of this point) can be constructed (so then $\sin\theta$ can also be constructed). Conversely if $\cos\theta$, then $\sin\theta$, can be constructed, the point with those coordinates gives the angle θ.

The problem of trisecting the angle θ is then equivalent to the problem: given $\cos\theta$ construct $\cos\theta/3$.

To see that this is not always possible (it is certainly occasionally possible, for example for $\theta = 180°$), consider $\theta = 60°$. Then $\cos\theta = \frac{1}{2}$. By the triple angle formula for cosines:

$$\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3,$$

substituting $\theta = 60°$, we see that $\beta = \cos 20°$ satisfies the equation

$$4\beta^3 - 3\beta - 1/2 = 0$$

or $8(\beta)^3 - 6\beta - 1 = 0$. This can be written $(2\beta)^3 - 3(2\beta) - 1 = 0$. Let $\alpha = 2\beta$. Then α is a real number between 0 and 2 satisfying the equation

$$\alpha^3 - 3\alpha - 1 = 0.$$

But we considered this equation in the last section and determined $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and as before we see that α is not constructible.

(III) Squaring the circle is equivalent to determining whether the real number $\pi = 3.14159\ldots$ is constructible. As mentioned previously, it is a difficult problem even to prove that this number is not rational. It is in fact transcendental (which we shall assume without proof), so that $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is not even finite, much less a power of 2, showing the impossibility of squaring the circle by straightedge and compass.

Remark: The proof above shows that $\cos 20°$ and $\sin 20°$ cannot be constructed. The question arises as to which integer angles (measured in degrees) are constructible? The angles $1°$ and $2°$ are not constructible, since otherwise the addition formulae for sines and cosines would give the constructibility for $20°$. On the other hand, elementary geometric constructions (of the regular 5-gon for an angle of $72°$ and the equilateral triangle for an angle of $60°$) together with the addition formulae and the half-angle formulae show that $\cos 3°$ and $\sin 3°$ are constructible. It follows from this that the trigonometric functions of an integer degree angle are constructible precisely when the angle is a multiple of $3°$. Explicitly,

$$\cos 3° = \frac{1}{8}(\sqrt{3}+1)\sqrt{5+\sqrt{5}} + \frac{1}{16}(\sqrt{6}-\sqrt{2})(\sqrt{5}-1)$$
$$\sin 3° = \frac{1}{16}(\sqrt{6}+\sqrt{2})(\sqrt{5}-1) - \frac{1}{8}(\sqrt{3}-1)\sqrt{5+\sqrt{5}},$$

showing that these are obtained from $\mathbb{Q}$ by successive extractions of square roots and field operations.

After discussing the cyclotomic fields in Section 14.5 we shall consider another classical geometric question: "which regular n-gons can be constructed by straightedge and compass?" (cf. Proposition 14.29).

We have been careful here to consider constructions using a *straightedge* rather than a *ruler*, the distinction being that a ruler has marks on it. If one uses a ruler, it is possible to construct many additional algebraic elements. For example, suppose θ is a given angle and the unit distance 1 is marked on the ruler. Draw a circle of radius 1 with central angle θ as shown in Figure 3 and then slide the ruler until the distance between points A and B on the circle is 1. Then some elementary geometry shows that (cf. the exercises) the angle α indicated is $\theta/3$, i.e., this construction (due to Archimedes) trisects θ. In particular, the second classical problem in Theorem 24 (Trisecting an Angle) can be solved with *ruler* and compass.

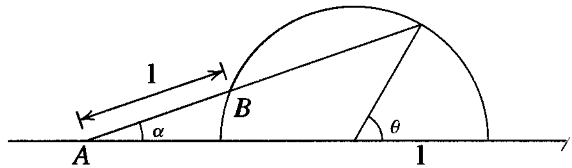

Fig. 3

The first of the classical problems in Theorem 24 (Duplication of the Cube), which amounts to the construction of $\sqrt[3]{2}$, can also be solved with ruler and compass. The following gives a construction for $k^{1/3}$ for any given positive real k which is less than 1. This construction was shown to us by J.H. Conway.

Drawing a circle of radius 1 and using the point $A = (k, 0)$ as center, construct the point $B = (0, \sqrt{1-k^2})$. Dividing this distance by 3, construct the point $(0, -\frac{1}{3}\sqrt{1-k^2})$ and draw the line connecting this point with A. Slide the ruler with marked unit length 1 so that it passes through the point B and so that the distance from the intersection point C to the intersection point D with the x-axis is of length 1, as indicated in Figure 4.

Then the distance between A and D is $2k^{1/3}$ and the distance between B and C is $2k^{2/3}$ (cf. the exercises).

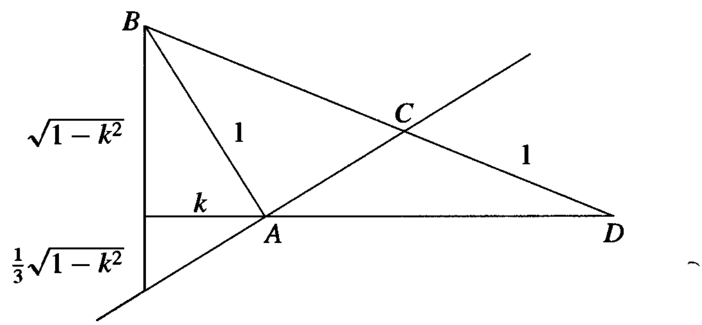

Fig. 4

EXERCISES

1. Prove that it is impossible to construct the regular 9-gon.
2. Prove that Archimedes' construction actually trisects the angle θ. [Note the isosceles triangles in Figure 5 to prove that $\beta = \gamma = 2\alpha$.]

