

# 2. FIELD EXTENSIONS

## (THE IMPOSSIBILITY OF ANGLE TRISECTION)

### §2.1. Ruler and Compass Constructions

The Greeks considered arithmetic and geometry as being two ways of looking at the same number system and geometrical constructions to perform arithmetic operations were considered very natural. And since the only numbers they could conceive of arithmetically were rational numbers they assumed that that's all that could be obtained geometrically.

So it came as a great shock for them to discover that  $\sqrt{2}$  is irrational, that is a number which had a proper geometric existence but did not have a proper arithmetic one. But then irrational numbers came to be accepted though they did not lose their geometric flavour. Number was a geometric concept. And it was accepted as an unwritten axiom that only numbers which arose in the context of geometric constructions could possibly exist.

Certain problems were posed where a construction "must exist but is hard to find". The three most famous were the doubling of a cube, the trisection of an angle and the squaring of a circle. The numbers involved in these three problems clearly exist, they thought (it's interesting that their intuition must have been using some primitive notion of continuity — a concept that took another couple of thousand years to become fully developed), so clearly there had to be a corresponding construction. And "construction" meant a construction using ruler and compass.

#### **Doubling the Cube:**

There is a legend that when asked for a way of stopping a plague that was attacking the city of Delos, the Oracle of Delphi advised that the altar of Apollo should be doubled in size. The altar was in the shape of a cube and although its sides were doubled the plague continued. The Oracle then revealed that the citizens of Delos had not done as instructed since they had increased the altar eight-fold. What was required was to double the volume. The problem of doubling the cube is thus:

**Given the side of a cube, construct the side of a cube with twice the volume.**

#### **Trisecting an Angle:**

**Divide any given angle into three equal pieces.**

For certain special angles, such as  $90^\circ$ , it can easily be done (a  $30^\circ$  angle can easily be constructed). But the problem is to do it for *any* given angle.

#### **Squaring the Circle:**

**Construct a square whose area is exactly equal to that of a given circle.**

The methods allowed in all these constructions are the use of a ruler and compass. The compass is to be used to draw circles through given points and passing through others. The ruler must be used solely as a straight-edge for joining points by straight lines, not for measurement. For this reason, ruler and compass constructions are often called constructions by *straight-edge* and compass.

The reason for disallowing measurement is the question of accuracy. The accuracy with which we can measure lengths is limited by the scale of the markings. Even if we had the means to magnify the scale we'd have to end up making judgements. The whole philosophy of ruler and compass constructions is to have a procedure that is theoretically exact.

There do exist ruler and compass methods for getting quite good approximations to the solutions to all three problems. But that's not the point. With a question of existence it's no good saying that these numbers *approximately* exist. We need methods which in themselves are *exact*. And it has been shown that all three problems are insoluble by ruler and compass methods. The geometric concept of number in terms of constructibility thus proved to be inadequate and so the more general concept of real number gradually emerged.

The objects in a ruler and compass construction are points (denoted A, B, C, ... ) and lines (denoted by a, b, c ... ). Lines include straight lines and circles, which can either be given or can be drawn in the course of the construction. Other curves, such as parabolas, can only occur if they are given at the beginning of the construction.

**LINE(A, B)** = the line through A,B (where  $A \neq B$ )

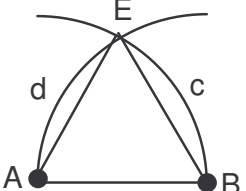
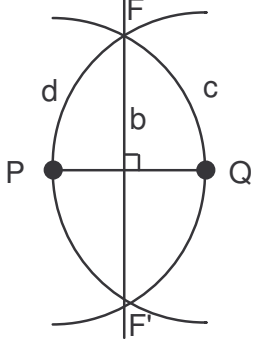
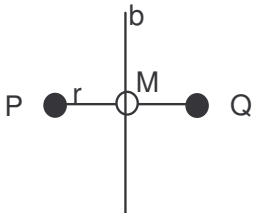
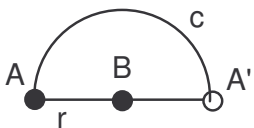
**CIRCLE(A, B)** = circle centre A, passing through B (where  $A \neq B$ )

