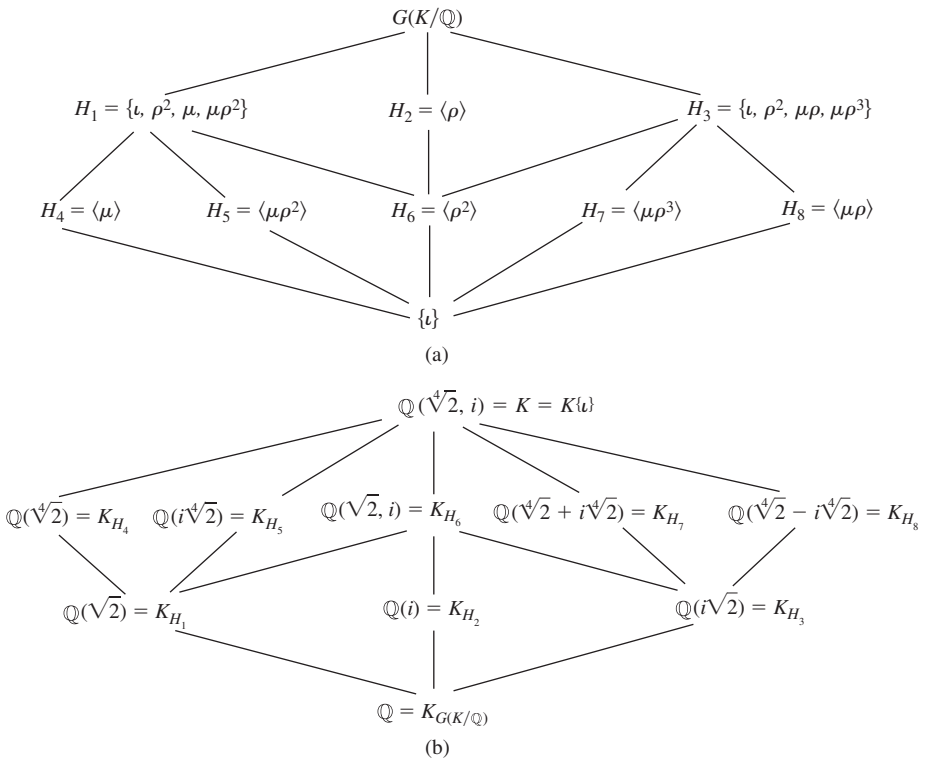


47.6 Figure (a) Group diagram. (b) Field diagram.

The conjugates of $\gamma = \alpha + i\alpha$ are thus $\alpha + i\alpha, i\alpha - \alpha, -\alpha - i\alpha$, and $-i\alpha + \alpha$. Hence

$$\begin{aligned}\operatorname{irr}(\gamma, \mathbb{Q}) &= [(x - (\alpha + i\alpha))(x - (i\alpha - \alpha))] \\ &\quad \cdot [(x - (-\alpha - i\alpha))(x - (-i\alpha + \alpha))] \\ &= (x^2 - 2i\alpha x - 2\alpha^2)(x^2 + 2i\alpha x - 2\alpha^2) \\ &= x^4 + 4\alpha^4 = x^4 + 8.\end{aligned}$$

▲

We have seen examples in which the splitting field of a quartic (4th degree) polynomial over a field F is an extension of F of degree 8 (Example 47.3) and of degree 24 (Theorem 47.2, with $n = 4$). The degree of an extension of a field F that is a splitting field of a quartic over F must always divide $4! = 24$. The splitting field of $(x - 2)^4$ over $\mathbb{Q}$ is $\mathbb{Q}$, an extension of degree 1, and the splitting field of $(x^2 - 2)^2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$, an extension of degree 2. Our last example will give an extension of degree 4 for the splitting field of a quartic.

