19. Roots of unity

19.1 Another proof of cyclicness
19.2 Roots of unity
19.3 $\mathbb{Q}$ with roots of unity adjoined
19.4 Solution in radicals, Lagrange resolvents
19.5 Quadratic fields, quadratic reciprocity
19.6 Worked examples

1. *Another proof of cyclicness*

Earlier, we gave a more complicated but more elementary proof of the following theorem, using cyclotomic polynomials. There is a cleaner proof using the structure theorem for finite abelian groups, which we give now. [1] Thus, this result is yet another corollary of the structure theory for finitely-generated free modules over PIDs.

[1.0.1] **Theorem:** Let G be a finite subgroup of the multiplicative group $k^\times$ of a field k. Then G is cyclic.

Proof: By the structure theorem, applied to abelian groups as $\mathbb{Z}$-modules,

$$G \approx \mathbb{Z}/d_1 \oplus \ldots \oplus \mathbb{Z}/d_n$$

where the integers d_i have the property $1 < d_1 | \ldots | d_n$ and no elementary divisor d_i is 0 (since G is finite). All elements of G satisfy the equation

$$x^{d_t} = 1$$

By unique factorization in $k[x]$, this equation has at most d_t roots in k. Thus, there can be only one direct summand, and G is cyclic. ///

[1] The argument using cyclotomic polynomials is wholesome and educational, too, but is much grittier than the present argument.

[1.0.2] **Remark:** Although we will not need to invoke this theorem for our discussion just below of solutions of equations

$$x^n = 1$$

one might take the viewpoint that the traditional pictures of these solutions as points on the unit circle in the complex plane are not at all misleading about more general situations.

---

2. *Roots of unity*

An element ω in any field k with the property that $\omega^n = 1$ for some integer n is a **root of unity**. For positive integer n, if $\omega^n = 1$ and $\omega^t \neq 1$ for positive integers [2] $t < n$, then ω is a **primitive** n^{th} root of unity. [3]

Note that

$$\mu_n = \{\alpha \in k^\times : \alpha^n = 1\}$$

is finite since there are at most n solutions to the degree n equation $x^n = 1$ in any field. This group is known to be *cyclic*, by at least two proofs.

[2.0.1] **Proposition:** Let k be a field and n a positive integer not divisible by the characteristic of the field. An element $\omega \in k^\times$ is a primitive n^{th} root of unity in k if and only if ω is an element of order n in the group μ_n of *all* n^{th} roots of unity in k. If so, then

$$\{\omega^\ell : 1 \leq \ell \leq n, \text{ and } \gcd(\ell, n) = 1\}$$

is a complete (and irredundant) list of all the primitive n^{th} roots of unity in k. A complete and irredundant list of *all* n^{th} roots of unity in k is

$$\{\omega^\ell : 1 \leq \ell \leq n\} = \{\omega^\ell : 0 \leq \ell \leq n-1\}$$

Proof: To say that ω is a *primitive* n^{th} root of unity is to say that its order in the group $k^\times$ is n. Thus, it generates a cyclic group of order n inside $k^\times$. Certainly any integer power ω^ℓ is in the group μ_n of n^{th} roots of unity, since

$$(\omega^\ell)^n = (\omega^n)^\ell = 1^\ell = 1$$

Since the group generated by ω is inside μ_n and has at least as large cardinality, it is the whole. On the other hand, a generator for μ_n has order n (or else would generate a strictly smaller group). This proves the equivalence of the conditions describing primitive n^{th} roots of unity.

As in the more general proofs of analogous results for finite cyclic groups, the set of all elements of a cyclic group of order n is the collection of powers $\omega^1, \omega^2, \ldots, \omega^{n-1}, \omega^n$ of any generator ω of the group.

As in the more general proofs of analogous results for cyclic groups, the order of a power ω^ℓ of a generator ω is exactly $n/\gcd(n, \ell)$, since $(\omega^\ell)^t = 1$ if and only if $n|\ell t$. Thus, the set given in the statement of the proposition is a set of primitive n^{th} roots of unity. There are $\varphi(n)$ of them in this set, where φ is Euler's totient-function. ///

---

[2] If $\omega^n = 1$ then in any case the *smallest* positive integer ℓ such that $\omega^\ell = 1$ is a divisor of n. Indeed, as we have done many times already, write $n = q\ell + r$ with $0 \leq r < |\ell|$, and $1 = \omega^n = \omega^{q\ell+r} = \omega^r$. Thus, since ℓ is least, $r = 0$, and ℓ divides n.

[3] If the characteristic p of the field k divides n, then there are no primitive n^{th} roots of unity in k. Generally, for $n = p^e m$ with p not dividing m, $\Phi_{p^e m}(x) = \Phi_m(x)^{\varphi(p^e)} = \Phi_m(x)^{(p-1)p^{e-1}}$. We'll prove this later.

3. $\mathbb{Q}$ with roots of unity adjoined

One of the general uses of *Galois theory* is to understand fields intermediate between a base field k and an algebraic field extension K of k. In the case of *finite fields* we already have simple means to completely understand intermediate fields. Any situation beyond from the finite field case is more complicated. But, to provide further examples, it is possible to consider fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$ where ζ is a (primitive) n^{th} root of unity.

