23. Solving equations by radicals

Around 1800, Ruffini sketched a proof, completed by Abel, that the general quintic equation is *not* solvable in radicals, by contrast to cubics and quartics whose solutions by radicals were found in the Italian renaissance, not to mention quadratic equations, understood in antiquity. Ruffini's proof required classifying the possible forms of radicals. By contrast, Galois' systematic development of the idea of *automorphism group* replaced the study of the expressions themselves with the study of their movements.

Galois theory solves some classical problems. Ruler-and-compass constructions, in coordinates, can *only* express quantities in repeated quadratic extensions of the field generated by given points, but nothing else. Thus, *trisection of angles* by ruler and compass is impossible for general-position angles, since the general trisection requires a cube root.

The examples and exercises continue with other themes.

1. *Galois' criterion*

We will not prove all the results in this section, for several reasons. First, solution of equations in radicals is no longer a critical or useful issue, being mostly of historical interest. Second, in general it is non-trivial to verify (or disprove) Galois' condition for solvability in radicals. Finally, to understand that Galois' condition is *intrinsic* requires the Jordan-Hölder theorem on *composition series* of groups (stated below). While its statement is clear, the proof of this result is technical, difficult to understand, and not re-used elsewhere here.

[1.0.1] Theorem: Let G be the Galois group of the splitting field K of an irreducible polynomial f over k. If G has a sequence of subgroups

$$\{1\} \subset G_1 \subset G_2 \subset \ldots \subset G_m = G$$

such that G_i is *normal* in G_{i+1} and G_{i+1}/G_i is *cyclic* for every index i, then a root of $f(x) = 0$ can be expressed in terms of radicals. Conversely, if roots of f can be expressed in terms of radicals, then the Galois group G has such a chain of subgroups.

Proof: (*Sketch*) On one hand, adjunction of n roots is cyclic of degree n if the primitive n^{th} roots of unity are in the base field. If the n^{th} roots of unity are *not* in the base field, we can *adjoin* them by taking a field extension obtainable by successive root-taking of orders strictly less than n. Thus, root-taking amounts to successive cyclic extensions, which altogether gives a *solvable* extension. On the other hand, a solvable extension is given by successive cyclic extensions. After n^{th} roots of unity are adjoined (which requires successive cyclic extensions of degrees less than n), one can prove that any cyclic extension is obtained by adjoining roots of $x^n - a$ for some a in the base. This fact is most usefully proven by looking at *Lagrange resolvents.* ///

[1.0.2] Theorem: The *general* n^{th} degree polynomial equation is not solvable in terms of radicals for $n > 4$.

Proof: The meaning of *general* is that the Galois group is the largest possible, namely the symmetric group S_n on n things. Then we invoke the theorem to see that we must prove that S_n is *not solvable* for $n > 4$. In fact, the normal subgroup A_n of S_n is *simple* for $n > 4$ (see just below), in the sense that it has no proper normal subgroups (and is not cyclic). In particular, A_n has no chain of subgroups normal in each other with cyclic quotients. This *almost* finishes the proof. What is missing is verifying the plausible claim that the simplicity of A_n means that no *other* possible chain of subgroups inside S_n can exist *with* cyclic quotients. We address this just below. ///

A group is **simple** if it has not proper normal subgroups (and maybe is not a cyclic group of prime order, and is not the trivial group). A group G with a chain of subgroups G_i, each normal in the next, with the quotients *cyclic*, is a **solvable** group, because of the conclusion of this theorem.

[1.0.3] Proposition: For $n \geq 5$ the alternating group A_n on n things is *simple.*

Proof: (*Sketch*) The trick is that for $n \geq 5$ the group A_n is generated by 3-cycles. Keeping track of 3-cycles, one can prove that the commutator subgroup of A_n, generated by expressions $xyx^{-1}y^{-1}$, for $x, y \in A_n$, is A_n itself. This yields the simplicity of A_n. ///

[1.0.4] Remark: A similar discussion addresses the question of **constructibility by ruler and compass**. One can prove that a point is *constructible* by ruler and compass if and only if its coordinates lie in a field extension of $\mathbb{Q}$ obtained by successive *quadratic* field extensions. Thus, for example, a regular n-gon can be constructed by ruler and compass exactly when $(\mathbb{Z}/n)^\times$ is a two-group. This happens exactly when n is of the form

$$n = 2^m \cdot p_1 \ldots p_\ell$$

where each p_i is a *Fermat prime*, that is, is a prime of the form $p = 2^{2^t} + 1$. Gauss constructed a regular 17-gon. The next Fermat prime is 257. Sometime in the early 19^{th} century someone *did* literally construct a regular 65537-gon, too.

