Chapter 19

Regular Polygons

We return with more sophisticated weapons to the time-honoured problem of ruler-and-compass construction. We shall consider the following question: for which values of n can the regular n-sided polygon be constructed by ruler and compasses?

The ancient Greeks knew of constructions for 3-, 5-, and 15-gons; they also knew how to construct a $2n$-gon given an n-gon, by the obvious method of bisecting the angles. We describe these constructions in Section 19.1. For about 2000 years little progress was made beyond the Greeks. If you answered Example 7.13, then you will have got further than they did. It seemed obvious that the Greeks had found all the constructible regular polygons ... Then, on 30 March 1796, Gauss made the remarkable discovery that the regular 17-gon can be constructed (Figure 19.1). He was 19 years old at the time. So pleased was he with this discovery that he resolved to dedicate the rest of his life to mathematics, having until then been unable to decide between that and the study of languages. In his *Disquisitiones Arithmeticae*, reprinted as Gauss (1966), he stated necessary and sufficient conditions for constructibility of the regular n-gon, and proved their sufficiency; he claimed to have a proof of necessity although he never published it. Doubtless he did; Gauss knew a proof when he saw one.

19.1 What Euclid Knew

Euclid's *Elements* gets down to business straight away. The first regular polygon constructed there is the equilateral triangle, in Book 1 Proposition 1. Figure 19.2 makes the construction fairly clear.

The square also makes its appearance in Book 1:

PROPOSITION 19.1 (Euclid)
On a given straight line to describe a square.

In the proof, which we give in detail to illustrate Euclid's style, notation such as [1,31] refers to Proposition 31 of Book 1 of the Elements. *The proof is taken from Heath (1956), the classic edition of Euclid's* Elements. *Refer to Figure 19.3 for the lettering.*

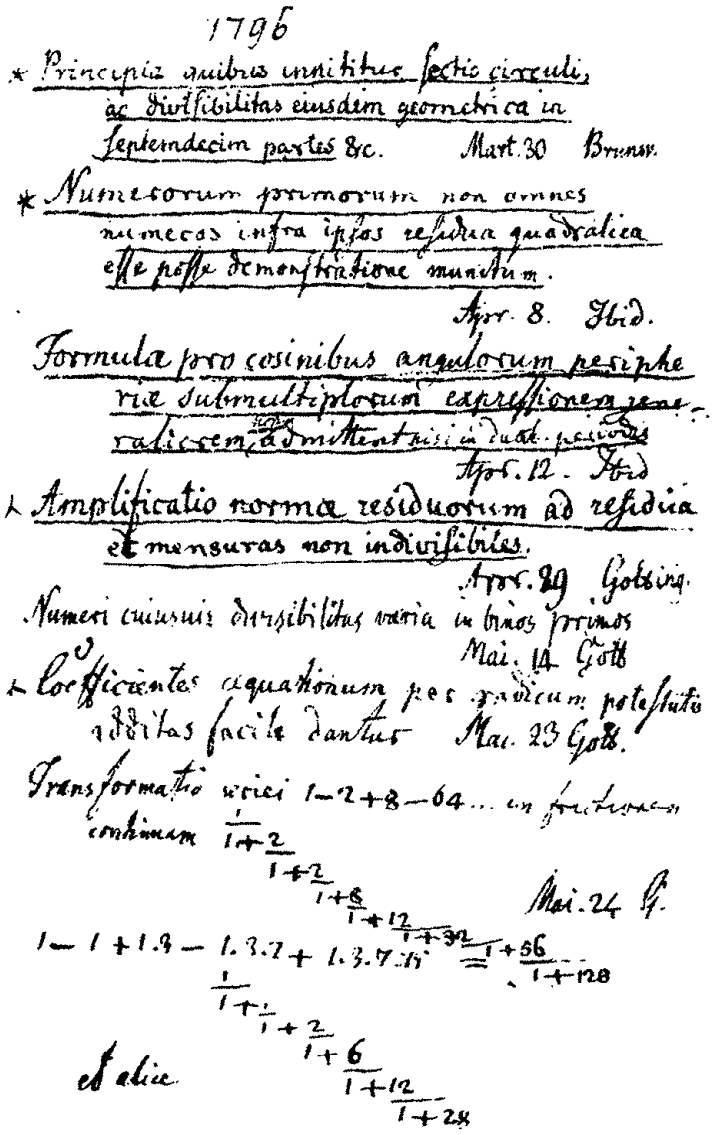

Figure 19.1: The first entry in Gauss's notebook records his construction of the regular 17-gon.

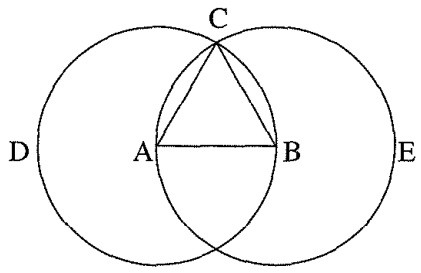

Figure 19.2: Euclid's construction of an equilateral triangle.