There are obvious and boring inclusions, since if ζ is a primitive mn^{th} root of unity, then ζ^m is a primitive n^{th} root of unity. That is, we have

$$\mathbb{Q}(\text{primitive } n^{th} \text{ root of unity}) \subset \mathbb{Q}(\text{primitive } mn^{th} \text{ root of unity})$$

In any case, by the *multiplicativity* of field extension degrees in towers, for a primitive n^{th} root of unity ζ, given

$$\mathbb{Q} \subset k \subset \mathbb{Q}(\zeta)$$

we have

$$[\mathbb{Q}(\zeta) : k] \cdot [k : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}]$$

In particular, for prime $n = p$, we have already seen that Eisenstein's criterion proves that the p^{th} cyclotomic polynomial $\Phi_p(x)$ is irreducible of degree $\varphi(p) = p - 1$, so

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$$

We will discuss the irreducibility of other cyclotomic polynomials a bit later.

[3.0.1] **Example:** With

$$\zeta_5 = \text{ a primitive fifth root of unity}$$

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 5 - 1 = 4$$

so any field k intermediate between $\mathbb{Q}(\zeta_5)$ and $\mathbb{Q}$ must be quadratic over $\mathbb{Q}$. In particular, from

$$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$$

by dividing through by ζ_5^2 we obtain

$$\zeta_5^2 + \zeta_5 + 1 + \zeta_5^{-1} + \zeta_5^{-2} = 0$$

and this can be rearranged to

$$\left(\zeta_5 + \frac{1}{\zeta_5}\right)^2 + \left(\zeta_5 + \frac{1}{\zeta_5}\right) - 1 = 0$$

Letting

$$\xi = \xi_5 = \zeta_5 + \frac{1}{\zeta_5}$$

we have

$$\xi^2 + \xi - 1 = 0$$

so

$$\xi = \frac{-1 \pm \sqrt{1 - 4(-1)}}{2} = \frac{-1 \pm \sqrt{5}}{2}$$

From the standard picture of 5^{th} roots of unity in the complex plane, we have

$$\xi = \zeta_5 + \frac{1}{\zeta_5} = e^{2\pi i/5} + e^{-2\pi i/5} = 2\cos\frac{2\pi}{5} = 2\cos 72^o$$

Therefore,

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$$

It should be a bit surprising that

$$\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$$

To prove that there are no *other* intermediate fields will require more work.

[3.0.2] **Example:** With

$$\zeta_7 = \text{ a primitive seventh root of unity}$$

$$[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 7 - 1 = 6$$

so any field k intermediate between $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}$ must be *quadratic* or *cubic* over $\mathbb{Q}$. We will find one of each degree. We can use the same front-to-back symmetry of the cyclotomic polynomial that we exploited for a fifth root of 1 in the previous example. In particular, from

$$\zeta_7^6 + \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2 + \zeta_7 + 1 = 0$$

by dividing through by ζ_7^3

$$\zeta_7^3 + \zeta_7^2 + \zeta_7 + 1 + \zeta_7^{-1} + \zeta_7^{-2} + \zeta_7^{-3} = 0$$

and thus

$$\left(\zeta_7 + \frac{1}{\zeta_7}\right)^3 + \left(\zeta_7 + \frac{1}{\zeta_7}\right)^2 - 2\left(\zeta_7 + \frac{1}{\zeta_7}\right) - 1 = 0$$

Again letting

$$\xi = \xi_7 = \zeta_7 + \frac{1}{\zeta_7}$$

we have

$$\xi^3 + \xi^2 - 2\xi - 1 = 0$$

and in the complex plane

$$\xi = \zeta_7 + \frac{1}{\zeta_7} = e^{2\pi i/7} + e^{-2\pi i/7} = 2\cos\frac{2\pi}{7}$$

Thus,

$$[\mathbb{Q}(\xi_7) : \mathbb{Q}] = 3$$

We will return to this number in a moment, after we find the intermediate field that is *quadratic* over $\mathbb{Q}$.

Take $n = p$ prime for simplicity. Let's think about the front-to-back symmetry a bit more, to see whether it can suggest something of broader applicability. Again, for any primitive p^{th} root of unity $\zeta = \zeta_p$, and for a relatively prime to p, ζ^a is another primitive p^{th} root of unity. Of course, since $\zeta^p = 1$. ζ^a only depends upon a mod p. Recalling that $1, \zeta.\zeta^2, \ldots, \zeta^{p-3}, \zeta^{p-2}$ is a $\mathbb{Q}$-basis[4] for $\mathbb{Q}(\zeta)$, we claim that the map

$$\sigma_a : c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + \ldots + c_{p-2}\zeta^{p-2} \longrightarrow c_0 + c_1\zeta^a + c_2\zeta^{2a} + c_3\zeta^{3a} + \ldots + c_{p-2}\zeta^{(p-2)a}$$

is a $\mathbb{Q}$-algebra automorphism of $\mathbb{Q}(\zeta)$. That is, σ_a raises each ζ^j to the a^{th} power. Since, again, ζ^j only depends upon j mod p, all the indicated powers of ζ are primitive p^{th} roots of 1. The $\mathbb{Q}$-linearity of this map is built into its definition, but the multiplicativity is not obvious. Abstracting just slightly, we have

[4] Yes, the highest index is $p-2$, not $p-1$, and not p. The p^{th} cyclotomic polynomial is of degree $p-1$, and in effect gives a non-trivial linear dependence relation among $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}, \zeta^{p-1}$.