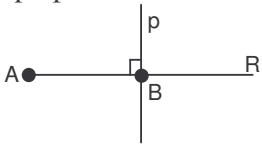
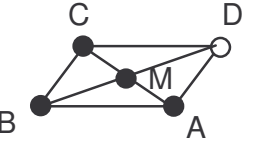
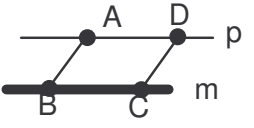
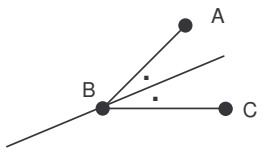
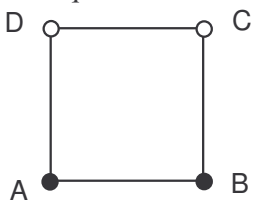
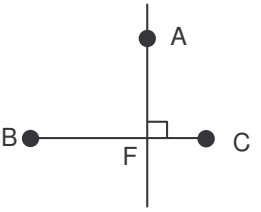
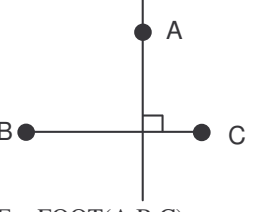
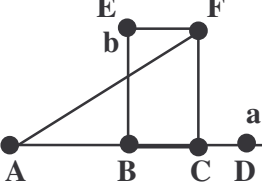
**INTERSECTIONS** of lines with lines.

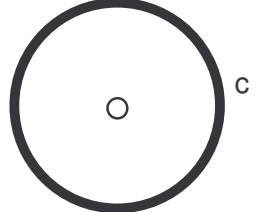
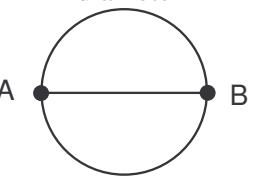
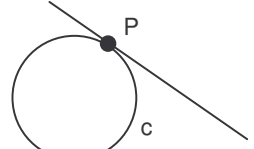
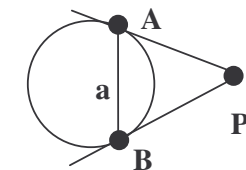
$A, B, \dots = p \cap q$  indicates that A, B, ... are the points of intersection of p, q.

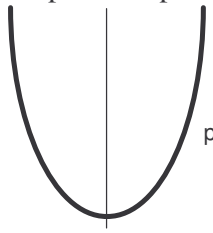
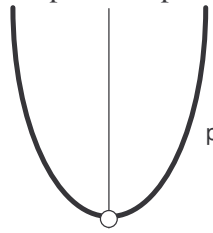
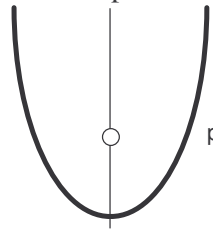
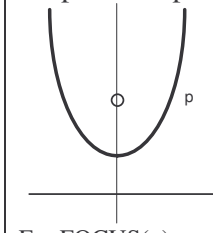
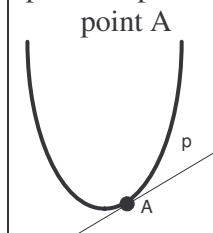
$A, B, \dots \in p$  describes A, B, C as arbitrary (but distinct) points on p.

## §2.2. Examples of Ruler and Compass Constructions

<b>LINES</b>			
<p><b>EQUILAT(A,B)</b> third vertex to make an equilateral triangle</p>  <p><math>c = \text{CIRCLE}(A,B)</math> <math>d = \text{CIRCLE}(B,A)</math> <math>E, E' = d \cap c</math></p>	<p><b>PERPBIS(P,Q)</b> perpendicular bisector of PQ</p>  <p><math>c = \text{CIRCLE}(P,Q)</math> <math>d = \text{CIRCLE}(Q,P)</math> <math>F, F' = c \cap d</math> <math>b = \text{LINE}(F, F')</math></p>	<p><b>MIDPT(P,Q)</b> midpoint of the interval PQ</p>  <p><math>r = \text{LINE}(P,Q)</math> <math>b = \text{PERPBIS}(P,Q)</math> <math>M = r \cap b</math></p>	<p><b>REFLECT(A,B)</b> reflection A' of A in B</p>  <p><math>r = \text{LINE}(A,B)</math> <math>c = \text{CIRCLE}(B,A)</math> <math>A, A' = r \cap c</math></p>