47.7 Example Consider the splitting field of $x^4 + 1$ over $\mathbb{Q}$. By Theorem 28.12, we can show that $x^4 + 1$ is irreducible over $\mathbb{Q}$, by arguing that it does not factor in $\mathbb{Z}[x]$. (See Exercise 1.) The work on complex numbers in Section 3 shows that the zeros of $x^4 + 1$ are $(1 \pm i)/\sqrt{2}$ and $(-1 \pm i)/\sqrt{2}$. A computation shows that if

$$\alpha = \frac{1 + i}{\sqrt{2}},$$

then

$$\alpha^3 = \frac{-1+i}{\sqrt{2}}, \qquad \alpha^5 = \frac{-1-i}{\sqrt{2}}, \qquad \text{and} \qquad \alpha^7 = \frac{1-i}{\sqrt{2}}.$$

Thus the splitting field K of x^4+1 over $\mathbb{Q}$ is $\mathbb{Q}(\alpha)$, and $[K:\mathbb{Q}] = 4$. Let us compute $G(K/\mathbb{Q})$ and give the group and field diagrams. Since there exist automorphisms of K mapping α onto each conjugate of α, and since an automorphism σ of $\mathbb{Q}(\alpha)$ is completely determined by $\sigma(\alpha)$, we see that the four elements of $G(K/\mathbb{Q})$ are defined by Table 47.8.

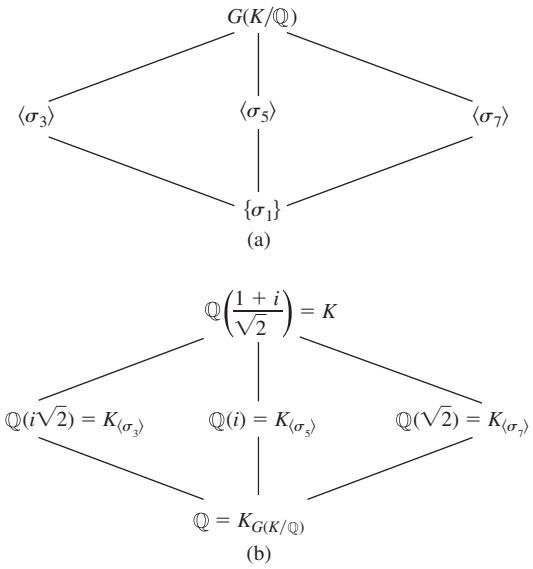
47.8 Table

	σ_1	σ_3	σ_5	σ_7
$\alpha \to$	α	α^3	α^5	α^7

Since

$$(\sigma_j\sigma_k)(\alpha) = \sigma_j(\alpha^k) = (\alpha^j)^k = \alpha^{jk}$$

and $\alpha^8 = 1$, we see that $G(K/\mathbb{Q})$ is isomorphic to the group $\{1, 3, 5, 7\}$ under multiplication modulo 8. There are only two groups of order 4 up to isomorphism, the cyclic group and the Klein 4-group. Since each element of $\{1,3,5,7\}$ has order 2 or 1, $G(K/\mathbb{Q})$ is isomorphic with the Klein 4-group. The diagrams are given in Fig. 47.9.



47.9 Figure (a) Group diagram. (b) Field diagram.

To find $K_{\langle\sigma_3\rangle}$, it is only necessary to find an element of K not in $\mathbb{Q}$ fixed by $\{\sigma_1, \sigma_3\}$, since $[K_{\langle\sigma_3\rangle} : \mathbb{Q}] = 2$. Clearly $\sigma_1(\alpha) + \sigma_3(\alpha)$ is fixed by both σ_1 and σ_3, since $\{\sigma_1, \sigma_3\} = \langle\sigma_3\rangle$ is a group. We have

$$\sigma_1(\alpha) + \sigma_3(\alpha) = \alpha + \alpha^3 = i\sqrt{2}.$$

Similarly,

$$\sigma_1(\alpha) + \sigma_7(\alpha) = \alpha + \alpha^7 = \sqrt{2}$$

is fixed by $\langle\sigma_7\rangle = \{\sigma_1, \sigma_7\}$. This technique is of no use in finding $E_{\langle\sigma_5\rangle}$, for

$$\sigma_1(\alpha) + \sigma_5(\alpha) = \alpha + \alpha^5 = 0,$$

and $0 \in \mathbb{Q}$. But by a similar argument, $\sigma_1(\alpha)\sigma_5(\alpha)$ is fixed by both σ_1 and σ_5, and

$$\sigma_1(\alpha)\sigma_5(\alpha) = \alpha\alpha^5 = -i.$$

Thus $\mathbb{Q}(-i) = \mathbb{Q}(i)$ is the field we are after.