2. *Composition series, Jordan-Hölder theorem*

Now we should check that the simplicity of A_n really does prevent there being any *other* chain of subgroups with cyclic quotients that might secretly permit a solution in radicals.

A **composition series** for a finite group G is a chain of subgroups

$$\{1\} \subset G_1 \subset \ldots \subset G_m = G$$

where each G_i is normal in G_{i+1} and the quotient G_{i+1}/G_i is either *cyclic of prime order* or *simple.* [1]

[2.0.1] **Theorem:** Let

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_m = G$$

$$\{1\} = H_0 \subset H_1 \subset \ldots \subset H_n = G$$

be two composition series for G. Then $m = n$ and the *sets* of quotients $\{G_{i+1}/G_i\}$ and $\{H_{j+1}/G_j\}$ (counting multiplicities) are identical.

Proof: (*Comments*) This theorem is quite non-trivial, and we will not prove it. The key ingredient is the *Jordan-Zassenhaus butterfly lemma*, which itself is technical and non-trivial. The proof of the analogue for modules over a ring is more intuitive, and is a worthwhile result in itself, which we leave to the reader. ///

3. *Solving cubics by radicals*

We follow *J.-L. Lagrange* to recover the renaissance Italian formulas of Cardan and Tartaglia in terms of radicals for the zeros of the general cubic

$$x^3 + ax^2 + bx + c$$

with a, b, c in a field k of characteristic neither 3 nor 2. [2] Lagrange's method creates an expression, the *resolvent*, having more accessible symmetries. [3]

Let ω be a primitive cube root of unity. Let α, β, γ be the three zeros of the cubic above. The **Lagrange resolvent** is

$$\lambda = \alpha + \omega \cdot \beta + \omega^2\gamma$$

The point is that any cyclic permutation of the roots alters λ by a cube root of unity. Thus, λ^3 is *invariant* under cyclic permutations of the roots, so we anticipate that λ^3 lies in a smaller field than do the roots. This is intended to reduce the problem to a simpler one.

Compute

$$\lambda^3 = \left(\alpha + \omega\beta + \omega^2\gamma\right)^3$$

[1] Again, it is often convenient that the notion of *simple* group makes an exception for cyclic groups of prime order.

[2] In characteristic 3, there are no primitive cube roots of 1, and the whole setup fails. In characteristic 2, unless we are somehow assured that the discriminant is a square in the ground field, the *auxiliary quadratic* which arises does not behave the way we want.

[3] The complication that cube roots of unity are involved was disturbing, historically, since complex number were viewed with suspicion until well into the 19th century.

$$= \alpha^3 + \beta^3 + \gamma^3 + 3\omega\alpha^2\beta + 3\omega^2\alpha\beta^2 + 3\omega^2\alpha^2\gamma + 3\omega\alpha\gamma^2 + 3\omega\beta^2\gamma + 3\omega^2\beta\gamma^2 + 6\alpha\beta\gamma$$

$$= \alpha^3 + \beta^3 + \gamma^3 + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega^2(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma) + 6\alpha\beta\gamma$$

Since $\omega^2 = -1 - \omega$ this is

$$\alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) - 3\omega(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma) - 3(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma)$$

In terms of the *elementary symmetric polynomials*

$$s_1 = \alpha + \beta_\gamma \qquad s_2 = \alpha\beta + \beta\gamma + \gamma\alpha \qquad s_3 = \alpha\beta\gamma$$

we have

$$\alpha^3 + \beta^3 + \gamma^3 = s_1^3 - 3s_1s_2 + 3s_3$$

Thus,

$$\lambda^3 = s_1^3 - 3s_1s_2 + 9s_3 + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) - 3\omega(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma) - 3(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma)$$

Neither of the two trinomials

$$A = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha \qquad B = \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$$

is invariant under *all* permutations of α, β, γ, but only under the subgroup generated by 3-*cycles*, so we cannot use symmetric polynomial algorithm to express these two trinomials *polynomially* in terms of elementary symmetric polynomials. [4]

But all is not lost, since $A + B$ and AB *are* invariant under *all* permutations of the roots, since any 2-cycle permutes A and B. So both $A + B$ and AB are expressible in terms of elementary symmetric polynomials, and then the two trinomials are the roots of

$$x^2 - (A + B)x + AB = 0$$

which is solvable by radicals in characteristic not 2.