<p><b>PERP(A,B)</b> line through B that's perpendicular to AB</p>  <p><math>R = \text{REFLECT}(A,B)</math> <math>p = \text{PERPBIS}(A,R)</math></p>	<p><b>PGRAM(A,B,C)</b> point D such that ABCD is a parallelogram</p>  <p><math>M = \text{MIDPT}(A,C)</math> <math>D = \text{REFLECT}(B,M)</math></p>	<p><b>PARR(A,m)</b> line through A that's parallel to m</p>  <p><math>B, C \in m</math> <math>D = \text{PGRAM}(A,B,C)</math> <math>p = \text{LINE}(A,D)</math></p>	<p><b>BISECT(A,B,C)</b> bisector of angle ABC</p>  <p><math>m = \text{LINE}(B,C)</math> <math>c = \text{CIRCLE}(B,A)</math> <math>F, F' = m \cap c</math> <math>G = \text{PGRAM}(A,B,F)</math> <math>b = \text{LINE}(B,G)</math></p>
<p><b>SQUARE(A,B)</b> square ABCD</p>  <p><math>m = \text{PERP}(B,A)</math> <math>c = \text{CIRCLE}(A, B)</math> <math>D, D' = m \cap c</math> <math>C = \text{PGRAM}(D,A,B)</math></p>	<p><b>FOOT(A,B,C)</b> foot of the perpendicular from A to BC</p>  <p><math>a = \text{LINE}(B,C)</math> <math>c = \text{CIRCLE}(A,B)</math> <math>D, E = a \cap c</math> <math>F = \text{MIDPT}(D,E)</math></p>	<p><b>PERP(A,B,C)</b> perpendicular from A to BC</p>  <p><math>F = \text{FOOT}(A,B,C)</math> <math>a = \text{LINE}(A, F)</math></p>	<p><b>PYTHAG(A,B,C)</b> point D on the line ABC with <math>AD^2 = AB^2 + AC^2</math></p>  <p><math>a = \text{LINE}(A, B)</math> <math>b = \text{PERP}(A,B)</math> <math>E = \text{CIRCLE}(B,A) \cap b</math> <math>F = \text{PGRAM}(B,E,F)</math> <math>D = \text{CIRCLE}(A,D) \cap a</math></p>

<b>CIRCLES</b>			
<p><b>CENTRE(c)</b> centre of circle c</p>  <p><math>P, P', P'' \in c</math> <math>b' = \text{PERPBIS}(P,P')</math> <math>b'' = \text{PERPBIS}(P,P'')</math> <math>C = b' \cap b''</math></p>	<p><b>DIAM(A,B)</b> circle on AB as diameter</p>  <p><math>C = \text{MIDPT}(A,B)</math> <math>c = \text{CIRCLE}(C,A)</math></p>	<p><b>TANG(c,P)</b> tangent to circle c at P lying on the circle</p>  <p><math>C = \text{CENTRE}(c)</math> <math>t = \text{PERP}(C,P)</math></p>	<p><b>CHORD(c, P)</b> chord of contact of tangents from P to circle c</p>  <p><math>C = \text{CENTRE}(c)</math> <math>b = \text{DIAM}(C, P)</math> <math>A, B = b \cap c</math> <math>p = \text{LINE}(A, B)</math></p>

<b>PARABOLAS</b>				
<b>AXIS(p)</b> axis of parabola p 	<b>VERTEX(p)</b> vertex of parabola p 	<b>FOCUS(p)</b> focus of parabola p 	<b>DIRECTRIX(p)</b> directrix of parabola p 	<b>TANG(p,A)</b> tangent to parabola p at the point A 
A, B, C ∈ p t = LINE(A, B) r = PARR(C, t) D = r ∩ p E = MIDPT(A, D) F = MIDPT(B, C) g = PERP(F, E) H, H' = g ∩ p a = PERPBIS(H, H')	V = AXIS(p) ∩ p	P ∈ p a = AXIS(p) V = VERTEX(p) y = PARR(P, a) x = PERP(V, a) M = x ∩ y G = REFLECT(P, M) d = PERPBIS(P, G) F = a ∩ d	F = FOCUS(p) V = VERTEX(p) R = REFLECT(F, V) d = PERP(R, F)	a = AXIS(p) F = FOCUS(p) d = DIRECTRIX(p) c = CIRCLE(A, F) T = d ∩ c t = BISECT(F, A, T)

## §2.3. Constructible Numbers

We identify the complex number with its corresponding point on the complex plane. A **constructible number** is a complex number whose corresponding point on the complex plane can be constructed by ruler and compass, starting with two points representing 0 and 1.