▲

EXERCISES 47

Computations (requiring more than the usual amount of theory)

1. Show that $x^4 + 1$ is irreducible in $\mathbb{Q}[x]$, as we asserted in Example 47.7.

2. Verify that the intermediate fields given in the field diagram in Fig. 47.6 are correct. (Some are verified in the text. Verify the rest.)

3. For each field in the field diagram in Fig. 47.6, find a primitive element generating the field over $\mathbb{Q}$ (see Theorem 45.13) and give its irreducible polynomial over $\mathbb{Q}$.

4. Let ζ be a primitive 5th root of unity in $\mathbb{C}$.

a. Show that $\mathbb{Q}(\zeta)$ is the splitting field of $x^5 - 1$ over $\mathbb{Q}$.

b. Show that every automorphism of $K = \mathbb{Q}(\zeta)$ maps ζ onto some power ζ^r of ζ.

c. Using part (b), describe the elements of $G(K/\mathbb{Q})$.

d. Give the group and field diagrams for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, computing the intermediate fields as we did in Examples 47.3 and 47.7.

5. Describe the group of the polynomial $(x^5 - 2) \in (\mathbb{Q}(\zeta))[x]$ over $\mathbb{Q}(\zeta)$, where ζ is a primitive 5th root of unity.

6. Repcat Exercise 4 for ζ a primitive 7th root of unity in $\mathbb{C}$.

7. In the easiest way possible, describe the group of the polynomial

$$(x^8 - 1) \in \mathbb{Q}[x]$$

over $\mathbb{Q}$.

8. Find the splitting field K in $\mathbb{C}$ of the polynomial $(x^4 - 4x^2 - 1) \in \mathbb{Q}[x]$. Compute the group of the polynomial over $\mathbb{Q}$ and exhibit the correspondence between the subgroups of $G(K/\mathbb{Q})$ and the intermediate fields. In other words, do the complete job.

9. Express each of the following symmetric functions in y_1, y_2, y_3 over $\mathbb{Q}$ as a rational function of the elementary symmetric functions s_1, s_2, s_3.

a. ${y_1}^2 + {y_2}^2 + {y_3}^2$

b. $\dfrac{y_1}{y_2} + \dfrac{y_2}{y_1} + \dfrac{y_1}{y_3} + \dfrac{y_3}{y_1} + \dfrac{y_2}{y_3} + \dfrac{y_3}{y_2}$

10. Let $\alpha_1, \alpha_2, \alpha_3$ be the zeros in $\mathbb{C}$ of the polynomial

$$(x^3 - 4x^2 + 6x - 2) \in \mathbb{Q}[x].$$

Find the polynomial having as zeros precisely the following:

a. $\alpha_1 + \alpha_2 + \alpha_3$

b. ${\alpha_1}^2, {\alpha_2}^2, {\alpha_3}^2$

Theory

11. Show that every finite group is isomorphic to some Galois group $G(K/F)$ for some finite normal extension K of some field F.

12. Let $f(x) \in F[x]$ be a monic polynomial of degree n having all its irreducible factors separable over F. Let K be the splitting field of $f(x)$ over F, and suppose that $f(x)$ factors in $K[x]$ into

$$\prod_{i=1}^{n}(x - \alpha_i).$$

Let

$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j);$$

the product $(\Delta(f))^2$ is the **discriminant of** $f(x)$.

a. Show that $\Delta(f) = 0$ if and only if $f(x)$ has as a factor the square of some irreducible polynomial in $F[x]$.

b. Show that $(\Delta(f))^2 \in F$.

c. $G(K/F)$ may be viewed as a subgroup of $\overline{S_n}$, where $\overline{S_n}$ is the group of all permutations of $\{\alpha_i \mid i = 1, \cdots, n\}$. Show that $G(K/F)$, when viewed in this fashion, is a subgroup of $\overline{A_n}$, the group formed by all even permutations of $\{\alpha_i \mid i = 1, \cdots, n\}$, if and only if $\Delta(f) \in F$.

13. An element of $\mathbb{C}$ is an **algebraic integer** if it is a zero of some *monic* polynomial in $\mathbb{Z}[x]$. Show that the set of all algebraic integers forms a subring of $\mathbb{C}$.