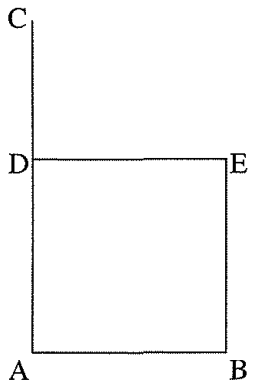

Figure 19.3: Euclid's construction of a square.

PROOF Let AB be the given straight line; thus it is required to describe a square on the straight line AB.

Let AC be drawn at right angles to the straight line AB from the point A on it [1, 11], and let AD be made equal to AB; through the point D let DE be drawn parallel to AB, and through the point B let BE be drawn parallel to AD [1,31].

Therefore, ADEB is a parallelogram; therefore, AB is equal to DE, and AD to BE [1, 34]. But AB is equal to AD; therefore, the four straight lines BA, AD, DE, EB are equal to one another; therefore, the parallelogram ADEB is equilateral.

I say next that it is also right-angled. For, since the straight line AD falls upon the parallels AB, DE, the angles BAD, ADE are equal to two right angles [1, 29].

But the angle BAD is also right; therefore, the angle ADE is also right.

And in parallelogrammic areas the opposite sides and angles are equal to one another [1, 34]; therefore, each of the opposite angles ABE, BED is also right. Therefore, ADEB is right-angled. And it was also proved equilateral. Therefore, it is a square; and it is described on the straight line AB. Q.E.F. □

Here Q.E.F. (*quod erat faciendum* — that which was to be done) replaces the familiar Q.E.D. (*quod erat demonstrandum* — that which was to be proved) because this is not a theorem but a construction. In any case, the Latin arises in later translations; Euclid wrote in Greek. Now imagine you are a Victorian schoolboy — it always *was* a schoolboy in those days — trying to learn Euclid's proof by heart, including the exact choice of letters in the diagrams.

The construction of the regular pentagon has to wait until Book 4 Proposition 11, because it depends on some quite sophisticated ideas, notably Proposition 10 of Book 4: *To construct an isosceles triangle having each of the angles at the base double of the remaining one.* In modern terms, construct a triangle with angles $4\pi/5$, $4\pi/5$, $2\pi/5$. Euclid's method for doing this is shown in Figure 19.4. Given AB, find C so that $AB \times BC = CA^2$. To do that, see Book 2 Proposition 11, which is itself quite complicated — the construction here is essentially the famous "golden section," a name that seems to have been introduced in 1835 by Martin Ohm (Herz-Fischler, 1998; Livio, 2002). Euclid's method is given in Exercise 19.10. Next, draw the circle centre

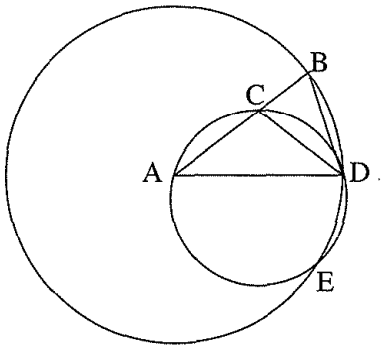

Figure 19.4: Euclid's construction of an isosceles triangle with base angles $4\pi/5$.

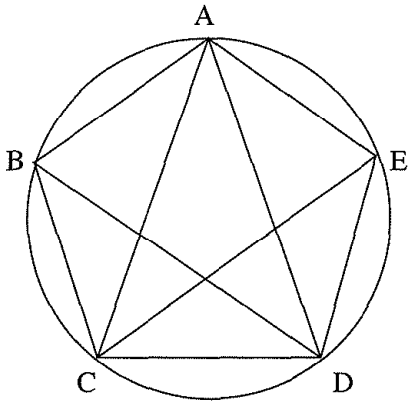

Figure 19.5: Euclid's construction of a regular pentagon. Make ACD similar to triangle ABD in Figure 19.4, and proceed from there.

A radius AB, and find D such that BD = AC. Then triangle ABD is the one required.

With this triangle shape under his belt, Euclid then constructs the regular pentagon. Figure 19.5 makes his method clear.

The hexagon occurs in Book 4 Proposition 15, the 15-gon in Book 4 Proposition 16. Bisection of any angle, Book 1 Proposition 9, effectively completes the Euclidean catalogue of constructible regular polygons.

19.2 Which Constructions are Possible?

That, however, was not the end of the story.

In order to obtain necessary and sufficient conditions for the existence of a ruler-and-compass construction, we must prove a more detailed theorem than Theorem 4. This requires a careful examination of which constructions are possible.

LEMMA 19.2
If P is a subset of $\mathbb{R}^2$ containing the points $(0, 0)$ and $(1, 0)$, then the point (x, y) can be constructed from P whenever x and y lie in the subfield of $\mathbb{R}$ generated by the coordinates of points in P.