[3.0.3] **Proposition:** Let k be a field, $k(\alpha)$ a finite algebraic extension, where $f(x)$ is the minimal polynomial of α over k. Let $\beta \in k(\alpha)$ be another root [5] of $f(x) = 0$. Then there is a unique field automorphism [6] σ of $k(\alpha)$ over k sending α to β, given by the formula

$$\sigma\left(\sum_{0\le i<\deg f} c_i\alpha^i\right) = \sum_{0\le i<\deg f} c_i\beta^i$$

where $c_i \in \mathbb{Q}$.

Proof: Thinking of the universal mapping property of the polynomial ring $k[x]$, let

$$q_\alpha : k[x] \longrightarrow k[\alpha] = k(\alpha)$$

be the unique k-algebra homomorphism sending $x \longrightarrow \alpha$. By definition of the minimal polynomial f of α over k, the kernel of a_α is the principal ideal $\langle f\rangle$ in $k[x]$ generated by f. Let

$$q_\beta : k[x] \longrightarrow k[\alpha] = k(\alpha)$$

be the unique k-algebra homomorphism [7] sending $x \longrightarrow \beta$. Since β satisfies the same monic equation $f(x) = 0$ with f irreducible, the kernel of q_β is also the ideal $\langle f\rangle$. Thus, since

$$\ker q_\beta \supset \ker q_\alpha$$

the map q_β factors through q_α in the sense that there is a unique k-algebra homomorphism

$$\sigma : k(\alpha) \longrightarrow k(\alpha)$$

such that

$$q_\beta = \sigma \circ q_\alpha$$

That is, the obvious attempt at defining σ, by

$$\sigma\left(\sum_{0\le i<\deg f} c_i\alpha^i\right) = \sum_{0\le i<\deg f} c_i\beta^i$$

with $c_i \in \mathbb{Q}$ gives a *well-defined* map. [8] Since

$$\dim_k \sigma(k(\alpha)) = \dim_k q_\beta(k[x]) = \deg f = \dim_k k[\alpha] = \dim_k k(\alpha)$$

the map σ is *bijective*, hence invertible. ///

---

[5] It is critical that the second root lie in the field generated by the first. This issue is a presagement of the idea of *normality* of $k(\alpha)$ over k, meaning that *all* the other roots of the minimal polynomial of α lie in $k(\alpha)$ already. By contrast, for example, the field $\mathbb{Q}(\alpha)$ for any cube root α of 2 does *not* contain any *other* cube roots of 2. Indeed, the ratio of two such would be a primitive cube root of unity lying in $\mathbb{Q}(\alpha)$, which various arguments show is impossible.

[6] This use of the phrase *automorphism over* is standard terminology: a field automorphism $\tau : K \longrightarrow K$ of a field K to itself, with τ fixing every element of a subfield k, is an automorphism of K *over* k.

[7] Such a homomorphism exists for *any* element β of any k-algebra $k[\alpha]$, whether or not β is related to α.

[8] Note that this approach makes the multiplicativity easy, packaging all the issues into the well-definedness, which then itself is a straightforward consequence of the hypothesis that α and β are two roots of the same equation, and that $\beta \in k(\alpha)$.

[3.0.4] **Corollary:** Let p be prime and ζ a primitive p^{th} root of unity. The automorphism group $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to

$$(\mathbb{Z}/p)^\times \approx \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

by the map

$$a \leftrightarrow \sigma_a$$

where

$$\sigma_a(\zeta) = \zeta^a$$

Proof: This uses the irreducibility of $\Phi_p(x)$ in $\mathbb{Q}[x]$. Thus, for all $a \in (\mathbb{Z}/p)^\times$ the power ζ^a is another root of $\Phi_p(x) = 0$, and $\Phi_p(x)$ is the minimal polynomial of both ζ and ζ^a. This gives an injection

$$(\mathbb{Z}/p)^\times \longrightarrow \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

On the other hand, any automorphism σ of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ must send ζ to another root of its minimal polynomial, so $\sigma(\zeta) = \zeta^a$ for some $a \in (\mathbb{Z}/p)^\times$, since all primitive p^{th} roots of unity are so expressible. This proves that the map is surjective. ///

Returning to roots of unity: for a primitive p^{th} root of unity ζ, the map

$$\zeta \longrightarrow \zeta^{-1}$$

maps ζ to another primitive p^{th} root of unity lying in $\mathbb{Q}(\zeta)$, so this map extends to an automorphism

$$\sigma_{-1} : \mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta)$$

of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. And [9]

$$2\cos\frac{2\pi}{p} = \xi = \zeta + \frac{1}{\zeta} = \zeta + \sigma_{-1}(\zeta)$$

