APPENDIX 1

THE INSOLUBILITY OF SOME GEOMETRIC CONSTRUCTION PROBLEMS

In this appendix we show that the problems of doubling the cube, trisecting an arbitrary angle, and producing the side of a regular heptagon cannot be solved using Euclidean tools.

We begin by introducing the notion of a *constructible* real number. Start with two points in the Cartesian plane at unit distance apart: for convenience we may take these to be the points (0, 0) and (1, 0) on the x-axis. A real number α is said to be *constructible* if the point $(\alpha, 0)$ is obtainable from the given points (0, 0) and (1, 0) by means of a finite number of applications of straightedge and compasses, subject to the Euclidean rules (see Chapter 2 for these). It is easily shown—and we leave this as an exercise to the reader—that if α and β are constructible numbers, so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and, if $\beta \neq 0$, α/β. Accordingly the set of constructible numbers forms a *field*.

We now prove the

Lemma. Suppose that F is a field of real numbers. Let k be a positive member of F such that $\sqrt{k}$ is not in F. Then the set $F(\sqrt{k})$ consisting of all numbers of the form $\alpha + \beta\sqrt{k}$ with α, β in F is also a field, called a *quadratic extension* of F.

Proof. It is clearly enough to show that, if $x \in F(\sqrt{k})$ and $x \neq 0$, then $1/x \in F(\sqrt{k})$. To this end suppose that $x = \alpha + \beta\sqrt{k}$, with $\alpha, \beta \in F$. If $x \neq 0$, then also $\alpha \neq 0$ or $\beta \neq 0$, and so $\alpha^2 - \beta^2 k \neq 0$. Hence

$$\frac{1}{x} = \frac{1}{\alpha + \beta\sqrt{k}} = \frac{\alpha - \beta\sqrt{k}}{(\alpha + \beta\sqrt{k})(\alpha - \beta\sqrt{k})} = \frac{\alpha^2}{\alpha^2 - \beta^2 k} - \frac{\beta\sqrt{k}}{\alpha^2 - \beta^2 k}$$

and this last quantity is clearly a member of F. This proves the lemma.

A *quadratic surd* is a real number which can be obtained in a finite number of steps from the numbers 0 and 1 using only the operations $+, \times, -, \div$ and the extraction of square roots. It is clear that the quadratic surds form a field. Moreover, it is quickly seen that a given real number a is a quadratic surd if and only if we can find a finite sequence of fields $F_0, F_1, \ldots, F_n$, which we call a *formation sequence* for a, such that $a \in F_n$, F_0 is the field $\mathbb{Q}$ of rational numbers, and each F_i is a quadratic extension of F_{i-1}. For example, if

$$a = \sqrt{2} + \sqrt{3} + \sqrt{5}$$

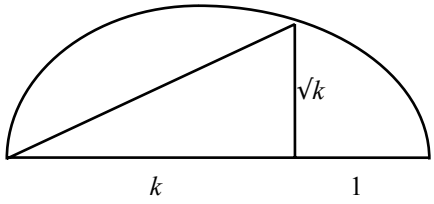
then F_0, F_1, F_2, F_3, F_4 *is* a formation sequence for a, where

$$F_0 = \mathbb{Q},\ F_1 = \mathbb{Q}(\sqrt{2}),\ F_2 = F_1(\sqrt{3}),\ F_3 = F_2(\sqrt{5}),\ F_4 = F_3(\sqrt{2} + \sqrt{3} + \sqrt{5}).$$

We can now prove the crucial

Theorem. The constructible numbers are precisely the quadratic surds.

Proof. The field $\mathbb{Q}$ of rational numbers obviously consists of constructible numbers. Moreover, if k is constructible, so is $\sqrt{k}$, as can be seen from the diagram below:



It follows that, if F is a field of constructible numbers, then each quadratic extension of F also consists of constructible numbers. Now let a be a quadratic surd, and let $F_0, \ldots, F_n$ be a formation sequence for a. Then $F_0 = \mathbb{Q}$ consists of constructible numbers, and so therefore do $F_1, \ldots, F_n$. Thus a, as a member of F_n, must be constructible.