PROOF Given any point (x_0, y_0) it is obvious how to construct $(0, x_0)$ and $(0, y_0)$. From $(0, 0)$ and $(1, 0)$ we can construct the coordinate axes, and then proceed as in Figure 19.6.

If we are given $(0, x_0)$ and $(0, y_0)$, then the same construction in reverse gives (x_0, y_0). Thus to prove the lemma it is sufficient to show that given $(0, x)$ and $(0, y)$ we can construct $(0, x + y)$, $(0, x - y)$, $(0, xy)$, and $(0, x/y)$ when $y \neq 0$. The first two are obvious. If we swing arcs of radius y centre $(0, x)$, they cut the y-axis at $(0, x+y)$ and $(0, x-y)$. For the other two points we proceed as follows. Join $(1, 0)$ to $(0, y)$ and draw a line parallel to this through $(0, x)$ (see Exercise 19.1). This line cuts the x-axis at $(u, 0)$. By similar triangles $u/x = 1/y$, so that $u = x/y$. Taking $x = 1$ (the point (0,1) is clearly constructible) we can construct $(1/y, 0)$, hence $(0, 1/y)$; by taking $1/y$ instead of y, we get $(xy, 0)$. From these we can find $(0, xy)$ and $(0, x/y)$. See Figure 19.7. □

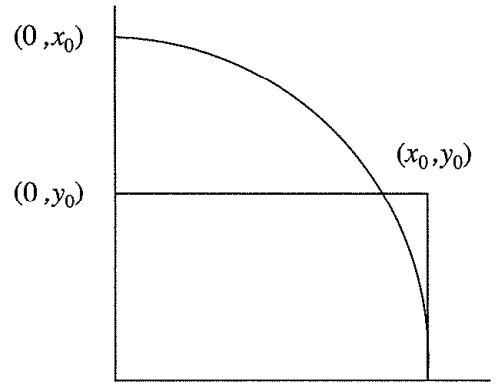

Figure 19.6: Constructing $(0, x_0)$ and $(0, y_0)$ from (x_0, y_0).

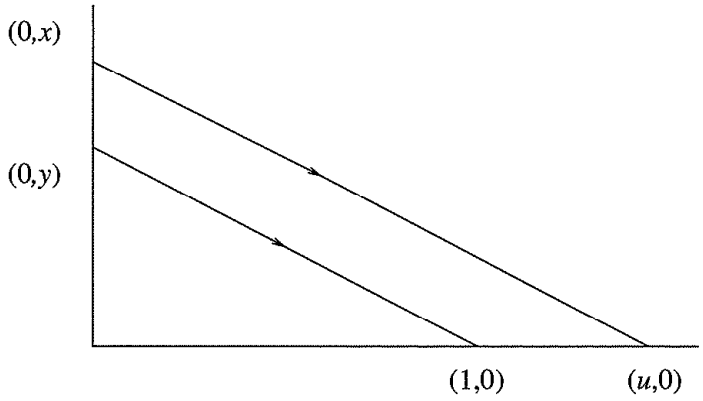

Figure 19.7: Constructing $u = x/y$.

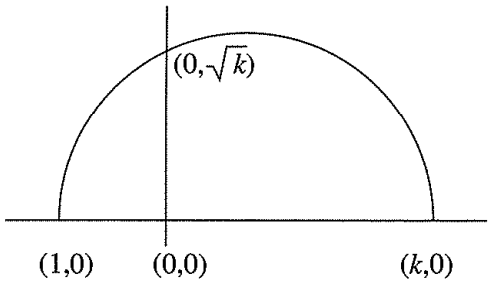

Figure 19.8: Constructing $\sqrt{k}$.

LEMMA 19.3
Suppose that $K(\alpha) : K$ is an extension of degree 2 such that $K(\alpha) \subseteq \mathbb{R}$. Then any point (z, w) of $\mathbb{R}^2$ whose coordinates z, w lie in $K(\alpha)$ can be constructed from some suitable finite set of points whose coordinates lie in K.

PROOF We have $\alpha^2 + p\alpha + q = 0$, where $p, q \in K$. Hence

$$\alpha = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

and since $K(\alpha) \subseteq R$ then $p^2 - 4q$ must be positive. Using Lemma 2 the result will follow if we can construct $(0, \sqrt{k})$ for any positive $k \in K$ from finitely many points (x_r, y_r) where $x_r, y_r \in K$. To do this, construct $(-1, 0)$ and $(k, 0)$. Draw the semicircle with these points as the ends of a diameter, meeting the y-axis at $(0, v)$. By the intersecting chords theorem, $v^2 = 1 \cdot k$ so that $v = \sqrt{k}$ (see Figure 19.8). □

THEOREM 19.4
Suppose that K is a subfield of $\mathbb{R}$ generated by the coordinates of points in a subset $P \subseteq \mathbb{R}^2$. Let α, β lie in an extension L of K, contained in $\mathbb{R}$, such that there exists a finite series of subfields

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$$

such that $[K_{j+1} : K_j] = 2$ for $j = 0, \ldots, r-1$. Then the point (α, β) is constructible from P.