SECTION 48 CYCLOTOMIC EXTENSIONS

The Galois Group of a Cyclotomic Extension

In this section we consider subfields of the complex numbers obtained by adjoining roots of unity to the rational numbers, $\mathbb{Q}$. We apply Galois theory to these extensions to determine which regular n-gons are constructible.

48.1 Definition The splitting field of $x^n - 1$ over a field F is the ***n*th cyclotomic extension of** F. ■

Since fields of characteristic zero are perfect, the splitting field, K, of $f(x) = x^n - 1$ over $\mathbb{Q}$ is separable and thus a normal extension of $\mathbb{Q}$. The distinct n zeros of $f(x)$ form a cyclic group U_n. (See Section 3.) We saw in Corollary 6.17 that the number of generators of a cyclic group of order n is the number of positive integers less than n that are relatively prime to n, which we defined to be the Euler phi-function $\varphi(n)$. These $\varphi(n)$ generators are exactly the primitive nth roots of unity.

48.2 Definition The polynomial

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)}(x - \alpha_i)$$

where the α_i are the primitive nth roots of unity in $\mathbb{Q}$, is the ***n*th cyclotomic polynomial over** $\mathbb{Q}$. ■

Let $\sigma \in G(K/\mathbb{Q})$. Since an automorphism of the Galois group $G(K/\mathbb{Q})$ must permute the primitive nth roots of unity, we see that $\sigma_x(\Phi_n(x)) = \Phi_n(x)$, where $\sigma_x : K[x] \to K[x]$ is the polynomial extension of σ. Thus the coefficients of Φ_n are fixed by every $\sigma \in G(K/\mathbb{Q})$, and therefore, all the coefficients of $\Phi_n(x)$ are rational numbers. That is, $\Phi_n(x) \in \mathbb{Q}[x]$. The nth cyclotomic polynomial $\Phi_n(x)$ must divide $x^n - 1$, so $\Phi_n(x) \in \mathbb{Z}[x]$ by Theorem 28.12. For p a prime number, Corollary 28.18 says that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$. Although we do not prove it here, it can be shown that $\Phi_n(x)$ is irreducible even when $n \geq 2$ is not a prime number.

■ HISTORICAL NOTE

Carl Gauss considered cyclotomic polynomials in the final chapter of his *Disquisitiones Arithmeticae* of 1801. In that chapter, he gave a constructive procedure for actually determining the roots of $\Phi_p(x)$ in the case where p is prime. Gauss's method, which became an important example for Galois in the development of the general theory, was to solve a series of auxiliary equations, each of degree a prime factor of $p-1$, with the coefficients of each in turn being determined by the roots of the previous equation. Gauss, of course, knew that the roots of $\Phi_p(x)$ were all powers of one of them, say ζ. He determined the auxiliary equations by taking certain sets of sums of the roots ζ^j, which were the desired roots of these equations. For example, in the case where $p = 19$ (and $p - 1 = 18 = 3 \times 3 \times 2$), Gauss needed to find two equations of degree 3 and one of degree 2 as his auxiliaries. It turned out that the first one had the three roots, $\alpha_1 = \zeta + \zeta^8 + \zeta^7 + \zeta^{18} + \zeta^{11} + \zeta^{12}, \alpha_2 = \zeta^2 + \zeta^{16} + \zeta^{14} + \zeta^{17} + \zeta^3 + \zeta^5$, and $\alpha_3 = \zeta^4 + \zeta^{13} + \zeta^9 + \zeta^{15} + \zeta^6 + \zeta^{10}$. In fact, these three values are the roots of the cubic equation $x^3 + x^2 - 6x - 7$. Gauss then found a second cubic equation, with coefficients involving the α's, whose roots were sums of two of the powers of ζ, and finally a quadratic equation, whose coefficients involved the roots of the previous equation, which had ζ as one of its roots. Gauss then asserted (without a complete proof) that each auxiliary equation can in turn be reduced to an equation of the form $x^m - A$, which clearly can be solved by radicals. That is, he showed that the solvability of the Galois group in this case, the cyclic group of order $p-1$, implied that the cyclotomic equation was solvable in terms of radicals. (See Section 49.)

