48.7 Example The regular 7-gon is not constructible, since 7 is not a Fermat prime. Similarly, the regular 18-gon is not constructible, for while 3 is a Fermat prime, its square divides 18. ▲

We now demonstrate that all these regular n-gons that are candidates for being constructible are indeed actually constructible. Let ζ again be the primitive nth root of unity $\cos(2\pi/n) + i\sin(2\pi/n)$. We saw above that

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

and that

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

Suppose now that $\varphi(n)$ is a power 2^s of 2. We saw above that $\mathbb{Q}(\zeta + 1/\zeta)$ is the subfield of $K = \mathbb{Q}(\zeta)$ fixed by $H_1 = \{\iota, \tau\}$, where ι is the identity element of $G(K/\mathbb{Q})$ and $\tau(\zeta) = 1/\zeta$. By Sylow theory, there exist additional subgroups H_j of order 2^j of $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ for $j = 0, 2, 3, \cdots, s$ such that

$$\{\iota\} = H_0 < H_1 < \cdots < H_s = G(\mathbb{Q}(\zeta)/\mathbb{Q}).$$

By Galois theory,

$$\mathbb{Q} = K_{H_s} < K_{H_{s-1}} < \cdots < K_{H_1} = \mathbb{Q}\left(\zeta + \frac{1}{\zeta}\right),$$

and $[K_{H_{j-1}} : K_H] = 2$. Note that $(\zeta + 1/\zeta) \in \mathbb{R}$, so $\mathbb{Q}(\zeta + 1/\zeta) < \mathbb{R}$. If $K_{H_{j-1}} = K_{H_j}(\alpha_j)$, then α_j is a zero of some $(a_j x^2 + b_j x + c_j) \in K_{H_j}[x]$. By the familiar "quadratic formula," we have

$$K_{H_{j-1}} = K_{H_j}\left(\sqrt{b_j{}^2 - 4a_j c_j}\right).$$

Since we saw in Section 41 that construction of square roots of positive constructible numbers can be achieved by a straightedge and a compass, we see that every element in $\mathbb{Q}(\zeta + 1/\zeta)$, in particular $\cos(2\pi/n)$, is constructible. Hence the regular n-gons where $\varphi(n)$ is a power of 2 are constructible.

We summarize our work under this heading in a theorem.

48.8 Theorem The regular n-gon is constructible with a compass and a straightedge if and only if all the odd primes dividing n are Fermat primes whose squares do not divide n.

48.9 Example The regular 60-gon is constructible, since $60 = (2^2)(3)(5)$ and 3 and 5 are both Fermat primes. ▲

EXERCISES 48

Computations

1. Referring to Example 48.3, complete the indicated computation, showing that $\Phi_8(x) = x^4 + 1$. [*Suggestion:* Compute the product in terms of ζ, and then use the fact that $\zeta^8 = 1$ and $\zeta^4 = -1$ to simplify the coefficients.]

2. Classify the group of the polynomial $(x^{20} - 1) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ according to the Fundamental Theorem of Finitely Generated Abelian Groups. Theorem 9.12. [*Hint:* Use Theorem 48.4.]

3. Using the formula for $\varphi(n)$ in terms of the factorization of n, as given in Eq. (1), compute the indicated value:

a. $\varphi(60)$ **b.** $\varphi(1000)$ **c.** $\varphi(8100)$

4. Give the first 30 values of $n \geq 3$ for which the regular n-gon is constructible with a straightedge and a compass.

5. Find the smallest angle of integral degree, that is, $1°, 2°, 3°$, and so on, constructible with a straightedge and a compass. [*Hint:* Constructing a $1°$ angle amounts to constructing the regular 360-gon, and so on.]

6. Let K be the splitting field of $x^{12} - 1$ over $\mathbb{Q}$.

a. Find $[K : \mathbb{Q}]$.

b. Show that for $\sigma \in G(K/\mathbb{Q})$, σ^2 is the identity automorphism. Classify $G(K/\mathbb{Q})$ according to the Fundamental Theorem 9.12 of finitely generated abelian groups.

