL$. Since $\Delta OAC$ is isosceles, $\angle CAO = 2\alpha$ and so $\angle AOB = 3\alpha$ being the exterior angle of $\Delta OAL$.

Although this method exactly trisects a given angle, it is not a ruler and compass construction. The sliding of $L'$ and $C'$ until the line passes through $A$ is not a permissible operation according to the definition of ruler and compass constructions.
**Exercise 7:** Let $c = \cos \frac{2\pi}{5}$ and let $s = \sin \frac{2\pi}{5}$. Then $(c + is)^5 = \cos(2\pi) + is\sin(2\pi) = 1$.

Equating imaginary parts we have $5c^4s - 10c^2s^3 + s^5 = 0$. Dividing by $s$ (clearly non-zero) and writing $s^2 = 1 - c^2$ we get $5c^4 - 10c^2(1 - c^2) + (1 - c^2)^2 = 0$, that is, $16c^4 - 12c^2 + 1 = 0$.

Considering this as a quadratic in $c^2$, we get $c^2 = \frac{12 \pm \sqrt{80}}{32}$, whence $c = \pm \sqrt{\frac{12 \pm \sqrt{80}}{32}}$. With a calculator we can check that, of the four alternatives, $c = \sqrt{\frac{12 - \sqrt{80}}{32}}$. Hence $c$ is constructible.

**Exercise 8:**

Let $c = \cos \frac{2\pi}{7}$ and let $s = \sin \frac{2\pi}{7}$. Then $(c + is)^7 = \cos(2\pi) + is\sin(2\pi) = 1$.

Equating imaginary parts we have $7c^6s - 35c^4s^3 + 21c^2s^5 - s^6 = 0$. Dividing by $s$ (clearly non-zero) and writing $s^2 = 1 - c^2$ we get $7c^6 - 35c^4(1 - c^2) + 21c^2(1 - c^2)^2 - (1 - c^2)^3 = 0$, that is, $64c^6 - 80c^4 + 24c^2 - 1 = 0$. Let $x = c^2$. Then $64x^3 - 80x^2 + 24x - 1 = 0$. If the regular heptagon is constructible then so is $c$ and hence $x$ is constructible.

Let $\frac{a}{b}$ be a rational root of this cubic (with $a, b$ coprime and $a > 0$).

Then $64\left(\frac{a^3}{b^3}\right) - 80\left(\frac{a^2}{b^2}\right) + 24\left(\frac{a}{b}\right) - 1 = 0$ and so $64a^3 - 80a^2b + 24ab^2 - b^3 = 0$. If $p$ is any prime divisor of $a$ then $p$ divides $b^3$ and hence divides $b$. If $a > 1$ this contradicts the coprimeness of $a, b$ and hence $a = 1$.

So if $g(x) = x^3 - 24x^2 + 80x - 64$ then $g(b) = 0$. But $g(1) = -7$, $g(2) = 8$ and $g(3) = -13$ so there are zeros between 1 and 2 and between 2 and 3. Clearly there must be a third zero beyond 3, since ultimately $g(x)$ becomes positive again. With a bit of persistence we find that it lies between 20 and 21.

So $g(x)$ has no integer zeros and hence $f(x) = 64x^3 - 80x^2 + 24x - 1$ has no rational zeros. It must therefore be prime over $\mathbb{Q}$. So the degree of $\cos(2\pi/7)$ over $\mathbb{Q}$ is 3 and hence it is not constructible.