Let i be the usual complex zero of $x^2 + 1$. Our work with complex numbers in Section 3 shows that

$$\left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^n = \cos 2\pi + i\sin 2\pi = 1,$$

so $\cos(2\pi/n) + i\sin(2\pi/n)$ is an nth root of unity. The least integer m such that $(\cos(2\pi/n) + i\sin(2\pi/n))^m = 1$ is n. *Thus* $\cos(2\pi/n) + i\sin(2\pi/n)$ *is a primitive* n*th root of unity, a zero of*

$$\Phi_n(x) \in \mathbb{Q}[x].$$

48.3 Example A primitive 8th root of unity in $\mathbb{C}$ is

$$\begin{aligned}\zeta &= \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8}\\ &= \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\\ &= \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} = \frac{1+i}{\sqrt{2}}.\end{aligned}$$

By the theory of cyclic groups, in particular by Corollary 6.17, all the primitive 8th roots of unity in $\mathbb{Q}$ are ζ, ζ^3, ζ^5, and ζ^7, so

$$\Phi_8(x) = (x-\zeta)(x-\zeta^3)(x-\zeta^5)(x-\zeta^7).$$

We can compute, directly from this expression, $\Phi_8(x) = x^4 + 1$ (see Exercise 1). Compare this with Example 47.7. ▲

Let us assume, without proof, that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. Let

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

so that ζ is a primitive nth root of unity. Note that ζ is a generator of the cyclic multiplicative group of order n consisting of *all* nth roots of unity. All the primitive nth roots of unity, that is, all the generators of this group, are of the form ζ^m for $1 \leq m < n$ and m relatively prime to n. The field $\mathbb{Q}(\zeta)$ is the whole splitting field of $x^n - 1$ over $\mathbb{Q}$. Let $K = \mathbb{Q}(\zeta)$. If ζ^m is another primitive nth root of unity, then since ζ and ζ^m are conjugate over $\mathbb{Q}$, there is an automorphism τ_m in $G(K/\mathbb{Q})$ mapping ζ onto ζ^m. Let τ_r be the similar automorphism in $G(K/\mathbb{Q})$ corresponding to a primitive nth root of unity ζ^r. Then

$$(\tau_m \tau_r)(\zeta) = \tau_m(\zeta^r) = (\tau_m(\zeta))^r = (\zeta^m)^r = \zeta^{rm}.$$

This shows that composing automorphisms τ_m and τ_r corresponds to multiplying m and r modulo n. In other words, the Galois group $G(K/\mathbb{Q})$ is isomorphic with the group of units in $\mathbb{Z}_n$ under multiplication, with the isomorphism mapping τ_m to m. The units in $\mathbb{Z}_n$ are the numbers less than n that are relatively prime to n. Thus $G(K/\mathbb{Q})$ is an abelian group with $\varphi(n)$ elements.

Special cases of this material have appeared several times in the text and exercises. For example, α of Example 47.7 is a primitive 8th root of unity, and we made arguments in that example identical to those given here. We summarize these results in a theorem.

48.4 Theorem The Galois group of the nth cyclotomic extension of $\mathbb{Q}$ has $\varphi(n)$ elements and is isomorphic to the group consisting of the positive integers less than n and relatively prime to n under multiplication modulo n.

48.5 Example Example 47.7 illustrates this theorem, for it is easy to see that the splitting field of $x^4 + 1$ is the same as the splitting field of $x^8 - 1$ over $\mathbb{Q}$. This follows from the fact that $\Phi_8(x) = x^4 + 1$ (see Example 48.3 and Exercise 1). ▲

48.6 Corollary The Galois group of the pth cyclotomic extension of $\mathbb{Q}$ for a prime p is cyclic of order $p - 1$.