To prove the converse, we observe that, if F is any field of real numbers, the points of intersection of lines and circles of F have coordinates which are members of some quadratic extension of F. (Here a *line of F* is any line passing through two points whose coordinates are in F, and a *circle of F* any circle whose centre has coordinates in F, and the length of whose radius is in F.) To prove this, notice that the coordinates (x, y) of such points of intersection are obtained by solving two simultaneous equations, each of which has one of the forms

$$\alpha x + \beta y + \gamma = 0 \qquad x^2 + y^2 + \varepsilon x + \eta y + \zeta = 0,$$

where $\alpha, \beta, \gamma, \varepsilon, \eta, \zeta$ are all members of F. By solving these equations explicitly for x and y we see immediately that they will both be members of some quadratic extension of F. Thus, starting with the points (0, 0) and (1, 0), straightedge and compass constructions can lead only to points whose coordinates lie in members of some sequence $F_0, F_1, \ldots, F_n$, with $F_0 = \mathbb{Q}$ and each F_i a quadratic extension of F_{i-1}. Accordingly each constructible number is a quadratic surd, and the theorem is proved.

Now we can show that *doubling the cube* cannot be performed with Euclidean tools. Taking the given cube to have side of unit length, the cube with double the

volume will have side $\sqrt[3]{2}$. Thus we must show that this number is not constructible; by the theorem above this is tantamount to showing that it is not a quadratic surd. In fact we shall prove the ostensibly[1] stronger result that *no solution to the equation* $x^3 - 2 = 0$ *can be a quadratic surd.*

For suppose that a solution x to the equation $x^3 - 2 = 0$ were a quadratic surd, and let $F_0, ..., F_n$ be a formation sequence for x. Since (as is easily shown) $\sqrt[3]{2}$ is irrational, it cannot be a member of $F_0 = \mathbb{Q}$, and so n must be positive. Now assume that n is as small as it can be; thus x is in F_n but not in F_{n-1}. Now there is a member w of F_{n-1} such that $\sqrt{w}$ is not in F_{n-1} and $F_n = F_{n-1}(\sqrt{w})$, so that

$$x = p + q\sqrt{w},$$

for some $p, q \in F_{n-1}$.

We next show that, if $x = p + q\sqrt{w}$ is a solution of $x^3 - 2 = 0$, then so is $y = p - q\sqrt{w}$. For since x is in F_n, it follows that $x^3 - 2$ is also in F_n, and so

$$x^3 - 2 = a + b\sqrt{w}, \tag{1}$$

with $a, b \in F_{n-1}$. By substituting for x, and recalling that $\sqrt{w}$ is not in F_{n-1}, we easily find

$$a = p^3 + 3p^2qw - 2,$$
$$b = 3p^2q + q^3w.$$

Now put $y = p - q\sqrt{w}$. Then a substitution of $-q$ for q in the expressions for a and b above gives

$$y^3 - 2 = a - b\sqrt{w}.$$

Now x was assumed to satisfy $x^3 - 2 = 0$, so, by (1), we must have $a + b\sqrt{w} = 0$. But since $\sqrt{w} \notin F_{n-1}$, it follows that $a = b = 0$. (For if $b \neq 0$, then $\sqrt{w} = a/b$ which is a member of F_{n-1}. So $b = 0$ and $a = -b\sqrt{w} = 0$.) Therefore

$$y^3 - 2 = a - b\sqrt{w} = 0,$$

so that y is also a solution to $x^3 - 2 = 0$, as claimed.

Since $q \neq 0$ (for otherwise $x = p + q\sqrt{w}$ would be in F_{n-1}), it follows that x and y are distinct, so that the equation $x^3 - 2 = 0$ would have *two* real roots. But this contradicts the fact, evident from graphical considerations, that this equation has *only one* real root. This contradiction shows that our original assumption that the equation has a solution

[1]Only ostensibly stronger since it is easily seen that the equation $x^3 - 2 = 0$ has only the one real root $\sqrt[3]{2}$; the other roots, being complex numbers, by definition cannot be quadratic surds.

which is a quadratic surd was incorrect, and we conclude from this that the doubling of the cube cannot be carried out with Euclidean tools.