**Theorem 1:** A complex number is constructible if and only if its real and imaginary parts are constructible.

**Proof:** The real and imaginary axes are  $r = \text{LINE}(0, 1)$  and  $i = \text{PERP}(1, 0)$  respectively.

$\text{Re}(z) = \text{FOOT}(a, r)$  and  $\pm \text{Im}(z) = \text{CIRCLE}(0, \text{FOOT}(a, i)) \cap r$  so if  $z$  is constructible then so are  $\text{Re}(z)$  and  $\text{Im}(z)$ . Conversely  $z = \text{PYTHAG}(0, \text{Re}(z), \text{Im}(z))$  so if the real and imaginary parts are constructible so is  $z$ .

**Theorem 2:** The set of constructible numbers is a field.

**Proof:** Firstly the set of all real constructible numbers is a field since:

$$x + y = \text{PGRAM}(0, x, y) = \text{REFLECT}(0, \text{MIDPT}(x, y))$$

$$-x = \text{REFLECT}(x, 0)$$

$$xy = \text{LINE}(0, \text{PYTHAG}(0, 1, x)) \cap \text{PERP}(0, y)$$

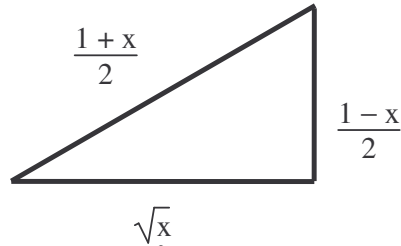
$$1/x = \text{LINE}(0, \text{PYTHAG}(0, x, 1)) \cap \text{PERP}(0, 1)$$

Since the sum, product and additive and multiplicative inverses of a complex number can be expressed in terms of their real and imaginary parts, using only the field operations of addition, subtraction, multiplication and division, the theorem follows from the real case and Theorem 1.

**Corollary:** Rational numbers are constructible.

**Theorem 3:** The square roots of a constructible number are constructible.

**Proof:** The theorem is true for positive real constructible numbers as the following construction shows (we leave it as an exercise to obtain an explicit construction).



For a non-real constructible number,  $z = re^{i\theta}$  we construct  $r = \text{CIRCLE}(0, z) \cap \text{LINE}(0, 1)$ . Then we construct  $\sqrt{r}$  as above. The square roots of  $z$  are  $\text{BISECT}(z, 0, 1) \cap \text{CIRCLE}(0, \sqrt{r})$ .

**Example 1:**  $\sqrt{3 + \sqrt{5 - \sqrt{\frac{3 + \sqrt{2}}{\sqrt{7}}}}} + \frac{\sqrt[4]{5}}{\sqrt{3 + \sqrt{2}}} i$  is constructible (though it would probably be a nightmare to obtain an explicit construction).

While there are infinitely many constructible numbers, of arbitrary complexity, most complex numbers are not constructible. In the course of this chapter we shall prove that  $\sqrt[3]{2}$  and  $e^{2\pi i/9}$  are not constructible, thereby proving the impossibility of doubling the cube and trisecting a given angle, by ruler and compass. Another famous non-constructible number is  $\pi$  whose non-constructibility establishes the impossibility of squaring the circle.

## §2.4. Number Fields and Field Extensions

We translate the geometric problem of trisecting a given angle into an algebraic one, using the concept of a number field. A **number field** is defined to be any field of complex numbers, that is, any subfield of  $\mathbb{C}$ .

**Example 2:**  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are number fields but  $\mathbb{Z}$  is not a field. The field  $\mathbb{Z}_p$ , that is the integers modulo the prime  $p$ , form a field but as  $\mathbb{Z}_p$  is not a subfield of  $\mathbb{C}$  (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 is sufficient to check that  $0, 1 \in F$  and that  $x + y, -x$  and  $x^{-1}$  (if  $x \neq 0$ ) all belong to  $F$  whenever  $x, y \in F$ . This is because all other field axioms (associative, commutative and distributive laws) hold automatically.

**Example 3:**  $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$  is a number field.

The only axiom which is not immediately obvious is the existence of multiplicative inverses. Suppose  $a + b\sqrt{2} \neq 0$ . Then  $a - b\sqrt{2} \neq 0$  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  $F \leq K$ , 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  $F[\alpha]$  where this denotes the smallest number field containing  $F$  (as a subfield) and  $\alpha$  (as an element). Such a smallest number field will always exist because it will be the intersection of all number fields containing  $F$  and  $\alpha$  (and the intersection of any collection of fields is itself a field).