We obtain the expression for $A+B$ in terms of elementary symmetric polynomials. Without even embarking upon the algorithm, a reasonable guess finishes the problem:

$$s_1s_2 - 3s_3 = (\alpha + \beta + \gamma)(\alpha\beta + \beta\gamma + \gamma\alpha) - 3\alpha\beta\gamma = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha + \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2 = A + B$$

Determining the expression for AB is more work, but not so bad.

$$AB = (\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) \cdot (\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma) = \alpha^3\beta^3 + \beta^3\gamma^3 + \gamma^3\alpha^3 + \alpha^4\beta\gamma + \alpha\beta^4\gamma + \alpha\beta\gamma^4 + 3s_3^2$$

We can observe that already (using an earlier calculation)

$$\alpha^4\beta\gamma + \alpha\beta^4\gamma + \alpha\beta\gamma^4 = s_3 \cdot (\alpha^3 + \beta^3 + \gamma^3) = s_3(s_1^3 - 3s_1s_2 + 3s_3)$$

For $\alpha^3\beta^3 + \beta^3\gamma^3 + \gamma^3\alpha^3$ follow the algorithm: its value at $\gamma = 0$ is $\alpha^3\beta^3 = s_2^3$ (with the s_2 for α, β alone). Thus, we consider

$$\alpha^3\beta^3 + \beta^3\gamma^3 + \gamma^3\alpha^3 - (\alpha\beta + \beta\gamma + \gamma\alpha)^3$$
$$= -6s_3^2 - 3\left(\alpha^2\beta^3\gamma + \alpha^3\beta^2\gamma + \alpha\beta^3\gamma^2 + \alpha\beta^2\gamma^3 + \alpha^2\beta\gamma^3 + \alpha^3\beta\gamma^2\right)$$

[4] In an earlier computation regarding the special cubic $x^3 + x^2 - 2x - 1$, we could make use of the connection to the 7^{th} root of unity to obtain explicit expressions for $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$ and $\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma$, but for the general cubic there are no such tricks available.

$$= -6s_3^2 - 3s_3\left(\alpha\beta^2 + \alpha^2\beta + \beta^2\gamma + \beta\gamma^2 + \alpha\gamma^2 + \alpha^2\gamma\right) = -6s_3^2 - 3s_3(s_1s_2 - 3s_3)$$

by our computation of $A+B$. Together, the three parts of AB give

$$AB = s_3(s_1^3 - 3s_1s_2 + 3s_3) + \left(s_2^3 - 6s_3^2 - 3s_3(s_1s_2 - 3s_3)\right) + 3s_3^2$$

$$= s_1^3s_3 - 3s_1s_2s_3 + 3s_3^2 + s_2^3 - 6s_3^2 - 3s_1s_2s_3 + 9s_3^2 + 3s_3^2 = s_1^3s_3 - 6s_1s_2s_3 + 9s_3^2 + s_2^3$$

That is, A and B are the two zeros of the quadratic

$$x^2 - (s_1s_2 - 3s_3)x + (s_1^3s_3 - 6s_1s_2s_3 + 9s_3^2 + s_2^3) = x^2 - (-ab + 3c)x + (a^3c - 6abc + 9c^2 + b^3)$$

The **discriminant** of this monic quadratic is[5]

$$\Delta = (\text{linear coef})^2 - 4(\text{constant coef}) = (-ab + 3c)^2 - 4(a^3c - 6abc + 9c^2 + b^3)$$

$$= a^2b^2 - 6abc + 9c^2 - 4a^3c + 24abc - 36c^2 - 4b^3 = a^2b^2 - 27c^2 - 4a^3c + 18abc - 4b^3$$

In particular, the quadratic formula[6] gives

$$A, B = \frac{(ab - 3c) \pm \sqrt{\Delta}}{2}$$

Then

$$\lambda^3 = s_1^3 - 3s_1s_2 + 9s_3 + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) - 3\omega(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma) - 3(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma)$$

$$= -a^3 + 3bc - 9c + 3(\omega - 1)A - 3\omega B$$

$$= -a^3 + 3bc - 9c + 3(\omega - 1)\cdot\frac{(ab - 3c) + \sqrt{\Delta}}{2} - 3\omega\cdot\frac{(ab - 3c) - \sqrt{\Delta}}{2}$$

$$= -a^3 + 3bc - 9c - \frac{3}{2}(ab - 3c) + (3\omega - \frac{1}{2})\sqrt{\Delta}$$