We now turn to the problem of *trisecting an arbitrary angle*. Here it is simplest to regard an angle as given by its *cosine*: $g = \cos\theta$. Thus the problem of trisecting θ is equivalent to finding the quantity $x = \cos\theta/3$. From trigonometry one knows that

$$\cos\theta = g = 4\cos^3(\theta/3) - 3\cos(\theta/3),$$

and so the problem of trisecting an angle θ given by $\cos\theta = g$ with Euclidean tools amounts to constructing a solution to the cubic equation

$$4z^3 - 3z - g = 0.$$

To show that this cannot be done in general, we take θ to be 60°, so that $g = \frac{1}{2}$. The above equation then becomes

$$8z^3 - 6z - 1 = 0. \tag{2}$$

We show that this equation has no solution which is a quadratic surd. To do this we need a general

Lemma. If a cubic equation with rational coefficients has no rational root, it has no root which is a quadratic surd.

Proof. Let the given equation be

$$z^3 + az^2 + bz + c = 0,$$

with *a, b, c* rational. It is a well known—and easily established—algebraic fact that the roots x_1, x_2, x_3 of such an equation themselves satisfy the relation

$$x_1 + x_2 + x_3 = -a. \tag{3}$$

Now suppose that the given cubic equation has no rational root, but does have at least one root which is a quadratic surd. Such a root will have a formation sequence $F_0, \ldots, F_n$. Let n be the least length of a formation sequence in which a quadratic surd root x to the equation can be found in its last member F_n: then n must be positive since the equation has no rational roots (recall that $F_0 = \mathbb{Q}$). The root x can be written in the form

$$x = p + q\sqrt{w},$$

with *p, q, w,* but not $\sqrt{w}$, in F_{n-1}. As before, one shows that

$$y = p - q\sqrt{w}$$

is also a root. But then, by (3), the third root u satisfies

$$u = -a - x - y.$$

Since $x + y = 2p$, it follows that

$$u = -a - 2p.$$

Since $-a - 2p \in F_{n-1}$, so also, therefore, is u. Thus the root u lies in the last member F_{n-1} of a formation sequence of length $n - 1$, contradicting the choice of n as the least such number. This contradiction shows that our supposition above was mistaken, and the Lemma is proved.

Next, we show that equation (2) has no quadratic surd root. By the Lemma, this reduces to showing that it has no rational roots. To this end, put $v = 2z$. Then (2) becomes

$$v^3 - 3v = 1. \tag{4}$$

Suppose that (4) had a rational solution of the form $v = r/s$, where we may assume that r and s have no common factors. Then

$$r^3 - 3s^2r = s^3.$$

Therefore

$$s^3 = r(r^2 - 3s^2)$$

is divisible by r, which means that r and s have a common factor, contrary to assumption, unless $r = \pm 1$. Likewise, s^2 is a factor of

$$r^3 = s^2(s + 3r),$$

which means that r and s again have a common factor unless $s = \pm 1$. Thus 1 and -1 are the only rational numbers which could satisfy the equation. But it is clear that neither of these satisfies it, so that no rational satisfies it, and we are done.

Finally, we turn to the problem of constructing the side of a regular heptagon, which we may take as being inscribed in the unit circle in the complex plane. If each vertex has coordinates x, y, then we know that $z = x + iy$ is a root of the equation $z^7 - 1 = 0$. One root of this equation is $z = 1$, and the others are the roots of the equation

$$(z^7 - 1)/(z - 1) = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0.$$

Dividing this by z^3, we obtain the equation

$$z^3+1/z^3+z^2+1/z^2+z+1/z+1=0.$$

This may be written in the form

$$(z+1/z)^3+(z+1/z)^2-2(z+1/z)-1=0.$$

Writing y for $z+1/z$, this last equation becomes

$$y^3+y^2-2y-1=0. \tag{5}$$

Now we have seen in Chapter 3 that z, the seventh root of unity, is given by $z = \cos\theta + i\sin\theta$, where $\theta = 360°/7$. We also know that $1/z = \cos\theta - i\sin\theta$, so that $y = z + 1/z = 2\cos\theta$. It follows that the constructibility of y is equivalent to that of $\cos\theta$. Accordingly, if we can show that y is not constructible, we will also have shown that z, and so also the side of the heptagon, is not constructible. By the theorem and the second lemma above, to do this we need merely show that equation (5) has no rational roots. So suppose that r/s were a rational root of (5), with r and s possessing no common factor. Substitution into (5) then gives

$$r^3+r^2s-2rs^2-s^3=0,$$

and, as above, it follows that r^3 is divisible by s, and s^3 by r. Since r and s have no common factor, each must be ±1, so that $y = \pm1$ likewise. But neither of these values of y satisfies (5). Therefore (5) has no rational roots and we are finished.