PROOF Use induction on r. The case $r = 0$ is covered by Lemma 19.2. Otherwise, (α, β) is constructible from finitely many points whose coordinates lie in K_{r-1} by Lemma 19.3. By induction, these points are constructible from P, so (α, β) is constructible from P. □

From the proof of Theorem 19.4, the existence of such fields K_i is also a necessary condition for (α, β) to be constructible from P.

There is a more useful, but weaker, version of Theorem 19.4. To prove it, we first need:

LEMMA 19.5
If G is a finite group and $|G| = 2^r$, then $Z(G)$ contains an element of order 2.

PROOF Use the class equation (14.2). We have

$$1 + C_2 + \cdots + C_k = 2^r$$

so some C_j is odd. By Corollary 14.12 this C_j also divides 2^r, so we must have $|C_j| = 1$. Hence $Z(G) \neq 1$. Now apply Lemma 14.14. □

COROLLARY 19.6
If G is a finite group and $|G| = 2^r$, then there exists a series of normal subgroups

$$1 = G_0 \subseteq \cdots \subseteq G_r = G$$

such that $|G_j| = 2^j$ for $0 \leq j \leq r$.

PROOF Use Lemma 19.5 and induction. □

Now we can state and prove the promised modification of Theorem 19.4.

PROPOSITION 19.7
If K is a subfield of $\mathbb{R}$, generated by the coordinates of points in a subset $P \subseteq \mathbb{R}^2$, and if α and β lie in a normal extension L of K such that $L \subseteq \mathbb{R}$ and $[L : K] = 2^r$ for some integer r, then (α, β) is constructible from P.

PROOF $L : K$ is separable since the characteristic is zero. Let G be the Galois group of $L : K$. By Theorem 12.1(1) $|G| = 2^r$, so G is a 2-group. By Corollary 19.6, G has a series of normal subgroups

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$$

such that $|G_j| = 2^j$. Let K_j be the fixed field $G_{r-j}^{\dagger}$. Then by Theorem 12.1(3) $[K_{j+1} : K_j] = 2$ for all j. By Theorem 19.4, (α, β) is constructible from P. □

19.3 Regular Polygons

We shall use a mixture of algebraic and geometric ideas to find those values of n for which the regular n-gon is constructible. To save breath, let us make the following (nonstandard):

DEFINITION 19.8 *The positive integer n is* constructive *if the regular n-gon is constructible by ruler and compasses.*

The first step is to reduce the problem to prime-power values of n.

LEMMA 19.9
If n is constructive and m divides n, then m is constructive. If m and n are coprime and constructive, then mn is constructive.

PROOF If m divides n, then we can construct a regular m-gon by joining every dth vertex of a regular n-gon, where $d = n/m$.

If m and n are coprime, then there exist integers a, b such that $am + bn = 1$. Therefore,

$$\frac{1}{mn} = a\frac{1}{n} + b\frac{1}{m}$$

Hence from angles $2\pi/m$ and $2\pi/n$ we can construct $2\pi/mn$, and from this we obtain a regular mn-gon. □

COROLLARY 19.10
Suppose that $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ where $p_1, \dots, p_r$ are distinct primes. Then n is constructive if and only if each $p_j^{\alpha_j}$ is constructive.

Another obvious result:

LEMMA 19.11
For any positive integer α, the number 2^α is constructive.

PROOF The angle can be bisected by ruler and compasses, and the result follows by induction on α. □

This reduces the problem of constructing regular polygons to the case when the number of sides is an odd prime power. Now we bring in the algebra. In the complex plane, the set of nth roots of unity forms the vertices of a regular n-gon. Further, these roots of unity are the zeros in $\mathbb{C}$ of the polynomial

$$t^n - 1 = (t - 1)(t^{n-1} + t^{n-2} + \cdots + t + 1)$$

We concentrate on the second factor on the right-hand side.

LEMMA 19.12
Let p be a prime such that p^n is constructive. Let ζ be a primitive p^nth root of unity in $\mathbb{C}$. Then the degree of the minimal polynomial of ζ over $\mathbb{Q}$ is a power of 2.

PROOF Take $\zeta = \exp(2\pi i/p^n)$. Since p^n is constructive we can construct the point (α, β) where $\alpha = \cos(2\pi/p^n)$ and $\beta = \sin(2\pi/p^n)$ by projecting a vertex of the regular p^n-gon on to the coordinate axes. Hence by Theorem 19.4

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^r$$

for some integer r. Therefore,

$$[\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = 2^{r+1}$$

But $\mathbb{Q}(\alpha, \beta, i)$ contains $\alpha + i\beta = \zeta$, so that $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is a power of 2, since $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\alpha, \beta, i)$. Hence the degree of the minimal polynomial of ζ over $\mathbb{Q}$ is a power of 2.