That is, now we can solve for λ by taking a cube root of the mess on the right-hand side:

$$\lambda = \sqrt[3]{(\text{right-hand side})}$$

The same computation works for the analogue λ' of λ with ω replaced by the *other*[7] primitive cube root of unity

$$\lambda' = \alpha + \omega^2\cdot\beta + \omega\cdot\gamma$$

The analogous computation is much easier when ω is replaced by 1, since

$$\alpha + 1\cdot\beta + 1^2\cdot\gamma = s_1 = -a$$

Thus, we have a linear system

[5] When the x^2 coefficient a vanishes, we will recover the better-known special case that the discriminant is $-27c^2 - 4b^3$.

[6] Which is an instance of this general approach, but for quadratics rather than cubics.

[7] In fact, there is no way to distinguish the two primitive cube roots of unity, so neither has primacy over the other. And, still, either is the square of the other.

The linear system

$$\begin{cases} \alpha+\beta+\gamma &= -a \\ \alpha+\omega\beta+\omega^2\gamma &= \lambda \\ \alpha+\omega^2\beta+\omega\gamma &= \lambda' \end{cases}$$

has coefficients that readily allow solution, since for a primitive n^{th} root of unity ζ the matrix

$$M = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta & \zeta^2 & \ldots & \zeta^{n-1} \\ 1 & \zeta^2 & (\zeta^2)^2 & \ldots & (\zeta^2)^{n-1} \\ 1 & \zeta^3 & (\zeta^3)^2 & \ldots & (\zeta^3)^{n-1} \\ & & \vdots & & \\ 1 & \zeta^{n-1} & (\zeta^{n-1})^2 & \ldots & (\zeta^{n-1})^{n-1} \end{pmatrix}$$

has inverse

$$M^{-1} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta^{-1} & (\zeta^{-1})^2 & \ldots & (\zeta^{-1})^{n-1} \\ 1 & \zeta^{-2} & (\zeta^{-2})^2 & \ldots & (\zeta^{-2})^{n-1} \\ 1 & \zeta^{-3} & (\zeta^{-3})^2 & \ldots & (\zeta^{-3})^{n-1} \\ & & \vdots & & \\ 1 & \zeta^{-n+1} & (\zeta^{-n+1})^2 & \ldots & (\zeta^{-n+1})^{n-1} \end{pmatrix}$$

In the present simple case this gives the three roots[8] of the cubic as

$$\begin{cases} \alpha &= \frac{-a+\lambda+\lambda'}{3} \\ \beta &= \frac{-a+\omega^2\lambda+\omega\lambda'}{3} \\ \gamma &= \frac{-a+\omega\lambda+\omega^2\lambda'}{3} \end{cases}$$

4. *Worked examples*

[23.1] Let k be a field of characteristic 0. Let f be an irreducible polynomial in $k[x]$. Prove that f has no repeated factors, even over an algebraic closure of k.

If f has a factor P^2 where P is irreducible in $k[x]$, then P divides $\gcd(f, f') \in k[x]$. Since f was monic, and since the characteristic is 0, the derivative of the highest-degree term is of the form nx^{n-1}, and the coefficient is non-zero. Since f' is not 0, the degree of $\gcd(f, f')$ is at most $\deg f'$, which is strictly less than $\deg f$. Since f is irreducible, this *gcd* in $k[x]$ must be 1. Thus, there are polynomials a, b such that $af + bf' = 1$. The latter identity certainly persists in $K[x]$ for any field extension K of k. ///

[23.2] Let K be a finite extension of a field k of characteristic 0. Prove that K is separable over k.

Since K is finite over k, there is a finite list of elements $\alpha_1, \ldots, \alpha_n$ in K such that $K = k(\alpha_1, \ldots, \alpha_n)$. From the previous example, the minimal polynomial f of α_1 over k has no repeated roots in an algebraic closure $\overline{k}$ of k, so $k(\alpha_1)$ is separable over k.

[8] Again, the seeming asymmetry among the roots is illusory. For example, since λ is a cube root of something, we really cannot distinguish among λ, $\omega\lambda$, and $\omega^2\lambda$. And, again, we cannot distinguish between ω and ω^2.

