Proposition 29. The regular n-gon can be constructed by straightedge and compass if and only if $n = 2^k p_1 \cdots p_r$ is the product of a power of 2 and distinct Fermat primes.

The proof above actually indicates a procedure for constructing the regular n-gon as a succession of square roots. For example, the construction of the regular 17-gon (solved by Gauss in 1796 at age 19) requires the construction of the subfields of degrees 2, 4, 8 and 16 in $\mathbb{Q}(\zeta_{17})$. These subfields can be constructed by forming the *periods* of ζ_{17} as in the example of the 13^{th} roots of unity above. In this case, the fact that $\mathbb{Q}(\zeta_{17})$ is obtained by a series of quadratic extensions reflects itself in the fact that the periods can be "halved" successively (i.e., if $H_1 < H_2$ are subgroups with $[H_2 : H_1] = 2$ then the periods for H_1 satisfy a quadratic equation whose coefficients involve the periods for H_2). For example, the periods for the subgroup of index 2 (generated by σ_2) in the Galois group are ($\zeta = \zeta_{17}$)

$$\eta_1 = \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16}$$
$$\eta_2 = \zeta^3 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^{10} + \zeta^{11} + \zeta^{12} + \zeta^{14}$$

which "halve" the period for the full Galois group and which satisfy

$$\eta_1 + \eta_2 = -1$$

(from the minimal polynomial satisfied by ζ_{17}) and

$$\eta_1 \eta_2 = -4$$

(which requires computation — we know that it must be rational by Galois Theory, since this product is fixed by all the elements of the Galois group). Hence these two periods are the roots of the quadratic equation

$$x^2 + x - 4 = 0$$

which we can solve explicitly. In a similar way, the periods for the subgroup of index 4 (generated by σ_4) naturally halve these periods, so are quadratic over these, etc. In this way one can determine ζ_{17} explicitly in terms of iterated square roots. For example, one finds that $8(\zeta + \zeta^{-1}) = 16\cos(\frac{2\pi}{17})$ (which is enough to construct the regular 17-gon) is given explicitly by

$$-1+\sqrt{17}+\sqrt{2(17-\sqrt{17})}+2\sqrt{17+3\sqrt{17}-\sqrt{2(17-\sqrt{17})}-2\sqrt{2(17+\sqrt{17})}}\,.$$

A relatively simple construction of the regular 17-gon (shown to us by J.H. Conway) is indicated in the exercises.

While we have seen that it is not possible to solve for ζ_n using only successive square roots in general, by definition it is possible to obtain ζ_n by successive extraction of higher roots (namely, taking an n^{th} root of 1). This is not the case for solutions of general equations of degree n, where one cannot generally determine solutions by radicals, as we shall see in the next sections.

EXERCISES

1. Determine the minimal polynomials satisfied by the primitive generators given in the text for the subfields of $\mathbb{Q}(\zeta_{13})$.
2. Determine the subfields of $\mathbb{Q}(\zeta_8)$ generated by the periods of ζ_8 and in particular show that not every subfield has such a period as primitive element.
3. Determine the quadratic equation satisfied by the period $\alpha = \zeta_5 + \zeta_5^{-1}$ of the 5^{th} root of unity ζ_5. Determine the quadratic equation satisfied by ζ_5 over $\mathbb{Q}(\alpha)$ and use this to explicitly solve for the 5^{th} root of unity.
4. Let $\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ denote the automorphism of the cyclotomic field of n^{th} roots of unity which maps ζ_n to ζ_n^a where a is relatively prime to n and ζ_n is a primitive n^{th} root of unity. Show that $\sigma_a(\zeta) = \zeta^a$ for *every* n^{th} root of unity.
5. Let p be a prime and let $\epsilon_1, \epsilon_2, \ldots, \epsilon_{p-1}$ denote the primitive p^{th} roots of unity. Set $p_n = \epsilon_1^n + \epsilon_2^n + \cdots + \epsilon_{p-1}^n$, the sum of the n^{th} powers of the ϵ_i. Prove that $p_n = -1$ if p does not divide n and that $p_n = p - 1$ if p does divide n. [One approach: $p_1 = -1$ from $\Phi_p(x)$; show that p_n is a Galois conjugate of p_1 for p not dividing n, hence is also -1.]
6. Let ζ_n denote a primitive n^{th} root of unity and let $K = \mathbb{Q}(\zeta_n)$ be the associated cyclotomic field. Let a denote the trace of ζ_n from K to $\mathbb{Q}$ (cf. Exercise 18 of Section 2). Prove that $a = 1$ if $n = 1$, $a = 0$ if n is divisible by the square of a prime, and $a = (-1)^r$ if n is the product of r distinct primes.
7. Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of n^{th} roots of unity. Show that the field $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the *maximal real subfield of* K.
8. Let $K_n = \mathbb{Q}(\zeta_{2^{n+2}})$ be the cyclotomic field of 2^{n+2}-th roots of unity, $n \geq 0$. Set $\alpha_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$ and $K_n^+ = \mathbb{Q}(\alpha_n)$, the maximal real subfield of K_n.
   (a) Show that for all $n \geq 0$, $[K_n : \mathbb{Q}] = 2^{n+1}$, $[K_n : K_n^+] = 2$, $[K_n^+ : \mathbb{Q}] = 2^n$, and $[K_{n+1}^+ : K_n^+] = 2$.
   (b) Determine the quadratic equation satisfied by $\zeta_{2^{n+2}}$ over K_n^+ in terms of α_n.
   (c) Show that for $n \geq 0$, $\alpha_{n+1}^2 = 2 + \alpha_n$ and hence show that