Concepts

7. Determine whether each of the following is true or false.

a. $\Phi_n(x)$ is irreducible over every subfield of $\mathbb{C}$.

b. Every zero in $\mathbb{C}$ of $\Phi_n(x)$ is a primitive nth root of unity.

c. The group of $\Phi_n(x) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ has order n.

d. The group of $\Phi_n(x) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ is abelian.

e. The Galois group of the splitting field of $\Phi_n(x)$ over $\mathbb{Q}$ has order $\varphi(n)$.

f. The regular 25-gon is constructible with a straightedge and a compass.

g. The regular 17-gon is constructible with a straightedge and a compass.

h. For a prime p, the regular p-gon is constructible if and only if p is a Fermat prime.

i. All integers of the form $2^{(2^k)} + 1$ for nonnegative integers k are Fermat primes.

j. All Fermat primes are numbers of the form $2^{(2^k)} + 1$ for nonnegative integers k.

Theory

8. Show that

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

in $\mathbb{Q}[x]$, where the product is over all divisors d of n.

9. Find the cyclotomic polynomial $\Phi_n(x)$ over $\mathbb{Q}$ for $n = 1, 2, 3, 4, 5$, and 6. [*Hint:* Use Exercise 8.]

10. Find $\Phi_{12}(x)$ in $\mathbb{Q}[x]$. [*Hint:* Use Exercises 8 and 9.]

11. Show that in $\mathbb{Q}[x]$, $\Phi_{2n}(x) = \Phi_n(-x)$ for odd integers $n > 1$. [*Hint:* If ζ is a primitive nth root of unity for n odd, what is the order of $-\zeta$?]

12. Let $n, m \in \mathbb{Z}^+$ be relatively prime. Show that the splitting field in $\mathbb{C}$ of $x^{nm} - 1$ over $\mathbb{Q}$ is the same as the splitting field in $\mathbb{C}$ of $(x^n - 1)(x^m - 1)$ over $\mathbb{Q}$.

13. Let $n, m \in \mathbb{Z}^+$ be relatively prime. Show that the group of $(x^{nm} - 1) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ is isomorphic to the direct product of the groups of $(x^n - 1) \in \mathbb{Q}[x]$ and of $(x^m - 1) \in \mathbb{Q}[x]$ over $\mathbb{Q}$. [*Hint:* Using Galois theory, show that the groups of $x^m - 1$ and $x^n - 1$ can both be regarded as subgroups of the group of $x^{nm} - 1$. Then use Exercises 50 and 51 of Section 9.]

SECTION 49 INSOLVABILITY OF THE QUINTIC

The Problem

We are familiar with the fact that a quadratic polynomial $f(x) = ax^2 + bx + c, a \neq 0$, with real coefficients has $(-b \pm \sqrt{b^2 - 4ac})/2a$ as zeros in $\mathbb{C}$. Actually, this is true for $f(x) \in F[x]$, where F is any field of characteristic $\neq 2$ and the zeros are in $\bar{F}$. Exercise 4 asks us to show this. Thus, for example, $(x^2 + 2x + 3) \in \mathbb{Q}[x]$ has its zeros in $\mathbb{Q}(\sqrt{-2})$. You may wonder whether the zeros of a cubic polynomial over $\mathbb{Q}$ can also always be expressed in terms of radicals. The answer is yes, and indeed, even the zeros of a polynomial of degree 4 over $\mathbb{Q}$ can be expressed in terms of radicals. After mathematicians had tried for years to find the "radical formula" for zeros of a 5th degree polynomial, it was a triumph when Abel proved that a quintic need not be solvable by radicals. Our first job will be to describe precisely what this means. A large amount of the algebra we have developed is used in the forthcoming discussion.

Extensions by Radicals

49.1 Definition An extension K of a field F is an **extension of F by radicals** if there are elements $\alpha_1, \cdots, \alpha_r \in K$ and positive integers $n_1, \cdots, n_r$ such that $K = F(\alpha_1, \cdots, \alpha_r), \alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \cdots, \alpha_{i-1})$ for $1 < i \leq r$. A polynomial $f(x) \in F[x]$ is **solvable by radicals over** F if the splitting field E of $f(x)$ over F is contained in an extension of F by radicals. ■

A polynomial $f(x) \in F(x)$ is thus solvable by radicals over F if we can obtain every zero of $f(x)$ by using a finite sequence of the operations of addition, subtraction, multiplication, division, and taking n_ith roots, starting with elements of F. Now to say that the quintic is not solvable in the classic case, that is, characteristic 0, is not to say that no quintic is solvable, as the following example shows.