We recall[9] the fact that we can map $k(\alpha_1) \longrightarrow \overline{k}$ by sending α_1 to any of the $[k(\alpha_1) : k] = \deg f$ distinct roots of $f(x) = 0$ in $\overline{k}$. Thus, there are $[k(\alpha_1) : k] = \deg f$ distinct distinct imbeddings of $k(\alpha_1)$ into $\overline{k}$, so $k(\alpha_1)$ is separable over k.

Next, observe that for any imbedding $\sigma : k(\alpha_1) \longrightarrow \overline{k}$ of $k(\alpha_1)$ into an algebraic closure $\overline{k}$ of k, by proven properties of $\overline{k}$ we know that $\overline{k}$ is an algebraic closure of $\sigma(k(\alpha_1))$. Further, if $g(x) \in k(\alpha_1)[x]$ is the minimal polynomial of α_2 over $k(\alpha_1)$, then $\sigma(g)(x)$ (applying σ to the coefficients) is the minimal polynomial of α_2 over $\sigma(k(\alpha_1))$. Thus, by the same argument as in the previous paragraph we have $[k(\alpha_1, \alpha_2) : k(\alpha_1)]$ distinct imbeddings of $k(\alpha_1, \alpha_2)$ into $\overline{k}$ for a given imbedding of $k(\alpha_1)$. Then use induction. ///

[23.3] Let k be a field of characteristic $p > 0$. Suppose that k is **perfect**, meaning that for any $a \in k$ there exists $b \in k$ such that $b^p = a$. Let $f(x) = \sum_i c_i x^i$ in $k[x]$ be a polynomial such that its (algebraic) derivative

$$f'(x) = \sum_i c_i \, i \, x^{i-1}$$

is the zero polynomial. Show that there is a unique polynomial $g \in k[x]$ such that $f(x) = g(x)^p$.

For the derivative to be the 0 polynomial it must be that the characteristic p divides the exponent of every term (with non-zero coefficient). That is, we can rewrite

$$f(x) = \sum_i c_{ip} \, x^{ip}$$

Let $b_i \in k$ such that $b_i^p = c_{ip}$, using the perfectness. Since p divides all the inner binomial coefficients $p^!/i!(p-i)!$,

$$\left(\sum_i b_i \, x^i\right)^p = \sum_i c_{ip} \, x^{ip}$$

as desired. ///

[23.4] Let k be a perfect field of characteristic $p > 0$, and f an irreducible polynomial in $k[x]$. Show that f has no repeated factors (even over an algebraic closure of k).

If f has a factor P^2 where P is irreducible in $k[x]$, then P divides $\gcd(f, f') \in k[x]$. If $\deg \gcd(f, f') < \deg f$ then the irreducibility of f in $k[x]$ implies that the *gcd* is 1, so no such P exists. If $\deg \gcd(f, f') = \deg f$, then $f' = 0$, and (from above) there is a polynomial $g(x) \in k[x]$ such that $f(x) = g(x)^p$, contradicting the irreducibility in $k[x]$. ///

[23.5] Show that all finite fields $\mathbb{F}_{p^n}$ with p prime and $1 \le n \in \mathbb{Z}$ are perfect.

Again because the inner binomial coefficients $p!/i!(p-i)!$ are 0 in characteristic p, the (Frobenius) map $\alpha \longrightarrow \alpha^p$ is not only (obviously) multiplicative, but also additive, so is a ring homomorphism of $\mathbb{F}_{p^n}$ to itself. Since $\mathbb{F}_{p^n}^\times$ is cyclic (of order p^n), for any $\alpha \in \mathbb{F}_{p^n}$ (including 0)

$$\alpha^{(p^n)} = \alpha$$

Thus, since the map $\alpha \longrightarrow \alpha^p$ has the (two-sided) inverse $\alpha \longrightarrow \alpha^{p^{n-1}}$, it is a bijection. That is, everything has a p^{th} root. ///

[23.6] Let K be a finite extension of a finite field k. Prove that K is separable over k.

[9] Recall the proof: Let β be a root of $f(x) = 0$ in $\overline{k}$. Let $\varphi : k[x] \longrightarrow k[\beta]$ by $x \longrightarrow \beta$. The kernel of φ is the principal ideal generated by $f(x)$ in $k[x]$. Thus, the map φ factors through $k[x]/\langle f \rangle \approx k[\alpha_1]$.