Of course, the identity map on $\mathbb{Q}(\zeta)$ is the automorphism σ_1, and

$$\sigma_{-1}^2 = \sigma_1$$

That is,

$$\{\sigma_1, \sigma_{-1}\}$$

is a *subgroup* of the group of automorphisms of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Indeed, the map

$$a \longrightarrow \sigma_a$$

is a *group homomorphism*

$$(\mathbb{Z}/p)^\times \longrightarrow \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

since

$$\sigma_a\left(\sigma_b(\zeta)\right) = \sigma_a(\zeta^b) = \left(\sigma_a\zeta\right)^b$$

since σ_a is a ring homomorphism. Thus, recapitulating a bit,

$$\sigma_a\left(\sigma_b(\zeta)\right) = \sigma_a(\zeta^b) = \left(\sigma_a\zeta\right)^b = (\zeta^a)^b = \sigma_{ab}(\zeta)$$

[9] Writing an algebraic number in terms of cosine is not quite right, though it is appealing. The problem is that unless we choose an imbedding of $\mathbb{Q}(\zeta)$ into the complex numbers, we cannot really know *which* root of unity we have chosen. Thus, we cannot know which angle's cosine we have. Nevertheless, it is useful to think about this.

That is, we can take the viewpoint that ξ is formed from ζ by a certain amount of **averaging** or **symmetrizing** over the subgroup $\{\sigma_1, \sigma_{-1}\}$ of automorphisms.

That this symmetrizing or averaging does help isolate elements in smaller subfields of cyclotomic fields $\mathbb{Q}(\zeta)$ is the content of

[3.0.5] **Proposition:** Let G be the group of automorphisms of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ given by σ_a for $a \in (\mathbb{Z}/p)^\times$. Let $\alpha \in \mathbb{Q}(\zeta_p)$.

$$\alpha \in \mathbb{Q} \quad \text{if and only if} \quad \sigma(\alpha) = \alpha \quad \text{for all } \sigma \in G$$

Proof: Certainly elements of $\mathbb{Q}$ are invariant under all σ_a, by the definition. Let [10]

$$\alpha = \sum_{1 \le i \le p-1} c_i \zeta^i$$

with $c_i \in \mathbb{Q}$. The condition $\alpha = \sigma_a(\alpha)$ is

$$\sum_{1 \le i \le p-1} c_i \zeta^i = \sum_{1 \le i \le p-1} c_i \zeta^{ai}$$

Since $\zeta^p = 1$, the powers ζ^{ai} only depend upon $ai \bmod p$. The map

$$i \longrightarrow ai \bmod p$$

permutes $\{i : 1 \le i \le p-1\}$. Thus, looking at the coefficient of ζ^a as a varies, the equation $\alpha = \sigma_a(\alpha)$ gives

$$c_a = c_1$$

That is, the G-invariance of α requires that α be of the form

$$\alpha = c \cdot (\zeta + \zeta^2 + \ldots + \zeta^{p-1}) = c \cdot (1 + \zeta + \zeta^2 + \ldots + \zeta^{p-1}) - c = -c$$

for $c \in \mathbb{Q}$, using

$$0 = \Phi_p(\zeta) = 1 + \zeta + \zeta^2 + \ldots + \zeta^{p-1}$$

That is, G-invariance implies rationality. ///

[3.0.6] **Corollary:** Let H be a subgroup of $G = (\mathbb{Z}/p)^\times$, identified with a group of automorphisms of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ by $a \longrightarrow \sigma_a$. Let $\alpha \in \mathbb{Q}(\zeta_p)$ be fixed under H. Then

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \le [G : H] = \frac{|G|}{|H|}$$

Proof: Since α is H-invariant, the value

$$\sigma_a(\alpha)$$

depends only upon the image of a in G/H, that is, upon the coset $aH \in G/H$. Thus, in

$$f(x) = \prod_{a \in G/H} (x - \sigma_a(\alpha)) \in \mathbb{Q}(\zeta)[x]$$

[10] It is a minor cleverness to use the $\mathbb{Q}$-basis ζ^i with $1 \le i \le p-1$ rather than the $\mathbb{Q}$-basis with $0 \le i \le p-2$. The point is that the latter is stable under the automorphisms σ_a, while the former is not.

everything is well-defined. Since it is a ring homomorphism, $\sigma_b \in G$ may be applied to this polynomial factor-wise (acting trivially upon x, of course) merely permuting the $\sigma_a(\alpha)$ among themselves. That is, G fixes this polynomial. On the other hand, multiplying the factors out, this invariance implies that the coefficients of f are G-invariant. By the proposition, the coefficients of f are in $\mathbb{Q}$. Thus, the degree of α over $\mathbb{Q}$ is at most the index $[G : H]$. ///

[3.0.7] **Remark:** We know that $(\mathbb{Z}/p)^\times$ is *cyclic* of order $p-1$, so we have many explicit subgroups available in any specific numerical example.