49.2 Example The polynomial $x^5 - 1$ is solvable by radicals over $\mathbb{Q}$. The splitting field K of $x^5 - 1$ is generated over $\mathbb{Q}$ by a primitive 5th root ζ of unity. Then $\zeta^5 = 1$, and $K = \mathbb{Q}(\zeta)$. Similarly, $x^5 - 2$ is solvable by radicals over $\mathbb{Q}$, for its splitting field over $\mathbb{Q}$ is generated by $\sqrt[5]{2}$ and ζ, where $\sqrt[5]{2}$ is the real zero of $x^5 - 2$. ▲

To say that the quintic is insolvable in the classic case means that there exists *some* polynomial of degree 5 with real coefficients that is not solvable by radicals. We shall show this. *We assume throughout this section that all fields mentioned have characteristic 0.*

The outline of the argument is as follows, and it is worthwhile to try to remember it.

1. *We shall show that a polynomial $f(x) \in F[x]$ is solvable by radicals over F (if and) only if its splitting field E over F has a solvable Galois group*. Recall that a solvable group is one having a composition series with *abelian* quotients. While this theorem goes both ways, we shall not prove the "if" part.
2. *We shall show that there is a polynomial $f(x) \in \Phi[x]$ of degree 5 with a splitting field E over $\mathbb{Q}$ such that $G(E/\mathbb{Q}) \simeq S_5$, the symmetric group on 5 letters*. Recall that a composition series for S_5 is $\{\iota\} < A_5 < S_5$. Since A_5 is not abelian, we will be done.

The following lemma does most of our work for Step 1.

49.3 Lemma Let F be a field of characteristic 0, and let $a \in F$. If K is the splitting field of $x^n - a$ over F, then $G(K/F)$ is a solvable group.

Historical Note

The first publication of a formula for solving cubic equations in terms of radicals was in 1545 in the *Ars Magna* of Girolamo Cardano, although the initial discovery of the method is in part also due to Scipione del Ferro and Niccolo Tartaglia. Cardano's student, Lodovico Ferrari, discovered a method for solving quartic equations by radicals, which also appeared in Cardano's work.

After many mathematicians had attempted to solve quintics by similar methods, it was Joseph-Louis Lagrange who in 1770 first attempted a detailed analysis of the general principles underlying the solutions for polynomials of degree 3 and 4, and showed why these methods fail for those of higher degree. His basic insight was that in the former cases there were rational functions of the roots that took on two and three values, respectively, under all possible permutations of the roots, hence these rational functions could be written as roots of equations of degree less than that of the original. No such functions were evident in equations of higher degree.

The first mathematician to claim to have a proof of the insolvability of the quintic equation was Paolo Ruffini (1765–1822) in his algebra text of 1799. His proof was along the lines suggested by Lagrange, in that he in effect determined all of the subgroups of S_5 and showed how these subgroups acted on rational functions of the roots of the equation. Unfortunately, there were several gaps in his various published versions of the proof. It was Niels Henrik Abel who, in 1824 and 1826, published a complete proof, closing all of Ruffini's gaps and finally settling this centuries-old question.

Proof Suppose first that F contains all the nth roots of unity. By Corollary 28.7 the nth roots of unity form a cyclic subgroup of $\langle F^*, \cdot \rangle$. Let ζ be a generator of the subgroup. (Actually, the generators are exactly the *primitive* nth roots of unity.) Then the nth roots of unity are

$$1, \zeta, \zeta^2, \cdots, \zeta^{n-1}.$$

If $\beta \in \bar{F}$ is a zero of $(x^n - a) \in F[x]$, then all zeros of $x^n - a$ are

$$\beta, \zeta\beta, \zeta^2\beta, \cdots, \zeta^{n-1}\beta.$$

Since $K = F(\beta)$, an automorphism σ in $G(K/F)$ is determined by the value $\sigma(\beta)$ of the automorphism σ on β. Now if $\sigma(\beta) = \zeta^i\beta$ and $\tau(\beta) = \zeta^j\beta$, where $\tau \in G(K/F)$, then

$$(\tau\sigma)(\beta) = \tau(\sigma(\beta)) = \tau(\zeta^i\beta) = \zeta^i\tau(\beta) = \zeta^i\zeta^j\beta,$$

since $\zeta^i \in F$. Similarly,

$$(\sigma\tau)(\beta) = \zeta^j\zeta^i\beta.$$

Thus $\sigma\tau = \tau\sigma$, and $G(K/F)$ is abelian and therefore solvable.