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

**Example 4:**  $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ . We showed above that  $K = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$  is a field. Clearly any number field that contains  $\mathbf{Q}$  and  $\sqrt{2}$  must contain every element of  $K$ . So  $K$  must be the smallest number field containing  $\mathbf{Q}$  and  $\sqrt{2}$ .

**Example 5:**  $\mathbf{R}[i] = \mathbf{C}$  since a field that contains every real number as well as the complex number  $i$  must contain every complex number.

**Example 6:**  $\mathbf{R}[\pi] = \mathbf{R}$ . More generally  $F[\alpha] = F$  whenever  $\alpha \in F$ .

**Theorem 4:** 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  $\beta = \frac{-a}{b} + \frac{1}{b}\alpha$ , so  $F[\alpha]$  contains  $F$  and  $\beta$  and hence  $F[\beta] \leq F[\alpha]$ . Thus  $F[\alpha] = F[\beta]$ .

**Example 7:**  $\mathbf{Q}[e^{2\pi i/3}] = \mathbf{Q}[\sqrt{3}i]$  since  $e^{2\pi i/3} = -1/2 + 1/2(\sqrt{3}i)$ .

## §2.5. Fields as Vector Spaces

We are attempting to solve the geometric problem of angle trisection using the algebraic theory of fields. But there's a slightly more basic structure that is 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  $K:F$  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  $\sim$  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 is 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 8:** Find the degree of  $\sqrt{2}$  over  $\mathbf{Q}$ .

**Solution:** We must find a basis for  $\mathbf{Q}[\sqrt{2}]$  over  $\mathbf{Q}$ . We've shown that every element of  $\mathbf{Q}[\sqrt{2}]$  has the form  $a + b\sqrt{2}$  for  $a, b \in \mathbf{Q}$ . Writing this as  $a \cdot 1 + b \cdot \sqrt{2}$  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  $\mathbf{Q}[\sqrt{2}]$  over  $\mathbf{Q}$ . 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. Hence they form a basis for this field extension. The fact that it consists of two elements shows that the degree of the extension is 2.

**Example 9:** What is the degree of  $\sqrt[n]{n}$  over  $\mathbf{Q}$  (where  $n$  is an integer)?

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

**Example 10:** What is the degree of  $\pi i$  over  $\mathbf{C}$  and what is its degree over  $\mathbf{R}$ ?

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

## §2.6. Dimensions of Field Extensions

**Theorem 5:** 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  $\alpha_1, \alpha_2, \dots, \alpha_n$  be a basis for  $V$  as a vector space over  $K$  and let  $\beta_1, \beta_2, \dots, \beta_m$  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  $v = k_1\alpha_1 + \dots + k_n\alpha_n$  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  $k_i = h_{i1}\beta_1 + \dots + h_{im}\beta_m$  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  $\alpha_1, \dots, \alpha_n$  is a basis

for  $V$  over  $K$ , each  $\sum_j h_{ij}\beta_j = 0$ . Now each  $h_{ij} \in F$  and  $\beta_1, \dots, \beta_m$  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 hence a basis for  $V$  over  $F$ .

In this chapter we'll be mostly using this theorem where  $A \leq B \leq C$  is a sequence of field extensions, in which case  $|C:A| = |C:B| \cdot |B:A|$  but in chapter 3 we'll need to use it in this greater generality.

**Theorem 6:** If a point  $(\alpha, \beta)$  is constructible by ruler and compass with rational coordinates, the degrees of  $\alpha$  and  $\beta$  over  $\mathbf{Q}$  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  $(\alpha, \beta)$  which 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 with coefficients in  $F$ . Thus 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 7 the degree of each of these fields over  $\mathbf{Q}$  must be a power of 2. If  $\alpha$  is now a coordinate of any point which is constructible by ruler and compass (starting with points with rational coordinates) then  $\alpha \in F$  for some number field with  $|F:\mathbf{Q}| = 2^n$  for some  $n$ . By Theorem 7  $|F:\mathbf{Q}[x]| \cdot |\mathbf{Q}[x]| = |F:\mathbf{Q}| = 2^n$  and so  $|\mathbf{Q}[\alpha]:\mathbf{Q}|$  is a power of 2.