$$\alpha_n = \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}} \qquad (n \text{ times}),$$

   giving an explicit formula for the (constructible) 2^{n+2}-th roots of unity.
9. Notation as in the previous exercise.
   (a) Prove that K_n^+ is a cyclic extension of $\mathbb{Q}$ of degree 2^n. [Use an explicit isomorphism $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ as abelian groups (i.e., $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times$ is isomorphic to a cyclic group of order 2 and a cyclic group of order 2^n — cf. Exercises 22 and 23 of Section 2.3]
   (b) Prove that K_n is a biquadratic extension of K_{n-1}^+ and that two of the three intermediate subfields are K_n^+ and K_{n-1}. Prove that the remaining field intermediate between K_{n-1}^+ and K_n is a cyclic extension of $\mathbb{Q}$ of degree 2^n.
10. Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.
11. Prove that the primitive n^{th} roots of unity form a basis over $\mathbb{Q}$ for the cyclotomic field of n^{th} roots of unity if and only if n is squarefree (i.e., n is not divisible by the square of any prime).

12. Let σ_p denote the Frobenius automorphism $x \mapsto x^p$ of the finite field $\mathbb{F}_q$ of $q = p^n$ elements. Viewing $\mathbb{F}_q$ as a vector space V of dimension n over $\mathbb{F}_p$ we can consider σ_p as a linear transformation of V to V. Determine the characteristic polynomial of σ_p and prove that the linear transformation σ_p is diagonalizable over $\mathbb{F}_p$ if and only if n divides $p-1$, and is diagonalizable over the algebraic closure of $\mathbb{F}_p$ if and only if $(n, p) = 1$.

13. Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ be the prime factorization of n and let ζ_n be a primitive n^{th} root of unity. For each $i = 1, 2, \dots, k$ define d_i by $n = p_i^{a_i} d_i$ and let $\zeta_{p_i^{a_i}} = \zeta_n^{d_i}$, so that $\zeta_{p_i^{a_i}}$ is a particular primitive $p_i^{a_i}$-th root of unity. Let $\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ be the automorphism mapping ζ_n to ζ_n^a for a relatively prime to n.

(a) Prove that for $i = 1, 2, \dots, k$, σ_a maps $\zeta_{p_i^{a_i}}$ to $\zeta_{p_i^{a_i}}^a$ and gives an automorphism of $\mathbb{Q}(\zeta_{p_i^{a_i}})/\mathbb{Q}$ which depends only on $a \pmod{p_i^{a_i}}$, which we may denote $\sigma_{a \pmod{p_i^{a_i}}}$.

(b) Prove that the map $\sigma_a \mapsto (\sigma_{a \pmod{p_1^{a_1}}}, \dots, \sigma_{a \pmod{p_k^{a_k}}})$ is the isomorphism of Corollary 27 corresponding to the Chinese Remainder Theorem for $(\mathbb{Z}/n\mathbb{Z})^\times$.

The following Exercises 14 to 18 determine the periods associated to a primitive 17^{th} root of unity and provide a proof for the simple geometric construction indicated in Exercise 17 for the regular 17-gon. Let $\zeta = \zeta_{17} = \cos\dfrac{2\pi}{17} + i \sin\dfrac{2\pi}{17}$ be a fixed primitive 17^{th} root of unity in $\mathbb{C}$.

14. Define the *periods* of ζ as follows:

$$\eta_1 = \zeta+\zeta^2+\zeta^4+\zeta^8+\zeta^9+\zeta^{13}+\zeta^{15}+\zeta^{16} \qquad \eta_3' = \zeta^6+\zeta^7+\zeta^{10}+\zeta^{11}$$
$$\eta_2 = \zeta^3+\zeta^5+\zeta^6+\zeta^7+\zeta^{10}+\zeta^{11}+\zeta^{12}+\zeta^{14} \qquad \eta_4' = \zeta^3+\zeta^5+\zeta^{12}+\zeta^{14}$$
$$\eta_1' = \zeta+\zeta^4+\zeta^{13}+\zeta^{16} \qquad \eta_1'' = \zeta+\zeta^{16}$$
$$\eta_2' = \zeta^2+\zeta^8+\zeta^9+\zeta^{15} \qquad \eta_2'' = \zeta^4+\zeta^{13}.$$