Now suppose that F does not contain a primitive nth root of unity. Let ζ be a generator of the cyclic group of nth roots of unity under multiplication in $\bar{F}$. Let β again be a zero of $x^n - a$. Since β and $\zeta\beta$ are both in the splitting field K of $x^n - a, \zeta = (\zeta\beta)/\beta$ is in K. Let $F' = F(\zeta)$, so we have $F < F' \leq K$. Now F' is a normal extension of F, since F' is the splitting field of $x^n - 1$. Since $F' = F(\zeta)$, an automorphism η in $G(F'/F)$ is determined by $\eta(\zeta)$, and we must have $\eta(\zeta) = \zeta^i$ for some i, since all zeros of $x^n - 1$ are powers of ζ. If $\mu(\zeta) = \zeta^j$ for $\mu \in G(F'/F)$, then

$$(\mu\eta)(\zeta) = \mu(\eta(\zeta)) = \mu(\zeta^i) = \mu(\zeta)^i = (\zeta^j)^i = \zeta^{ij},$$

and, similarly,

$$(\eta\mu)(\zeta) = \zeta^{ij}.$$

Thus $G(F'/F)$ is abelian. By Theorem 46.10,

$$\{\iota\} \leq G(K/F') \leq G(K/F)$$

is a normal series and hence a subnormal series of groups. The first part of the proof shows that $G(K/F')$ is abelian, and Galois theory tells us that $G(K/F)/G(K/F')$ is isomorphic to $G(F'/F)$, which is abelian. Exercise 6 shows that if a group has a subnormal series of subgroups with abelian quotient groups, then any refinement of this series also has abelian quotient groups. Thus a composition series of $G(K/F)$ must have abelian quotient groups, so $G(K/F)$ is solvable. ◆

The following theorem will complete Step 1 of our program.

49.4 Theorem Let F be a field of characteristic zero, and let $F \leq E \leq K \leq \bar{F}$, where E is a normal extension of F and K is an extension of F by radicals. Then $G(E/F)$ is a solvable group.

Proof We first show that K is contained in a finite normal extension L of F by radicals and that the group $G(L/F)$ is solvable. Since K is an extension of F by radicals, $K = F(\alpha_1, \cdots, \alpha_r)$ where $\alpha_i^{n_i} \in F(\alpha_1, \cdots, \alpha_{i-1})$ for $1 < i \leq r$ and $\alpha_1^{n_1} \in F$. To form L, we first form the splitting field L_1 of $f_1(x) = x^{n_1} - \alpha_1^{n_1}$ over F. Then L_1 is a normal extension of F, and Lemma 49.3 shows that $G(L_1/F)$ is a solvable group. Now $\alpha_2^{n_2} \in L_1$ and we form the polynomial

$$f_2(x) = \prod_{\sigma \in G(L_1/F)} [(x^{n_2} - \sigma(\alpha_2)^{n_2}].$$

Since this polynomial is invariant under action by any σ in $G(L_1/F)$, we see that $f_2(x) \in F[x]$. We let L_2 be the splitting field of $f_2(x)$ over L_1. Then L_2 is a splitting field over F also and is a normal extension of F by radicals. We can form L_2 from L_1 via repeated steps as in Lemma 49.3, passing to a splitting field of $x^{n_2} - \sigma(\alpha_2)^{n_2}$ at each step. By Lemma 49.3 and Exercise 7, we see that the Galois group over F of each new extension thus formed continues to be solvable. We continue this process of forming splitting fields over F in this manner: At stage i, we form the splitting field of the polynomial

$$f_i(x) = \prod_{\sigma \in G(L_{i-1}/F)} [(x^{n_i} - \sigma(\alpha_i)^{n_i}]$$

over L_{i-1}. We finally obtain a field $L = L_r$ that is a normal extension of F by radicals, and we see that $G(L/F)$ is a solvable group. We see from construction that $K \leq L$.