[3.0.8] **Example:** Returning to $p = 7$, with $\zeta = \zeta_7$ a primitive 7^{th} root of unity, we want an element of $\mathbb{Q}(\zeta_7)$ of degree 2 over $\mathbb{Q}$. Thus, by the previous two results, we want an element invariant under the (unique [11]) subgroup H of $G = (\mathbb{Z}/7)^\times$ of order 3. Since $2^3 = 1 \bmod 7$, (and $2 \neq 1 \bmod 7$) the automorphism

$$\sigma_2 : \zeta \longrightarrow \zeta^2$$

generates the subgroup H of order 3. Thus, consider

$$\alpha = \zeta + \sigma_2(\zeta) + \sigma_2^2(\zeta) = \zeta + \zeta^2 + \zeta^4$$

Note that this α is *not* invariant under σ_3, since

$$\sigma_3(\zeta + \zeta^2 + \zeta^4) = \zeta^3 + \zeta^6 + \zeta^{12} = \zeta^3 + \zeta^5 + \zeta^6$$

That is, $\alpha \notin \mathbb{Q}$. Of course, this is clear from its expression as a linear combination of powers of ζ. Thus, we have not overshot the mark in our attempt to make a field element inside a smaller subfield. The corollary assures that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [G : H] = \frac{6}{3} = 2$$

Since $\alpha \notin \mathbb{Q}$, we must have equality. The corollary assures us that

$$f(x) = (x - \alpha)(x - \sigma_3(\alpha))$$

has rational coefficients. Indeed, the linear coefficient is

$$-\big((\zeta + \zeta^2 + \zeta^4) + (\zeta^3 + \zeta^6 + \zeta^{12})\big) = -\big(1 + \zeta + \zeta^2 + \ldots + \zeta^5 + \zeta^6)\big) - 1 = -1$$

since $1 + \zeta + \ldots + \zeta^6 = 0$. The constant coefficient is

$$(\zeta + \zeta^2 + \zeta^4) \cdot (\zeta^3 + \zeta^6 + \zeta^{12})$$

$$= \zeta^{(1+3)} + \zeta^{(1+6)} + \zeta^{(1+12)}\zeta^{(2+3)} + \zeta^{(2+6)} + \zeta^{(2+12)}\zeta^{(4+3)} + \zeta^{(4+6)} + \zeta^{(4+12)}$$

$$= \zeta^4 + 1 + \zeta^6 + \zeta^5 + \zeta + 1 + 1 + \zeta^3 + \zeta^2 = 2$$

Thus, $\alpha = \zeta + \zeta^2 + \zeta^4$ satisfies the quadratic equation

$$x^2 + x + 2 = 0$$

On the other hand, by the quadratic formula we have the roots

$$\alpha = \frac{-1 \pm \sqrt{(-1)^2 - 4 \cdot 2}}{2} = \frac{-1 \pm \sqrt{-7}}{2}$$

[11] The group $(\mathbb{Z}/7)^\times$ is cyclic, since 7 is prime.

That is,

$$\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$$

This is not obvious. [12]

---

4. *Solution in radicals, Lagrange resolvents*

As an example, we follow a method of *J.-L. Lagrange* to obtain an expression for

$$\xi = \xi_7 = \zeta_7 + \frac{1}{\zeta_7}$$

in terms of *radicals*, that is, in terms of *roots*. Recall from above that ξ satisfies the cubic equation [13]

$$x^3 + x^2 - 2x - 1 = 0$$

Lagrange's method was to create an expression in terms of the roots of an equation designed to have more accessible symmetries than the original. In this case, let ω be a cube root of unity, not necessarily primitive. For brevity, let $\tau = \sigma_2$. The **Lagrange resolvent** associated to ξ and ω is

$$\lambda = \xi + \omega\tau(\xi) + \omega^2\tau^2(\xi)$$

Since $\sigma_{-1}(\xi) = \xi$, the effect on ξ of σ_a for $a \in G = (\mathbb{Z}/7)^\times$ depends only upon the coset $aH \in G/H$ where $H = \{\pm 1\}$. Convenient representatives for this quotient are $\{1, 2, 4\}$, which themselves form a subgroup. [14] Grant for the moment that we can extend σ_a to an automorphism on $\mathbb{Q}(\xi, \omega)$ over $\mathbb{Q}(\omega)$, which we'll still denote by σ_a. [15] Then the simpler behavior of the Lagrange resolvent λ under the automorphism $\tau = \sigma_2$ is

$$\tau(\lambda) = \tau(\xi + \omega\tau(\xi) + \omega^2\tau^2(\xi)) = \tau(\xi) + \omega\tau^2(\xi) + \omega^2\tau^3(\xi) = \tau(\xi) + \omega\tau^2(\xi) + \omega^2\xi = \omega^{-1} \cdot \lambda$$

since $\tau^3(\xi) = \xi$. Similarly, $\tau^2(\lambda) = \omega^{-2} \cdot \lambda$. Consider

$$f(x) = (x - \lambda)(x - \tau(\lambda))(x - \tau^2(\lambda)) = (x - \lambda)(x - \omega^{-1}\lambda)(x - \omega\lambda)$$

Multiplying this out, since $1 + \omega + \omega^2 = 0$,

$$f(x) = x^3 - \lambda^3$$

And note that, because τ is a ring homomorphism,

$$\tau(\lambda^3) = (\tau(\lambda))^3 = (\omega^{-1}\lambda)^3 = \lambda^3$$

---

[12] Not only is this assertion not obvious, but, also, there is the mystery of why it is $\sqrt{-7}$, not $\sqrt{7}$.