To show that an angle of  $20^\circ$  cannot be constructed by ruler and compass we simply need to show that  $|\mathbf{Q}[\cos(2\pi/9)]:\mathbf{Q}|$  is not a power of 2. But how do we compute this degree?

## §2.7. Degree of the Minimum Polynomial

The next theorem gives the explicit form of the field  $F[\alpha]$  when  $\alpha$  is algebraic over  $F$ . It says that the elements of  $F[\alpha]$  consist of all polynomials over  $F$  evaluated at  $x = \alpha$ .

**Theorem 7:** If  $\alpha$  is algebraic over  $F$  then  $F[\alpha] = \{f(\alpha) \mid f(x) \in F[x]\}$ .

**Proof:** We show firstly that  $W = \{f(\alpha) \mid f(x) \in F[x]\}$  is a field. If  $f(\alpha), g(\alpha) \in W$ , clearly  $f(\alpha) + g(\alpha), f(\alpha)g(\alpha)$  and  $-f(\alpha)$  are in  $W$ . Moreover 0, 1 are in  $W$  since they are values of constant polynomials in  $F[x]$ . We now show that if  $f(\alpha) \neq 0, f(\alpha)^{-1} \in W$ .

Suppose  $f(\alpha) \neq 0$ . Let  $p(x)$  be the minimum polynomial of  $\alpha$  over  $F$ . Now if  $p(x)$  divides  $f(x)$  then  $f(\alpha) = 0$ , a contradiction. Hence  $p(x)$  is coprime with  $f(x)$  and so for some  $h(x), k(x) \in F[x]$  we have  $p(x)h(x) + f(x)k(x) = 1$ . Substitute  $x = \alpha$ . Then  $1 = p(\alpha)h(\alpha) + f(\alpha)k(\alpha) = f(\alpha)k(\alpha)$  and so  $1/f(\alpha) = k(\alpha) \in F[x]$ .

**Theorem 8:** If  $\alpha$  is algebraic over  $F$  then  $F[\alpha]$  is a finite-dimensional extension of  $F$  and the degree of the extension is equal to the degree of the minimum polynomial over  $F$ .

**Proof:** Let  $p(x)$  be the minimum polynomial of  $\alpha$  over  $F$ , with degree  $n$ . We'll show that  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  is a basis for  $F[\alpha]$  over  $F$ .

A typical element of  $F[\alpha]$  is, by Theorem 9,  $f(\alpha)$  for some  $f(x) \in F[x]$ . Now  $f(x) = p(x)q(x) + r(x)$  for some  $q(x), r(x) \in F[x]$  where  $r(x) = 0$  or  $\deg r(x) < \deg p(x)$ . Thus  $r(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  for some  $a_i$ 's  $\in F$ . Hence  $f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$ . Thus  $F[\alpha]$  is spanned by  $\{1, \alpha, \dots, \alpha^{n-1}\}$ .

We must now show that these elements are linearly independent over  $F$ . Suppose that  $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = 0$  where the  $a_i$ 's  $\in F$ . Then  $a(\alpha) = 0$  where  $a(x)$  is the polynomial  $a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in F[x]$ . Thus by Theorem 6,  $p(x)$  divides  $a(x)$ . If  $a(x)$  is a non-zero polynomial we get a contradiction since  $\deg a(x) \leq n - 1 < n = \deg p(x)$ . Thus  $a(x)$  is the zero polynomial and so all its coefficients,  $a_i$ , must be zero.

This shows that  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  is a basis for  $F[\alpha]$  over  $F$  and so  $|F[\alpha]:F| = n$ , the degree of the minimum polynomial.

So to prove the impossibility of trisecting a  $60^\circ$  angle by ruler and compass we simply need to compute the minimum polynomial of  $\cos(2\pi/9)$  and to show that its degree is not a power of 2.

**Example 17:** The set  $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$  is a basis for  $\mathbf{Q}[\sqrt[3]{2}]$  over  $\mathbf{Q}$ . Thus a typical element of  $\mathbf{Q}[\sqrt[3]{2}]$  has the form  $x + y\sqrt[3]{2} + z\sqrt[3]{4}$  for some  $x, y, z \in \mathbf{Q}$ .