The next step is to calculate the relevant minimal polynomials to find their degrees. It turns out to be sufficient to consider p and p^2 only. The analysis explains the result we obtained in (3.3) by direct computation. □

LEMMA 19.13

If p is a prime and ζ is a primitive pth root of unity in $\mathbb{C}$, then the minimal polynomial of ζ over $\mathbb{Q}$ is

$$f(t) = 1 + t + \cdots + t^{p-1}$$

PROOF Note that $f(t) = (t^p - 1)/(t - 1)$. We know that $f(\zeta) = 0$ since $\zeta^p - 1 = 0$ and $\zeta \neq 1$. We are home if we can show that $f(t)$ is irreducible. Put $t = 1 + u$ where u is a new indeterminate. Then $f(t)$ is irreducible over $\mathbb{Q}$ if and only if $f(1 + u)$ is irreducible. But

$$\begin{aligned} f(1+u) &= \frac{(1+u)^p - 1}{u} \\ &= u^{p-1} + ph(u) \end{aligned}$$

where h is a polynomial in u over $\mathbb{Z}$ with constant term 1, by the usual remark about binomial coefficients. By Eisenstein's Criterion, $f(1 + u)$ is irreducible over $\mathbb{Q}$. □

LEMMA 19.14

If p is a prime and ζ is a primitive p^2th root of unity in $\mathbb{C}$, then the minimal polynomial of ζ over $\mathbb{Q}$ is

$$g(t) = 1 + t^p + \cdots + t^{p(p-1)}$$

PROOF Note that $g(t) = (t^{p^2} - 1)/(t^p - 1)$. Now $\zeta^{p^2} - 1 = 0$ but $\zeta^p - 1 \neq 0$ so $g(\zeta) = 0$. It suffices to show that $g(t)$ is irreducible over $\mathbb{Q}$. As before, we make the substitution $t = 1 + u$. Then

$$g(1+u) = \frac{(1+u)^{p^2} - 1}{(1+u)^p - 1}$$

and modulo p this is

$$\frac{(1+u^{p^2})-1}{(1+u^p)-1} = u^{p(p-1)}$$

Therefore, $g(1+u) = u^{p(p-1)} + pk(u)$ where k is a polynomial in u over $\mathbb{Z}$. From the alternative expression

$$g(1+u) = 1 + (1+u)^p + \cdots + (1+u)^{p(p-1)}$$

it follows that k has constant term 1. By Eisenstein's Criterion, $g(1+u)$ is irreducible over $\mathbb{Q}$.

We now come to the main result. □

THEOREM 19.15 (Gauss)
The regular n-gon is constructible by ruler and compasses if and only if

$$n = 2^r p_1 \ldots p_s$$

where r and s are integers ≥ 0, *and* $p_1, \ldots, p_s$ *are odd primes of the form*

$$p_j = 2^{2^{r_j}} + 1$$

for positive integers r_j.

PROOF Let n be constructive. Then $n = 2^r p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ where $p_1, \ldots, p_s$ are distinct odd primes. By Corollary 19.10, each $p_j^{\alpha_j}$ is constructive. If $\alpha_j \geq 2$, then p_j^2 is constructive by Theorem 19.4. Hence the degree of the minimal polynomial of a primitive p_j^2th root of unity over $\mathbb{Q}$ is a power of 2 by Lemma 19.12. By Lemma 19.14, $p_j(p_j - 1)$ is a power of 2, which cannot happen since p_j is odd. Therefore $\alpha_j = 1$ for all j. Therefore, p_j is constructive. By Lemma 19.13

$$p_j - 1 = 2^{s_j}$$

for suitable s_j. Suppose that s_j has an odd divisor $a > 1$, so that $s_j = ab$. Then

$$p_j = (2^b)^a + 1$$

which is divisible by $2^b + 1$ since

$$t^a + 1 = (t+1)(t^{a-1} - t^{a-2} + \cdots + 1)$$

when a is odd. So p_j cannot be prime. Hence s_j has no odd factors, so

$$s_j = 2^{r_j}$$

for some $r_j > 0$.

This establishes the necessity of the given form of n. Now we prove sufficiency. By Corollary 19.10 we need consider only prime-power factors of n. By Lemma 19.11, 2^r is constructive. We must show that each p_j is constructive. Let ζ be a primitive p_jth root of unity. Then

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p_j - 1 = 2^a$$

for some a by Lemma 19.13. Now $\mathbb{Q}(\zeta)$ is a splitting field for $f(t) = 1 + \cdots + t^{p-1}$ over $\mathbb{Q}$, so that $\mathbb{Q}(\zeta) : \mathbb{Q}$ is normal. It is also separable since the characteristic is zero. By Lemma 15.6, the Galois group $\Gamma(\mathbb{Q}(\zeta):\mathbb{Q})$ is abelian. Let $K = \mathbb{R} \cap \mathbb{Q}(\zeta)$. Then

$$\cos(2\pi/p_j) = (\zeta + \zeta^{-1})/2 \in K$$

Now $\mathbb{Q}(\zeta) : K$ has degree 2, so by Theorem 12.1 $\Gamma(\mathbb{Q}(\zeta) : K)$ is a subgroup of $G = \Gamma(\mathbb{Q}(\zeta) : \mathbb{Q})$ of order 2. Further, it is a normal subgroup, since G is abelian. Therefore, $K : \mathbb{Q}$ is a normal extension of degree 2^{a-1}. By Proposition 19.7, the point $(\cos(2\pi/p_j), 0)$ is constructible. Hence p_j is constructive, and the proof is complete. □