[13] After some experimentation, one may notice that, upon replacing x by $x + 2$, the polynomial $x^3 + x^2 - 2x - 1$ becomes

$$x^3 + (3 \cdot 2 + 1)x^2 + (3 \cdot 2^2 + 2 \cdot 2 - 2)x + (2^3 + 2^2 - 2 \cdot 2 - 1) = x^3 + 7x^2 - 14x + 7$$

which by Eisenstein's criterion is *irreducible* in $\mathbb{Q}[x]$. Thus, $[\mathbb{Q}(\xi) : \mathbb{Q}] = 3$. This irreducibility is part of a larger pattern involving roots of unity and Eisenstein's criterion.

[14] That there is a set of representatives forming a subgroup ought not be surprising, since a cyclic group of order 6 is isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/3$, by either the structure theorem, or, more simply, by Sun-Ze's theorem.

[15] All of ω, $\zeta = \zeta_7$, and ξ are contained in $\mathbb{Q}(\zeta_{21})$, for a primitive 21^{th} root of unity ζ_{21}. Thus, the *compositum* field $\mathbb{Q}(\xi, \omega)$ can be taken inside $\mathbb{Q}(\zeta_{21})$.

Therefore,[16] $\lambda^3 \in \mathbb{Q}(\omega)$. What is it? Let α, β, γ be the three roots of $x^3 + x^2 - 2x - 1 = 0$.

$$\lambda^3 = \big(\xi + \omega\tau(\xi) + \omega^2\tau^2(\xi)\big)^3 = \big(\alpha + \omega\beta + \omega^2\gamma\big)^3$$
$$= \alpha^3 + \beta^3 + \gamma^3 + 3\omega\alpha^2\beta + 3\omega^2\alpha\beta^2 + 3\omega^2\alpha^2\gamma + 3\omega\alpha\gamma^2 + 3\omega\beta^2\gamma + 3\omega^2\beta\gamma^2 + 6\alpha\beta\gamma$$
$$= \alpha^3 + \beta^3 + \gamma^3 + 3\omega(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\omega^2(\alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma) + 6\alpha\beta\gamma$$

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 elementary symmetric polynomials,

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

Thus,

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

Note that neither of the two expressions

$$\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha \qquad \alpha\beta^2 + \beta\gamma^2 + \alpha^2\gamma$$

is invariant under *all* permutations of α, β, γ, but only under powers of the *cycle*

$$\alpha \longrightarrow \beta \longrightarrow \gamma \longrightarrow \alpha$$

Thus, we cannot expect to use the symmetric polynomial algorithm to express the two parenthesized items in terms of elementary symmetric polynomials. A more specific technique is necessary.

Writing α, β, γ in terms of the 7^{th} root of unity ζ gives

$$\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2 = (\zeta + \zeta^6)(\zeta^2 + \zeta^5)^2 + (\zeta^2 + \zeta^5)(\zeta^4 + \zeta^3)^2 + (\zeta^4 + \zeta^3)(\zeta + \zeta^6)^2$$
$$= (\zeta + \zeta^6)(\zeta^4 + 2 + \zeta^3) + (\zeta^2 + \zeta^5)(\zeta + 2 + \zeta^6) + (\zeta^4 + \zeta^3)(\zeta^2 + 2\zeta^5)$$
$$= (\zeta + \zeta^6)(\zeta^4 + 2 + \zeta^3) + (\zeta^2 + \zeta^5)(\zeta + 2 + \zeta^6) + (\zeta^4 + \zeta^3)(\zeta^2 + 2 + \zeta^5)$$
$$= 4(\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6)$$
$$= -4$$

since[17] $\Phi_7(\zeta) = 0$. This is one part of the second parenthesized expression. The other is superficially very similar, but in fact has different details:

$$\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha = (\zeta + \zeta^6)^2(\zeta^2 + \zeta^5) + (\zeta^2 + \zeta^5)^2(\zeta^4 + \zeta^3) + (\zeta^4 + \zeta^3)^2(\zeta + \zeta^6)$$
$$= (\zeta^2 + 2 + \zeta^5)(\zeta^2 + \zeta^5) + (\zeta^4 + 2 + \zeta^3)(\zeta^4 + \zeta^3) + (\zeta + 2 + \zeta^6)(\zeta + \zeta^6)$$
$$= 6 + 3(\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6) = 3$$

[16] We will return to address this variant of our earlier proposition and corollary about invariant expressions lying in subfields.

[17] Anticipating that ζ must not appear in the final outcome, we could have managed some slightly clever economies in this computation. However, the element of redundancy here is a useful check on the accuracy of the computation.

From the equation $x^3 + x^2 - 2x - 1 = 0$ we have

$$s_1 = -1 \qquad s_2 = -2 \qquad s_3 = 1$$

Putting this together, we have

$$\lambda^3 = s_1^3 - 3s_1s_2 + 9s_3 + 3\omega \cdot 3 - 3\omega \cdot (-4) - 3(-4)$$

$$= (-1)^3 - 3(-1)(-2) + 9(1) + 3\omega \cdot 3 - 3\omega \cdot (-4) - 3(-4)$$

$$= -1 - 6 + 9 + +9\omega + 12\omega + 12 = 14 + 21\omega$$

That is,

$$\lambda = \sqrt[3]{14 + 21\omega}$$

or, in terms of ξ

$$\xi + \omega\tau(\xi) + \omega^2\tau^2(\xi) = \sqrt[3]{14 + 21\omega}$$

Now we will obtain a system of three linear equations which we can solve for ξ.