That is, we want to prove that the number of distinct imbeddings σ of K into a fixed algebraic closure $\overline{k}$ is $[K:k]$. Let $\alpha \in K$ be a generator for the cyclic group $K^\times$. Then $K = k(\alpha) = k[\alpha]$, since powers of α already give every element but 0 in K. Thus, from basic field theory, the degree of the minimal polynomial $f(x)$ of α over k is $[K:k]$. The previous example shows that k is perfect, and the example before that showed that irreducible polynomials over a perfect field have no repeated factors. Thus, $f(x)$ has no repeated factors in any field extension of k.

We have also already seen that for algebraic α over k, we can map $k(\alpha)$ to $\overline{k}$ to send α to *any* root β of $f(x) = 0$ in $\overline{k}$. Since $f(x)$ has not repeated factors, there are $[K:k]$ distinct roots β, so $[K:k]$ distinct imbeddings. ///

[23.7] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$ where ζ is a primitive 17^{th} root of unity.

Since 17 is prime, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \approx (\mathbb{Z}/17)^\times$ is cyclic (of order 16), and we know that a cyclic group has a unique subgroup of each order dividing the order of the whole. Thus, there are intermediate fields corresponding to the proper divisors $2, 4, 8$ of 16. Let σ_a be the automorphism $\sigma_a\zeta = \zeta^a$.

By a little trial and error, 3 is a generator for the cyclic group $(\mathbb{Z}/17)^\times$, so σ_3 is a generator for the automorphism group. Thus, one reasonably considers

$$\begin{aligned} \alpha_8 &= \zeta + \zeta^{3^2} + \zeta^{3^4} + \zeta^{3^6} + \zeta^{3^8} + \zeta^{3^{10}} + \zeta^{3^{12}} + \zeta^{3^{14}} \\ \alpha_4 &= \zeta + \zeta^{3^4} + \zeta^{3^8} + \zeta^{3^{12}} \\ \alpha_2 &= \zeta + \zeta^{3^8} = \zeta + \zeta^{-1} \end{aligned}$$

The α_n is visibly invariant under the subgroup of $(\mathbb{Z}/17)^\times$ of order n. The linear independence of $\zeta, \zeta^2, \zeta^3, \ldots, \zeta^{16}$ shows α_n is *not* by accident invariant under any larger subgroup of the Galois group. Thus, $\mathbb{Q}(\alpha_n)$ is (by Galois theory) the unique intermediate field of degree $16/n$ over $\mathbb{Q}$.

We can also give other characterizations of some of these intermediate fields. First, we have already seen (in discussion of Gauss sums) that

$$\sum_{a \bmod 17} \left(\frac{a}{17}\right)_2 \cdot \zeta^a = \sqrt{17}$$

where $\left(\frac{a}{17}\right)_2$ is the quadratic symbol. Thus,

$$\begin{aligned} \alpha_8 - \sigma_3\alpha_8 &= \sqrt{17} \\ \alpha_8 + \sigma_3\alpha_8 &= 0 \end{aligned}$$

so α_8 and $\sigma_3\alpha_8$ are $\pm\sqrt{17}/2$. Further computation can likewise express all the intermediate fields as being obtained by adjoining square roots to the next smaller one. ///

[23.8] Let f, g be *relatively prime* polynomials in n indeterminates $t_1, \ldots, t_n$, with g not 0. Suppose that the ratio $f(t_1, \ldots, t_n)/g(t_1, \ldots, t_n)$ is invariant under all permutations of the t_i. Show that both f and g are polynomials in the elementary symmetric functions in the t_i.

Let s_i be the i^{th} elementary symmetric function in the t_j's. Earlier we showed that $k(t_1, \ldots, t_n)$ has Galois group S_n (the symmetric group on n letters) over $k(s_1, \ldots, s_n)$. Thus, the given ratio lies in $k(s_1, \ldots, s_n)$. Thus, it is *expressible* as a ratio

$$\frac{f(t_1, \ldots, t_n)}{g(t_1, \ldots, t_n)} = \frac{F(s_1, \ldots, s_n)}{G(s_1, \ldots, s_n)}$$

of polynomials F, G in the s_i.

To prove the stronger result that the original f and g were themselves literally polynomials in the t_i, we seem to need the characteristic of k to be not 2, and we certainly must use the unique factorization in $k[t_1, \ldots, t_n]$.