(a) Show that all of these periods are real numbers and that $\eta_1'' = 2\cos\dfrac{2\pi}{17}$. Show that as real numbers these periods are approximately

$$\eta_1 \sim 1.562 \qquad \eta_1' \sim 2.049 \qquad \eta_3' \sim -2.906 \qquad \eta_1'' \sim 1.865$$
$$\eta_2 \sim -2.562 \qquad \eta_2' \sim -0.488 \qquad \eta_4' \sim 0.344 \qquad \eta_2'' \sim 0.185.$$

(b) Prove that η_1 and η_2 are roots of the equation $x^2 + x - 4 = 0$.

(c) Prove that η_1' and η_2' are roots of the equation $x^2 - \eta_1 x - 1 = 0$ and that η_3' and η_4' are roots of the equation $x^2 - \eta_2 x - 1 = 0$.

(d) Prove that η_1'' and η_2'' are roots of the equation $x^2 - \eta_1' x + \eta_4' = 0$.

15. Prove that if $\tan 2\theta = a$ $(0 < 2\theta < \dfrac{\pi}{2})$ then $\tan\theta$ satisfies the equation $x^2 - \dfrac{2}{a}x - 1 = 0$.

16. Let C be the circle in $\mathbb{R}^2$ having the points (h, k) and $(0, 1)$ as a diameter. Prove that this circle intersects the x-axis if and only if $h^2 - 4k \geq 0$ and in this case the two intercepts are the roots of the equation $x^2 - hx + k = 0$.

17. (*Construction of the Regular 17-gon*) Draw a circle of radius 2 centered at the origin $(0, 0)$.

(a) Join the point $(4, 0)$ to the point $(0, 1)$ and construct the line ℓ_1 bisecting the angle

between this line and the y-axis. Construct the line ℓ_2 perpendicular to ℓ_1 in Figure 2.

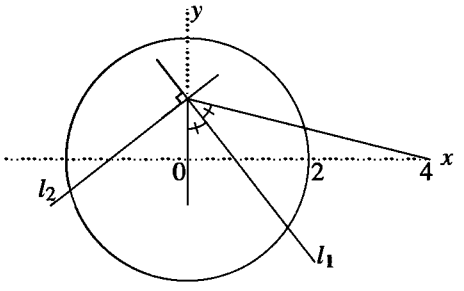

Fig. 2

(b) Using the intersection of ℓ_1 and the x-axis as center and radius equal to the distance to (0, 1), construct the circle C_1 and let $A = (s, 0)$ be the right-hand point of intersection of C_1 with the x-axis. Similarly, let $B = (t, 0)$ denote the right-hand point of intersection of the x-axis and the circle C_2 whose center is the intersection of ℓ_2 and the x-axis and whose radius is equal to the distance to (0, 1) as in Figure 3.

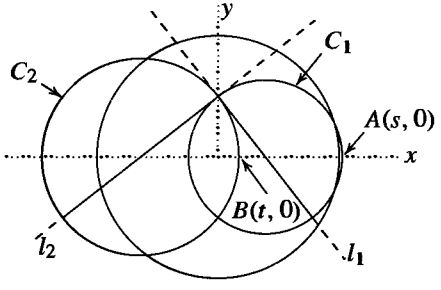

Fig. 3

(c) Construct a perpendicular to the x-axis at the point A and mark off the distance t from (0, 0) to B to construct the point (s, t). Construct the circle with (s, t) and (0, 1) as a diameter and let P denote the right-hand point of intersection of this circle with the x-axis. The perpendicular to the x-axis at P intersects the circle of radius 2 at the second vertex of a regular 17-gon whose first vertex is at (2,0), hence constructs the regular 17-gon by straightedge and compass as in Figure 4.

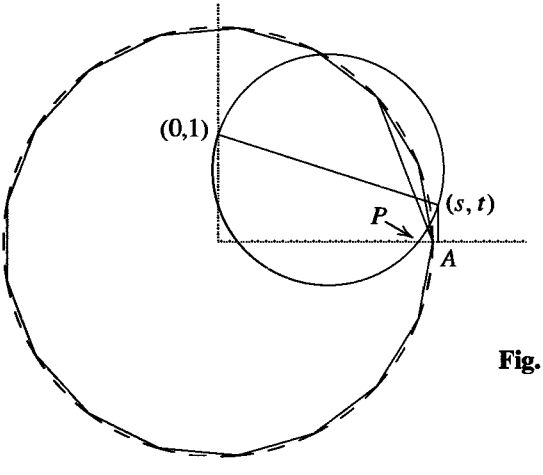

Fig. 4