Proof By Theorem 48.4, the Galois group of the pth cyclotomic extension of $\mathbb{Q}$ has $\varphi(p) = p - 1$ elements, and is isomorphic to the group of positive integers less than p and relatively prime to p under multiplication modulo p. This is exactly the multiplicative group $\langle \mathbb{Z}_p^*, \cdot \rangle$ of nonzero elements of the field $\mathbb{Z}_p$ under field multiplication. By Corollary 28.7, this group is cyclic. ◆

Constructible Polygons

We conclude with an application determining which regular n-gons are constructible with a compass and a straightedge. We saw in Section 41 that the regular n-gon is constructible if and only if $\cos(2\pi/n)$ is a constructible real number. Now let

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Then

$$\frac{1}{\zeta} = \cos\frac{2\pi}{n} - i\sin\frac{2\pi}{n},$$

for

$$\left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)\left(\cos\frac{2\pi}{n} - i\sin\frac{2\pi}{n}\right) = \cos^2\frac{2\pi}{n} + \sin^2\frac{2\pi}{n} = 1.$$

But then

$$\zeta + \frac{1}{\zeta} = 2\cos\frac{2\pi}{n}.$$

Thus Corollary 41.8 shows that the regular n-gon is constructible only if $\zeta + 1/\zeta$ generates an extension of $\mathbb{Q}$ of degree a power of 2.

If K is the splitting field of $x^n - 1$ over $\mathbb{Q}$, then $[K : \mathbb{Q}] = \varphi(n)$, by Theorem 48.4. If $\sigma \in G(K/\mathbb{Q})$ and $\sigma(\zeta) = \zeta^r$, then

$$\begin{aligned}\sigma\left(\zeta + \frac{1}{\zeta}\right) &= \zeta^r + \frac{1}{\zeta^r} \\ &= \left(\cos\frac{2\pi r}{n} + i\sin\frac{2\pi r}{n}\right) + \left(\cos\frac{2\pi r}{n} - i\sin\frac{2\pi r}{n}\right) \\ &= 2\cos\frac{2\pi r}{n}.\end{aligned}$$

But for $1 < r < n$, we have $2\cos(2\pi r/n) = 2\cos(2\pi/n)$ only in the case that $r = n - 1$. Thus the only elements of $G(K/\mathbb{Q})$ carrying $\zeta + 1/\zeta$ onto itself are the identity automorphism and the automorphism τ, with $\tau(\zeta) = \zeta^{n-1} = 1/\zeta$. This shows that the subgroup of $G(K/\mathbb{Q})$ leaving $\mathbb{Q}(\zeta + 1/\zeta)$ fixed is of order 2, so by Galois theory,

$$\left[\mathbb{Q}\left(\zeta + \frac{1}{\zeta}\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2}.$$

Hence the regular n-gon is constructible only if $\varphi(n)/2$, and therefore also $\varphi(n)$, is a power of 2.

It can be shown by elementary arguments in number theory that if

$$n = 2^v {p_1}^{s_1} \cdots {p_t}^{s_t},$$

where the p_i are the distinct odd primes dividing n, then

$$\varphi(n) = 2^{v-1}{p_1}^{s_1-1} \cdots {p_t}^{s_t-1}(p_1 - 1) \cdots (p_t - 1). \tag{1}$$

If $\varphi(n)$ is to be a power of 2, then every odd prime dividing n must appear only to the first power and must be one more than a power of 2. Thus we must have each

$$p_i = 2^m + 1$$

for some m. Since -1 is a zero of $x^q + 1$ for q an odd prime, $x + 1$ divides $x^q + 1$ for q an odd prime. Thus, if $m = qu$, where q is an odd prime, then $2^m + 1 = (2^u)^q + 1$ is divisible by $2^u + 1$. Therefore, for $p_i = 2^m + 1$ to be prime, it must be that m is divisible by 2 only, so p_i has to have the form

$$p_i = 2^{(2^k)} + 1,$$

a **Fermat prime.** Fermat conjectured that these numbers $2^{(2^k)} + 1$ were prime for all nonnegative integers k. Euler showed that while $k = 0, 1, 2, 3$, and 4 give the primes 3, 5, 17, 257, and 65537, for $k = 5$, the integer $2^{(2^5)} + 1$ is divisible by 641. It has been shown that for $5 \le k \le 19$, all the numbers $2^{(2^k)} + 1$ are composite. The case $k = 20$ is still unsolved as far as we know. For at least 60 values of k greater than 20, including $k = 9448$, it has been shown that $2^{2^k} + 1$ is composite. It is unknown whether the number of Fermat primes is finite or infinite.

We have thus shown that the only regular n-gons that might be constructible are those where the odd primes dividing n are Fermat primes whose squares do not divide n. In particular, the only regular p-gons that might be constructible for p a prime greater than 2 are those where p is a Fermat prime.