**Example 18:** Show that the minimum polynomial for  $\sqrt[3]{2} + \sqrt{3}$  over  $\mathbf{Q}$  is

$$x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23.$$

**Solution:** We showed in exercise 4 (v) of the last chapter that  $2^{1/3} + \sqrt{3}$  is a zero of this polynomial so that all that remained was to show that this polynomial is prime over  $\mathbf{Q}$ . Our usual techniques didn't look very promising but now we can now show the primeness of the polynomial by using degrees of field extensions. If  $\alpha = 2^{1/3} + \sqrt{3}$  then  $(\alpha - \sqrt{3})^3 = 2$  and so  $\alpha^3 - 3\alpha^2\sqrt{3} - 9\alpha - 3\sqrt{3} = 2$ . Hence  $\sqrt{3} = \frac{\alpha^3 - 9\alpha - 2}{3\alpha^2 + 3} \in \mathbf{Q}[\alpha]$ . It follows that  $2^{1/3} = \alpha - \sqrt{3} \in \mathbf{Q}[\alpha]$  and so  $\mathbf{Q}[2^{1/3}]$  and  $\mathbf{Q}[\sqrt{3}]$  are subfields of  $\mathbf{Q}[2^{1/3} + \sqrt{3}]$ . The minimum polynomials of  $\sqrt{3}$  and  $2^{1/3}$  over  $\mathbf{Q}$  are clearly  $x^2 - 3$  and  $x^3 - 2$  respectively and so the degrees of  $\mathbf{Q}[\sqrt{3}]$  and  $\mathbf{Q}[2^{1/3}]$  over  $\mathbf{Q}$  are 2 and 3 respectively. Thus, by Theorem 5,  $|\mathbf{Q}[2^{1/3} + \sqrt{3}]:\mathbf{Q}|$  is divisible by both 2 and 3 and hence by 6. So the degree of the minimum polynomial of  $2^{1/3} + \sqrt{3}$  over  $\mathbf{Q}$  is divisible by 6. But the fact that we have found a degree 6 polynomial over  $\mathbf{Q}$  having  $2^{1/3} + \sqrt{3}$  as a zero means that this degree is at most 6. Hence it is exactly 6 and so the polynomial we found is indeed the minimum polynomial.

## True or False Questions

- (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)  $\{a + b\sqrt[3]{2} \mid a, b \in \mathbf{Q}\}$  is a number field.
- (4)  $\mathbf{Q}[\sqrt[3]{8}] = \mathbf{Q}[\sqrt[3]{2}]$ .
- (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  $\mathbf{Q}$ .
- (7)  $\mathbf{Q}[1 + \sqrt[3]{2}] = \mathbf{Q}[\sqrt[3]{4}]$ .
- (8) If  $H, K$  are number fields then  $H \cap K$  a number field.
- (9)  $\{a + b\sqrt[3]{2} \mid a, b \in \mathbf{Q}\}$  is a vector space over  $\mathbf{Q}$ .
- (10)  $|\mathbf{Q}[e^{2\pi i/11}]:\mathbf{Q}| = 11$ .

## Exercises

- (1) Prove that all the zeros of  $x^8 + x^4 + 1$  are in  $\mathbf{Q}[i][\sqrt{3}]$ .
- (2) Prove that  $\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} \mid a, b, c, d \in \mathbf{Q}\}$  is a number field.
- (3) Prove that  $\sqrt{2} \in \mathbf{Q}[i][e^{\pi i/4}]$ .
- (4) Which of the following are quadratic extensions of  $\mathbf{Q}[\sqrt{3}]$  and which are  $\mathbf{Q}[\sqrt{3}]$  itself?
  - (a)  $\mathbf{Q}[\sqrt{3}][\sqrt{12}]$ ;
  - (b)  $\mathbf{Q}[\sqrt{3}][\sqrt{-5 + 7\sqrt{3}}]$ ;
  - (c)  $\mathbf{Q}[\sqrt{3}][\sqrt{7 + 4\sqrt{3}}]$ ;
  - (d)  $\mathbf{Q}[\sqrt{3}][\sqrt{1 + 2\sqrt{3}}]$ .
- (5) Prove that  $x^4 - 4x^2 + 2$  is irreducible over  $\mathbf{Q}$ . Hence or otherwise show that it is the minimum polynomial of  $\sqrt{2 + \sqrt{2}}$ .
- (6) Prove that  $\sqrt{3 + 2\sqrt{2}} \in \mathbf{Q}[\sqrt{2}]$ .
- (7) Prove that  $\sqrt{-1 + 2\sqrt{2}} \notin \mathbf{Q}[\sqrt{2}]$ .
- (8) Find the minimum polynomials of  $\sqrt{3 + 2\sqrt{2}}$  and  $\sqrt{-1 + 2\sqrt{2}}$  over  $\mathbf{Q}$ .
- (9) Find a basis for  $\mathbf{Q}[\sqrt{-1 + 2\sqrt{2}}]$  as a vector space over  $\mathbf{Q}$ .
- (10) Find  $|\mathbf{Q}[2^{1/4} + \sqrt{8}]:\mathbf{Q}|$ .