To conclude, we need only note that by Theorem 46.8, we have $G(E/F) \simeq G(L/F)/G(L/E)$. Thus $G(E/F)$ is a factor group, and hence a homomorphic image, of $G(L/F)$. Since $G(L/F)$ is solvable, Exercise 31 of Section 18 shows that $G(E/F)$ is solvable. ◆

The Insolvability of the Quintic

It remains to find a polynomial $f(x) \in \mathbb{Q}[x]$, whose splitting field has Galois group S_5. The polynomial $f(x) = 2x^5 - 5x^4 + 5$ does the trick as we now show. To begin, we prove the following theorem that gives a simple condition for a subgroup of S_5 to actually be all of S_5. We will use this theorem to show that the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$ is isomorphic with S_5.

49.5 Theorem Let H be a subgroup of S_5. If H has a transposition and a 5-cycle, then $H = S_5$.

Proof We can assume, by relabeling the points being permuted, that the 5-cycle $(0, 1, 2, 3, 4)$ is in H and the transposition $(0, j)$, $j \neq 0$, is also in H. We think of S_5 as permuting the

elements in $\mathbb{Z}_5$. By conjugating with the 5-cycle $(0,1,2,3,4)^r$, we have that for each $0 \leq r \leq 4$,

$$(0,1,2,3,4)^r(0,j)(0,1,2,3,4)^{-r} = (r, r+j),$$

where addition is in $\mathbb{Z}_5$. Thus $(0,j)$ and $(j,2j)$ are both in H; and therefore

$$(0,j)(j,2j)(0,j) = (0,2j) \in H.$$

As before, by conjugating $(0,2j)$ with $(0,1,2,3,4)^r$ we have $(r, r+2j) \in H$ for $0 \leq r \leq 4$. Now,

$$(0,2j)(2j,3j)(0,2j) = (0,3j) \in H.$$

Again, conjugating with powers of $(0,1,2,3,4)$ shows that $(r, r+3j) \in H$. Furthermore,

$$(0,3j)(3j,4j)(0,3j) = (0,4j) \in H$$

and $(r, r+4j) \in H$. Summarizing, we have that

$$\{(r, r+sj \mid r \in \mathbb{Z}_5 \text{ and } s = \mathbb{Z}_5^*\} \in H.$$

But

$$\{sj \mid s \in \mathbb{Z}_5^*\} = \mathbb{Z}_5^*$$

since $j \neq 0$ is a unit in the field $\mathbb{Z}_5$. Therefore, H contains all the transpositions in the set

$$\{(r, r+sj) \mid r \in \mathbb{Z}_5 \text{ and } s \in \mathbb{Z}_5^*\} = \{(r, r+t) \mid r \in \mathbb{Z}_5 \text{ and } t \in \mathbb{Z}_5^*\}.$$

This is the set of all transpositions in S_5. By Theorem 8.15, $H = S_5$. ◆

We now turn our attention back to the polynomial $f(x) = 2x^5 - 5x^4 + 5$. We first observe that $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, Theorem 28.16, using $p = 5$. In order to better understand the zeros of $f(x)$, we compute the following.

$$\begin{aligned} f(-1) &= -2 < 0 \\ f(0) &= 5 > 0 \\ f(2) &= -11 < 0 \\ f(3) &= 86 > 0 \end{aligned}$$

The intermediate value theorem from calculus says that if $f(x)$ is a continuous function and $f(a)$ and $f(b)$ have opposite signs, then $f(x)$ has a zero between a and b. Since the polynomial $f(x)$ is continuous, we have at least three real number zeros of $f(x)$; one between -1 and 0, one between 0 and 2, and the third between 2 and 3. The derivative of $f(x)$ is

$$f'(x) = 10x^4 - 20x^3 = 10x^3(x-2).$$

The only zeros of $f'(x)$ are 0 and 2. By the mean value theorem from calculus, between any two real number zeros of $f(x)$, there is a zero of $f'(x)$. Therefore, there cannot be more than three zeros of $f(x)$ that are real numbers. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Since $f(x)$ is irreducible over $\mathbb{Q}$ and $\mathbb{Q}$ is a perfect field, K contains five distinct zeros of $f(x)$. Thus $f(x)$ has two complex zeros, and they are complex conjugates.

We have that $G(K/\mathbb{Q})$ is isomorphic with a subgroup of the permutation group of the zeros of $f(x)$. The isomorphism maps each σ to the permutation given by the map σ restricted to the zeros of $f(x)$. For any zero $\alpha \in K$ of $f(x)$,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(\text{irr}(\alpha, \mathbb{Q})) = \deg(f(x)) = 5.$$