The same computation works for ω^2 in place of ω, since ω^2 is another primitive cube root of 1. The computation is much easier when ω is replaced by 1, since

$$(\alpha + 1 \cdot \beta + 1^2 \cdot \gamma)^3$$

is already $s_1^3 = -1$ Thus, fixing a primitive cube root ω of 1, we have

$$\begin{cases} \xi + \tau(\xi) + \tau^2(\xi) & = & -1 \\ \xi + \omega\tau(\xi) + \omega^2\tau^2(\xi) & = & \sqrt[3]{14 + 21\omega} \\ \xi + \omega^2\tau(\xi) + \omega\tau^2(\xi) & = & \sqrt[3]{14 + 21\omega^2} \end{cases}$$

Solving for ξ gives

$$\xi = \frac{-1 + \sqrt[3]{14 + 21\omega} + \sqrt[3]{14 + 21\omega^2}}{3}$$

Despite appearances, we know that ξ can in some sense be expressed without reference to the cube root of unity ω, since

$$\xi^3 + \xi^2 - 2\xi - 1 = 0$$

and this equations has rational coefficients. The apparent entanglement of a cube root of unity is an artifact of our demand to express ξ in terms of root-taking.

[4.0.1] Remark: There still remains the issue of being sure that the automorphisms σ_a of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ (with ζ a primitive 7^{th} root of unity) can be extended to automorphisms of $\mathbb{Q}(\zeta_7, \omega)$ over $\mathbb{Q}(\omega)$. As noted above, for a primitive 21^{th} root of unity η, we have

$$\zeta = \eta^3 \qquad \omega = \eta^7$$

so all the discussion above can take place inside $\mathbb{Q}(\eta)$.

We can take advantage of the fact discussed earlier that $\mathbb{Z}[\omega]$ is Euclidean, hence a PID.[18] Note that 7 is no longer prime in $\mathbb{Z}[\omega]$, since

$$7 = (2 - \omega)(2 - \omega^2) = (2 - \omega)(3 + \omega)$$

Let

$$N(a + b\omega) = (a + b\omega)(a + b\omega^2)$$

[18] We will eventually give a systematic proof that all cyclotomic polynomials are irreducible in $\mathbb{Q}[x]$.

be the *norm* discussed earlier. It is a multiplicative map $\mathbb{Z}[\omega] \longrightarrow \mathbb{Z}$, $N(a+b\omega) = 0$ only for $a+b\omega = 0$, and $N(a+b\omega) = 1$ if and only if $a+b\omega$ is a unit in $\mathbb{Z}[\omega]$. One computes directly

$$N(a+b\omega) = a^2 - ab + b^2$$

Then both $2-\omega$ and $3+\omega$ *are* prime in $\mathbb{Z}[\omega]$, since their norms are 7. They are not associate, however, since the hypothesis $3+\omega = \mu \cdot (2-\omega)$ gives

$$5 = (3+\omega) + (2-\omega) = (1+\mu)(2-\omega)$$

and then taking norms gives

$$25 = 7 \cdot N(1+\mu)$$

which is impossible. Thus, 7 is not a unit, and is square-free in $\mathbb{Z}[\omega]$.

In particular, we can still apply Eisenstein's criterion and Gauss' lemma to see that $\Phi_7(x)$ is irreducible in $\mathbb{Q}(\omega)[x]$. In particular,

$$[\mathbb{Q}(\zeta_7, \omega) : \mathbb{Q}(\omega)] = 6$$

And this allows an argument parallel to the earlier one for $\mathrm{Aut}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ to show that

$$(\mathbb{Z}/7)^\times \approx \mathrm{Aut}(\mathbb{Q}(\zeta_7, \omega)/\mathbb{Q}(\omega))$$

by

$$a \longrightarrow \tau_a$$

where

$$\tau_a(\zeta_7) = \zeta_7^a$$

Then the automorphisms σ_a of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$) are simply the *restrictions* of τ_a to $\mathbb{Q}(\zeta)$.

[4.0.2] **Remark:** If we look for zeros of the cubic $f(x) = x^3 + x^2 - 2x - 1$ in the real numbers $\mathbb{R}$, then we find three real roots. Indeed,

$$\begin{cases} f(2) &= 7 \\ f(1) &= -1 \\ f(-1) &= 1 \\ f(-2) &= -1 \end{cases}$$

Thus, by the intermediate value theorem there is a root in the interval $[1,2]$, a second root in the interval $[-1,1]$, and a third root in the interval $[-2,-1]$. All the roots are real. Nevertheless, the expression for the roots in terms of radicals involves primitive cube roots of unity, none of which is real. [19]

[19] Beginning in the Italian renaissance, it was observed that the formula for *real* roots to cubic equations involved complex numbers. This was troubling, both because complex numbers were certainly not widely accepted at that time, and because it seemed jarring that natural expressions for real numbers should necessitate complex numbers.