## Problems

- (1) Find ruler and compass constructions for the inscribed and circumscribed circles for a triangle ABC.
- (2) Find a ruler and compass construction to construct the common tangents (where they exist) to two given circles.
- (3) Find an explicit ruler and compass construction for finding the square root of an arbitrary positive real number  $x$ .
- (4) Find a ruler and compass construction for a regular pentagon.

- (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.
- (6) Investigate the following ruler and compass construction designed to trisect any given angle.  
*To trisect the angle AOB, draw a circle with centre O. Slide the ruler until the length CD is equal to the radius of the circle. The angle DCO is now one third of the angle AOB.*  
 What's wrong with it?
- (8) Prove that the regular heptagon (seven equal sides) is not constructible by ruler and compass.
- (9) Prove that if  $|\mathbb{F}[\alpha]:\mathbb{F}|$  is finite then  $\alpha$  is algebraic over  $\mathbb{F}$ .
- (10) Prove that if  $\mathbb{F}$  is a number field the set of all complex numbers that are algebraic over  $\mathbb{F}$  is also a field.
- (11) Prove that there is no number field  $\mathbb{F}$  such that  $\mathbb{R} < \mathbb{F} < \mathbb{C}$ .

## ANSWERS TO THE TRUE/FALSE QUESTIONS

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

## HINTS TO THE EXERCISES

- (1)  $x^8 + x^4 + 1$  is a quadratic in  $x^4$ .
- (2) Of course you could check it directly, but would Theorem 9 help to simplify things?
- (3)  $e^{2\pi i/4} = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ .
- (4) In other words, which of the following are the square of an element in  $\mathbb{Q}[\sqrt{3}]$ :  
 $12, -5 + 7\sqrt{3}, 7 + 4\sqrt{3}, 1 + 2\sqrt{3}$  ?
- (5) If it factorises over  $\mathbb{Q}$ , it does so over  $\mathbb{Z}_3$ .
- (6) If  $\sqrt{3 + 2\sqrt{3}} = a + b\sqrt{2}$  what must  $a, b$  be?

(7) Suppose  $\sqrt{-1 + 2\sqrt{2}} = a + b\sqrt{2}$

(8) Do exercises 6, 7 and Theorems 7 and 10 tell you anything about the degree of the minimum polynomials?

(9) The first thing to do is to work out the dimension.

(10)  $\sqrt[4]{8} \in \mathbf{Q}[2^{1/4}]$

## HINTS TO THE PROBLEMS

(1) The centre of the inscribed circle is the common intersection of the perpendicular bisectors of the sides. And the centre of the circumscribed circle is the common intersection of .....

(2) Construct a right-angled triangle whose hypotenuse is the interval joining the centres and which has, as one of its sides, the difference between the radii.

(3) Use the identity  $x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$  and construct a circle with diameter  $\frac{x+1}{2}$  and draw a suitable right-angled triangle in this semicircle.

(4) If  $x = 2\cos(2\pi/5)$  show that  $x^4 - 3x^2 + 1 = 0$ . Now solve this to find  $x$ .

(5) What is the minimum polynomial of  $2^{1/3}$  over  $\mathbf{Q}$ ?

(6) Join OD.

(7) By Theorem 8 there is a number field containing  $x, y$  whose dimension over  $\mathbf{Q}$  is a power of 2. But it might not contain  $i$ . So ...

(8) Show that the degree of  $e^{2\pi i/7}$  is 6 and use problem 7.

(9) Use Theorems 6 and 9.

(10) If  $\alpha, \beta$  are algebraic over  $F$  consider  $F[\alpha, \beta]$  and use problem 9.

(11) No hints!

(12) Prove that  $e^{2\pi i k}$  and  $e^{-2\pi i k}$  are algebraic over  $\mathbf{Q}$  and use problem 10.