19.4 Fermat Numbers

The problem now reduces to number theory. In 1640 Pierre de Fermat wondered when $2^k + 1$ is prime, and proved that a necessary condition is for k to be a power of 2. Thus we are led to:

DEFINITION 19.16 *The nth* Fermat number *is* $F_n = 2^{2^n} + 1$.

The question becomes: when is F_n prime?

Fermat noticed that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ are all prime. He conjectured that F_n is prime for all n, but this was disproved by Euler in 1732, who proved that F_5 is divisible by 641 (Exercise 19.5). Knowledge of factors of Fermat numbers is changing almost daily, thanks to the prevalence of fast computers and special algorithms for primality testing of Fermat numbers (see Internet References). At the time of writing, the largest known composite Fermat number was F_{382449}, with a factor $3.2^{382447} + 1$, and 210 Fermat numbers were known to be composite.

The only known Fermat primes are still those found by Fermat himself:

PROPOSITION 19.17

If p is a prime, then the regular p-gon is constructible for $p = 2, 3, 5, 17, 257, 65537$.

19.5 How to Draw a Regular 17-Gon

Many constructions for the regular 17-gon have been devised, the earliest published being that of Huguenin (see Klein, 1913) in 1803. For several of these constructions there are proofs of their correctness which use only synthetic geometry (ordinary Euclidean geometry without coordinates). A series of papers giving a construction for the regular 257-gon was published by F.J. Richelot (1832) under one of the longest titles I have ever seen. Bell (1965) tells of an overly zealous research student being sent away to find a construction for the 65537-gon, and reappearing with one 20 years later. This story, though apocryphal, is not far from the truth; Professor Hermes of Lingen spent 10 years on the problem, and his manuscripts are still preserved at Göttingen.

One way to construct a regular 17-gon is to follow faithfully the above theory, which in fact provides a perfectly definite construction after a little extra calculation. With ingenuity it is possible to shorten the work. The construction that we now describe is taken from Hardy and Wright (1962).

Our immediate object is to find radical expressions for the zeros of the polynomial

$$\frac{t^{17}-1}{t-1} = t^{16} + \cdots + t + 1 \tag{19.1}$$

over $\mathbb{C}$. Let

$$\theta = 2\pi/17$$
$$\varepsilon_k = e^{ki\theta} = \cos k\theta + i \sin k\theta$$

The zeros of equation (19.1) in $\mathbb{C}$ are then $\varepsilon_1, \ldots, \varepsilon_{16}$.

The powers of 3 reduced mod 17 are:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Define

$$\begin{aligned}
x_1 &= \varepsilon_1 + \varepsilon_9 + \varepsilon_{13} + \varepsilon_{15} + \varepsilon_{16} + \varepsilon_8 + \varepsilon_4 + \varepsilon_2 \\
x_2 &= \varepsilon_3 + \varepsilon_{10} + \varepsilon_5 + \varepsilon_{11} + \varepsilon_{14} + \varepsilon_7 + \varepsilon_{12} + \varepsilon_6 \\
y_1 &= \varepsilon_1 + \varepsilon_{13} + \varepsilon_{16} + \varepsilon_4 \\
y_2 &= \varepsilon_9 + \varepsilon_{15} + \varepsilon_8 + \varepsilon_2 \\
y_3 &= \varepsilon_3 + \varepsilon_5 + \varepsilon_{14} + \varepsilon_{12} \\
y_4 &= \varepsilon_{10} + \varepsilon_{11} + \varepsilon_7 + \varepsilon_6
\end{aligned}$$

Now

$$\varepsilon_k + \varepsilon_{17-k} = 2\cos k\theta \tag{19.2}$$

for $k = 1, \ldots, 16$, so

$$\begin{aligned} x_1 &= 2(\cos\ \theta + \cos\ 8\theta + \cos\ 4\theta + \cos\ 2\theta) \\ x_2 &= 2(\cos\ 3\theta + \cos\ 7\theta + \cos\ 5\theta + \cos\ 6\theta) \\ y_1 &= 2(\cos\ \theta + \cos\ 4\theta) \\ y_2 &= 2(\cos\ 8\theta + \cos\ 2\theta) \\ y_3 &= 2(\cos\ 3\theta + \cos\ 5\theta) \\ y_4 &= 2(\cos\ 7\theta + \cos\ 6\theta) \end{aligned} \tag{19.3}$$