Write

$$f(t_1, \ldots, t_n) = p_1^{e_1} \ldots p_m^{e_m}$$

where the e_i are positive integers and the p_i are irreducibles. Similarly, write

$$g(t_1, \ldots, t_n) = q_1^{f_1} \ldots q_m^{f_n}$$

where the f_i are positive integers and the q_i are irreducibles. The relative primeness says that none of the q_i are *associate* to any of the p_i. The invariance gives, for any permutation π of

$$\pi\left(\frac{p_1^{e_1} \ldots p_m^{e_m}}{q_1^{f_1} \ldots q_m^{f_n}}\right) = \frac{p_1^{e_1} \ldots p_m^{e_m}}{q_1^{f_1} \ldots q_m^{f_n}}$$

Multiplying out,

$$\prod_i \pi(p_i^{e_i}) \cdot \prod_i q_i^{f_i} = \prod_i p_i^{e_i} \cdot \prod_i \pi(q_i^{f_i})$$

By the relative prime-ness, each p_i divides some one of the $\pi(p_j)$. These ring automorphisms preserve irreducibility, and $\gcd(a, b) = 1$ implies $\gcd(\pi a, \pi b) = 1$, so, symmetrically, the $\pi(p_j)$'s divide the p_i's. And similarly for the q_i's. That is, permuting the t_i's must permute the irreducible factors of f (up to units $k^\times$ in $k[t_1, \ldots, t_n]$) among themselves, and likewise for the irreducible factors of g.

If all permutations *literally* permuted the irreducible factors of f (and of g), rather than merely up to *units*, then f and g would be symmetric. However, at this point we can only be confident that they are permuted *up to constants.*

What we have, then, is that for a permutation π

$$\pi(f) = \alpha_\pi \cdot f$$

for some $\alpha \in k^\times$. For another permutation τ, certainly $\tau(\pi(f)) = (\tau\pi)f$. And $\tau(\alpha_\pi f) = \alpha_\pi \cdot \tau(f)$, since permutations of the indeterminates have no effect on elements of k. Thus, we have

$$\alpha_{\tau\pi} = \alpha_\tau \cdot \alpha_\pi$$

That is, $\pi \longrightarrow \alpha_\pi$ is a group homomorphism $S_n \longrightarrow k^\times$.

It is very useful to know that the alternating group A_n is the *commutator subgroup* of S_n. Thus, if f is not actually invariant under S_n, in any case the group homomorphism $S_n \longrightarrow k^\times$ factors through the quotient S_n/A_n, so is the *sign function* $\pi \longrightarrow \sigma(\pi)$ that is $+1$ for $\pi \in A_n$ and -1 otherwise. That is, f is **equivariant** under S_n by the sign function, in the sense that $\pi f = \sigma(\pi) \cdot f$.

Now we claim that if $\pi f = \sigma(\pi) \cdot f$ then the square root

$$\delta = \sqrt{\Delta} = \prod_{i<j} (t_i - t_j)$$

of the discriminant Δ divides f. To see this, let s_{ij} be the 2-cycle which interchanges t_i and t_j, for $i \neq j$. Then

$$s_{ij} f = -f$$

Under any homomorphism which sends $t_i - t_j$ to 0, since the characteristic is not 2, f is sent to 0. That is, $t_i - t_j$ divides f in $k[t_1, \ldots, t_n]$. By unique factorization, since no two of the monomials $t_i - t_j$ are associate (for distinct pairs $i < j$), we see that the square root δ of the discriminant must divide f.

That is, for f with $\pi f = \sigma(\pi) \cdot f$ we know that $\delta | f$. For f/g to be invariant under S_n, it must be that also $\pi g = \sigma(\pi) \cdot g$. But then $\delta | g$ also, contradicting the assumed relative primeness. Thus, in fact, it must have been that both f and g were *invariant* under S_n, not merely equivariant by the sign function. ///

Exercises

23.[4.0.1] Let k be a field. Let $\alpha_1, \ldots, \alpha_n$ be distinct elements of $k^\times$. Suppose that $c_1, \ldots, c_n$ in k are such that for all positive integers ℓ

$$\sum_i c_i \, \alpha_i^\ell = 0$$

Show that all the c_i are 0.

23.[4.0.2] Solve the cubic $x^3 + ax + b = 0$ in terms of radicals.

23.[4.0.3] Express a primitive 11^{th} root of unity in terms of radicals.

23.[4.0.4] Solve $x^4 + ax + b = 0$ in terms of radicals.