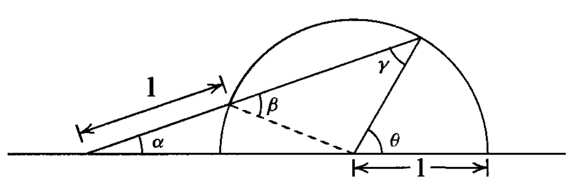

Fig. 5

3. Prove that Conway's construction indicated in the text actually constructs $2k^{1/3}$ and $2k^{2/3}$. [One method: let (x, y) be the coordinates of the point C, a the distance from B to C and b the distance from A to D; use similar triangles to prove (a) $\dfrac{y}{1} = \dfrac{\sqrt{1-k^2}}{1+a}$, (b) $\dfrac{x}{a} = \dfrac{b+k}{1+a}$, (c) $\dfrac{y}{x-k} = \dfrac{\sqrt{1-k^2}}{3k}$, and also show that (d) $(1-k^2)+(b+k)^2 = (1+a)^2$; solve these equations for a and b.]
4. The construction of the regular 7-gon amounts to the constructibility of $\cos(2\pi/7)$. We shall see later (Section 14.5 and Exercise 2 of Section 14.7) that $\alpha = 2\cos(2\pi/7)$ satisfies the equation $x^3 + x^2 - 2x - 1 = 0$. Use this to prove that the regular 7-gon is not constructible by straightedge and compass.
5. Use the fact that $\alpha = 2\cos(2\pi/5)$ satisfies the equation $x^2 + x - 1 = 0$ to conclude that the regular 5-gon is constructible by straightedge and compass.

13.4 SPLITTING FIELDS AND ALGEBRAIC CLOSURES

Let F be a field.

If $f(x)$ is any polynomial in $F[x]$ then we have seen in Section 2 that there exists a field K which can (by identifying F with an isomorphic copy of F) be considered an extension of F in which $f(x)$ has a root α. This is equivalent to the statement that $f(x)$ has a linear factor $x - \alpha$ in $K[x]$ (this is Proposition 9 of Chapter 9).

Definition. The extension field K of F is called a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (or *splits completely*) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

If $f(x)$ is of degree n, then $f(x)$ has at most n roots in F (Proposition 17 of Chapter 9) and has precisely n roots (counting multiplicities) in F if and only if $f(x)$ splits completely in $F[x]$.

Theorem 25. For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting field for $f(x)$.

Proof: We first show that there is an extension E of F over which $f(x)$ splits completely into linear factors by induction on the degree n of $f(x)$. If $n = 1$, then take $E = F$. Suppose now that $n > 1$. If the irreducible factors of $f(x)$ over F are all of degree 1, then F is the splitting field for $f(x)$ and we may take $E = F$. Otherwise, at least one of the irreducible factors, say $p(x)$ of $f(x)$ in $F[x]$ is of degree at least 2. By Theorem 3 there is an extension E_1 of F containing a root α of $p(x)$. Over E_1 the polynomial $f(x)$ has the linear factor $x - \alpha$. The degree of the remaining factor $f_1(x)$ of $f(x)$ is $n - 1$, so by induction there is an extension E of E_1 containing all the roots of $f_1(x)$. Since $\alpha \in E$, E is an extension of F containing all the roots of $f(x)$. Now let K be the intersection of all the subfields of E containing F which also contain all the roots of $f(x)$. Then K is a field which is a splitting field for $f(x)$.

We shall see shortly that any two splitting fields for $f(x)$ are isomorphic (which extends Theorem 8), so (by abuse) we frequently refer to *the* splitting field of a polynomial.

Definition. If K is an algebraic extension of F which is the splitting field over F for a collection of polynomials $f(x) \in F[x]$ then K is called a *normal* extension of F.

We shall generally use the term "splitting field" rather than "normal extension" (cf. also Section 14.9).

Examples

(1) The splitting field for $x^2 - 2$ over $\mathbb{Q}$ is just $\mathbb{Q}(\sqrt{2})$, since the two roots are $\pm\sqrt{2}$ and $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

(2) The splitting field for $(x^2 - 2)(x^2 - 3)$ is the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ generated over $\mathbb{Q}$ by $\sqrt{2}$ and $\sqrt{3}$ since the roots of the polynomial are $\pm\sqrt{2}$, $\pm\sqrt{3}$. We have already seen that this is an extension of degree 4 over $\mathbb{Q}$ and we have the following diagram of known subfields:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

(3) The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is not just $\mathbb{Q}(\sqrt[3]{2})$ since as previously noted the three roots of this polynomial in $\mathbb{C}$ are

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\left(\frac{-1 + i\sqrt{3}}{2}\right), \quad \sqrt[3]{2}\left(\frac{-1 - i\sqrt{3}}{2}\right)$$

and the latter two roots are not elements of $\mathbb{Q}(\sqrt[3]{2})$, since the elements of this field are of the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with rational a, b, c and all such numbers are real.

The splitting field K of this polynomial is obtained by adjoining all three of these roots to $\mathbb{Q}$. Note that since K contains the first two roots above, then it contains their quotient $\dfrac{-1 + \sqrt{-3}}{2}$ hence K contains the element $\sqrt{-3}$. On the other hand, any field containing $\sqrt[3]{2}$ and $\sqrt{-3}$ contains all three of the roots above. It follows that

$$K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

is the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Since $\sqrt{-3}$ satisfies the equation $x^2 + 3 = 0$, the degree of this extension over $\mathbb{Q}(\sqrt[3]{2})$ is at most 2, hence must be 2 since we observed above that $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field. It follows that

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = 6.$$

Note that we could have proceeded slightly differently at the end by noting that $\mathbb{Q}(\sqrt{-3})$ is a subfield of K, so that the index $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$ divides $[K : \mathbb{Q}]$.