Equation (19.1) implies that

$$x_1 + x_2 = -1$$

Now (19.3) and the identity

$$2\cos m\theta \cos n\theta = \cos(m+n)\theta + \cos(m-n)\theta$$

imply that

$$x_1 x_2 = 4(x_1 + x_2) = -4$$

using (19.2). Hence x_1 and x_2 are zeros of the quadratic polynomial

$$t^2 + t - 4 \tag{19.4}$$

Further, $x_1 > 0$ so that $x_1 > x_2$. By further trigonometric expansions,

$$y_1 + y_2 = x_1 \qquad y_1 y_2 = -1$$

and y_1, y_2 are the zeros of

$$t^2 - x_1 t - 1 \tag{19.5}$$

Further, $y_1 > y_2$. Similarly, y_3 and y_4 are the zeros of

$$t^2 - x_2 t - 1 \tag{19.6}$$

and $y_3 > y_4$. Now

$$\begin{aligned} 2\cos\theta + 2\cos 4\theta &= y_1 \\ 4\cos\theta\cos 4\theta = 2\cos 5\theta + 2\cos 3\theta &= y_3 \end{aligned}$$

so

$$z_1 = 2\cos\theta \qquad z_2 = 2\cos 4\theta$$

are the zeros of

$$t^2 - y_1 t + y_3 \tag{19.7}$$

and $z_1 > z_2$.

Solving the series of quadratics (19.4 to 19.7) and using the inequalities to decide which zero is which, we obtain

$$\cos\theta = \frac{1}{16}\Big(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})\sqrt{34 - 2\sqrt{17}}}\Big)$$

where the square roots are the positive ones.

From this we can deduce a geometric construction for the 17-gon by constructing the relevant square roots. By using greater ingenuity it is possible to obtain an aesthetically more satisfying construction. The following method (Figure 19.9) is due to Richmond (1893).

Let ϕ be the smallest positive acute angle such that $\tan 4\phi = 4$. Then ϕ, 2ϕ, and 4ϕ are all acute. Expression (19.4) can be written

$$t^2 + 4t\cot 4\phi - 4$$

whose zeros are

$$2\tan 2\phi \qquad -2\cot 2\phi$$

Hence

$$x_1 = 2\tan 2\phi \qquad x_2 = -2\cot 2\phi$$

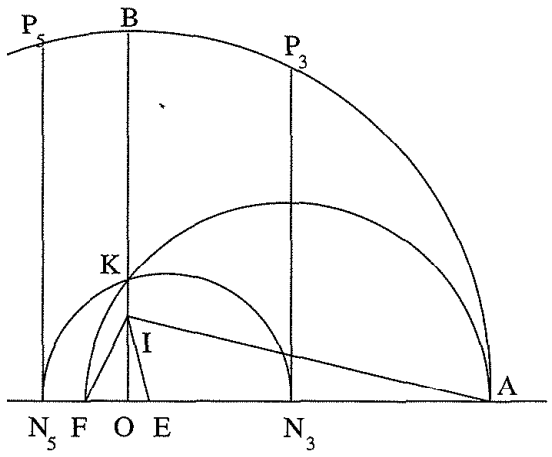

Figure 19.9: Construction for a regular 17-gon.

From this it follows that

$$y_1 = \tan\left(\phi + \frac{\pi}{4}\right) \qquad y_2 = \tan\left(\phi - \frac{\pi}{4}\right) \qquad y_3 = \tan\phi \qquad y_4 = -\cot\phi$$

Then

$$\begin{aligned} 2(\cos 3\theta + \cos 5\theta) &= \tan\phi \\ 4\cos 3\theta \cos 5\theta &= \tan\left(\phi - \frac{\pi}{4}\right) \end{aligned} \tag{19.8}$$

Now (Figure 19.9) let OA, OB be two perpendicular radii of a circle. Make $\mathrm{OI} = \frac{1}{4}\mathrm{OB}$ and $\angle\mathrm{OIE} = \frac{1}{4}\angle\mathrm{OIA}$. Find F on AO produced to make $\angle\mathrm{EIF} = \frac{\pi}{4}$. Let the circle on AF as diameter cut OB in K, and let the circle centre E through K cut OA in N_3 and N_5 as shown. Draw $\mathrm{N}_3\mathrm{P}_3$ and $\mathrm{N}_5\mathrm{P}_5$ perpendicular to OA. Then $\angle\mathrm{OIA} = 4\phi$ and $\angle\mathrm{OIE} = \phi$. Also,

$$\begin{aligned} 2(\cos\angle\mathrm{AOP}_3 + \cos\angle\mathrm{AOP}_5) &= 2\frac{\mathrm{ON}_3 - \mathrm{ON}_5}{\mathrm{OA}} \\ &= 4\frac{\mathrm{OE}}{\mathrm{OA}} + \frac{\mathrm{OE}}{\mathrm{OI}} = \tan\phi \end{aligned}$$

and

$$\begin{aligned} 4\cos\angle\mathrm{AOP}_3\ \cos\angle\mathrm{AOP}_5 &= -4\frac{\mathrm{ON}_3 \times \mathrm{ON}_5}{\mathrm{OA} \times \mathrm{OA}} \\ &= -4\frac{\mathrm{OK}^2}{\mathrm{OA}^2} \\ &= -4\frac{\mathrm{OF}}{\mathrm{OA}} \\ &= -\frac{\mathrm{OF}}{\mathrm{OI}} = \tan\left(\phi - \frac{\pi}{4}\right) \end{aligned}$$

Comparing these with Equation (19.8) we see that

$$\angle\mathrm{AOP}_3 = 3\theta \qquad \angle\mathrm{AOP}_5 = 5\theta$$

Hence A, P_3, P_5 are the zeroth, third, and fifth vertices of a regular 17-gon inscribed in the given circle. The other vertices are now easily found.

Exercises

19.1 Using only the operations ruler and compasses, show how to draw a parallel to a given line through a given point.

19.2 Verify the following approximate constructions for regular n-gons found by Oldroyd (1955):

a. 7-*gon*. Construct $\cos^{-1}\frac{4+\sqrt{5}}{10}$ giving an angle of approximately $2\pi/7$.

b. 9-*gon*. Construct $\cos^{-1}\frac{5\sqrt{3}-1}{10}$.

c. 11-*gon*. Construct $\cos^{-1}\frac{8}{9}$ and $\cos^{-1}\frac{1}{2}$ and take their difference.

d. 13-*gon*. Construct $\tan^{-1}1$ and $\tan^{-1}\frac{4+\sqrt{5}}{20}$ and take their difference.

19.3 Show that for n odd the only known constructible n-gons are precisely those for which n is a divisor of $2^{32}-1 = 4294967295$.

19.4 Work out the approximate size of F_{382449}, which is known to be composite. Explain why it is no easy task to find factors of Fermat numbers.

19.5 Use the equations

$$641 = 5^4 + 2^4 = 5.2^7 + 1$$

to show that 641 divides F_5.

19.6 Show that

$$F_{n+1} = 2 + F_n F_{n-1} \ldots F_0$$

and deduce that if $m \neq n$, then F_m and F_n are coprime. Hence show that there are infinitely many prime numbers.

19.7 List the values of $n \leq 100$ for which the regular n-gon can be constructed by ruler and compasses.

19.8 Verify the following construction for the regular pentagon.

Draw a circle centre O with two perpendicular radii OP_0, OB. Let D be the midpoint of OB, join P_0D. Bisect $\angle ODP_0$ cutting OP_0 at N. Draw NP_1 perpendicular to OP_0 cutting the circle at P_1. Then P_0 and P_1 are the zeroth and first vertices of a regular pentagon inscribed in the circle.

19.9* Discuss the construction of regular polygons using a ruler, compasses, and an angle trisector. (For example, 9-gons or 13-gons are then constructible. Use the trigonometric solution of cubic equations.)

19.10 Euclid's construction for an isosceles triangle with angles $4\pi/5, 4\pi/5, 2\pi/5$ depends on constructing the so-called golden section: that is, *to construct a given straight line so that the rectangle contained by the whole and one of the segments is equal to the square on the other segment.* The Greek term was "extreme and mean ratio." In Book 2 Proposition 11 of the *Elements* Euclid solves this problem as in Figure 19.10.

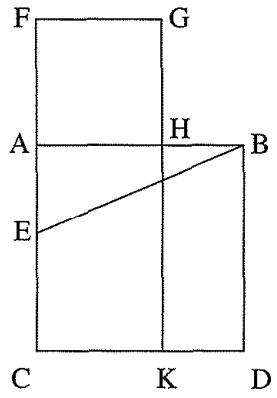

Figure 19.10: Cutting a line in extreme and mean ratio.

Let AB be the given line. Make ABDC a square. Bisect AC at E, and make EF = BE. Now find H such that AH = AF. Then the square on AH has the same area as the rectangle with sides AB and BH, as required.

Prove that Euclid was right.

19.11 Mark the following true or false.

a. $2^n + 1$ cannot be prime unless n is a power of 2.

b. If n is a power of 2, then $2^n + 1$ is always prime.

c. The regular 771-gon is constructible using ruler and compasses.

d. The regular 768-gon is constructible using ruler and compasses.

e. The regular 51-gon is constructible using ruler and compasses.

f. The regular 25-gon is constructible using ruler and compasses.

g. For an odd prime p, the regular p^2-gon is never constructible using ruler and compasses.

h. If n is an integer > 0, then a line of length $\sqrt{n}$ can always be constructed using ruler and compasses.

i. If n is an integer > 0, then a line of length $\sqrt[4]{n}$ can always be constructed using ruler and compasses.

j. A point whose coordinates lie in a normal extension of $\mathbb{Q}$ whose degree is a power of 2 is constructible using ruler and compasses.

k. If p is a prime, then $t^{p^2} - 1$ is irreducible over $\mathbb{Q}$.