5. *Quadratic fields, quadratic reciprocity*

This discussion will do two things: show that all field extensions $\mathbb{Q}(\sqrt{D})$ lie inside fields $\mathbb{Q}(\zeta_n)$ obtained by adjoining primitive n^{th} roots of unity [20] to $\mathbb{Q}$, and prove *quadratic reciprocity.* [21]

Let p be an odd prime and x an integer. The **quadratic symbol** is defined to be

$$\left(\frac{a}{p}\right)_2 = \begin{cases} 0 & (\text{for } a = 0 \bmod p) \\ 1 & (\text{for } a \text{ a non-zero square mod } p) \\ -1 & (\text{for } a \text{ a non-square mod } p) \end{cases}$$

One part of quadratic reciprocity is an easy consequence of the cyclicness of $(\mathbb{Z}/p)^\times$ for p prime, and amounts to a restatement of earlier results:

[5.0.1] **Proposition:** For p an odd prime

$$\left(\frac{-1}{p}\right)_2 = (-1)^{(p-1)/2} = \begin{cases} 1 & (\text{for } p = 1 \bmod 4) \\ -1 & (\text{for } p = 3 \bmod 4) \end{cases}$$

Proof: If -1 is a square mod p, then a square root of it has order 4 in $(\mathbb{Z}p)^\times$, which is of order $p-1$. Thus, by Lagrange, $4|(p-1)$. This half of the argument does not need the cyclicness. On the other hand, suppose $4|(p-1)$. Since $(\mathbb{Z}/p)^\times$ is cyclic, there are exactly two elements α, β of order 4 in $(\mathbb{Z}/p)^\times$, and exactly one element -1 of order 2. Thus, the squares of α and β must be -1, and -1 has two square roots. ///

Refining the previous proposition, as a corollary of the cyclicness of $(\mathbb{Z}/p)^\times$, we have **Euler's criterion**:

[5.0.2] **Proposition:** *(Euler)* Let p be an odd prime. For an integer a

$$\left(\frac{a}{p}\right)_2 = a^{(p-1)/2} \bmod p$$

Proof: If $p|a$, this equality certainly holds. For $a \neq 0 \bmod p$ certainly $a^{(p-1)/2} = \pm 1 \bmod p$, since

$$\left(a^{(p-1)/2}\right)^2 = a^{p-1} = 1 \bmod p$$

and the only square roots of 1 in $\mathbb{Z}/p$ are ± 1. If $a = b^2 \bmod p$ is a non-zero square mod p, then

$$a^{(p-1)/2} = (b^2)^{(p-1)/2} = b^{p-1} = 1 \bmod p$$

This was the easy half. For the harder half we need the cyclicness. Let g be a generator for $(\mathbb{Z}/p)^\times$. Let $a \in (\mathbb{Z}/p)^\times$, and write $a = g^t$. If a is not a square mod p, then t must be odd, say $t = 2s+1$. Then

$$a^{(p-1)/2} = g^{t(p-1)/2} = g^{(2s+1)(p-1)/2} = g^{s(p-1)} \cdot g^{(p-1)/2} = g^{(p-1)/2} = -1$$

[20] The fact that every *quadratic* extension of $\mathbb{Q}$ is contained in a field generated by roots of unity is a very special case of the *Kronecker-Weber* theorem, which asserts that any *galois extension* of $\mathbb{Q}$ with *abelian* galois group lies inside a field generated over $\mathbb{Q}$ by roots of unity.

[21] Though Gauss was the first to give a proof of quadratic reciprocity, it had been conjectured by Lagrange some time before, and much empirical evidence supported the conclusion.

since g is of order $p-1$, and since -1 is the unique element of order 2. ///

[5.0.3] Corollary: The quadratic symbol has the multiplicative property

$$\left(\frac{ab}{p}\right)_2 = \left(\frac{a}{p}\right)_2 \cdot \left(\frac{b}{p}\right)_2$$

Proof: This follows from the expression for the quadratic symbol in the previous proposition. ///

A more interesting special case [22] is

[5.0.4] Theorem: For p an odd prime, we have the formula [23]

$$\left(\frac{2}{p}\right)_2 = (-1)^{(p^2-1)/8} = \begin{cases} 1 & (\text{for } p = 1 \bmod 8) \\ -1 & (\text{for } p = 3 \bmod 8) \\ -1 & (\text{for } p = 5 \bmod 8) \\ 1 & (\text{for } p = 7 \bmod 8) \end{cases}$$

Proof: Let i denote a square root of -1, and we work in the ring $\mathbb{Z}[i]$. Since the binomial coefficients $\binom{p}{k}$ are divisible by p for $0 < k < p$, in $\mathbb{Z}[i]$

$$(1+i)^p = 1^p + i^p = 1 + i^p$$

Also, $1+i$ is roughly a square root of 2, or at least of 2 times a unit in $\mathbb{Z}[i]$, namely

$$(1+i)^2 = 1 + 2i - 1 = 2i$$

Then, using Euler's criterion, in $\mathbb{Z}[i]$ modulo the ideal generated by p

$$\left(\frac{2}{p}\right)_2 = 2^{(p-1)/2} = (2i)^{(p-1)/2} \cdot i^{-(p-1)/2}$$

$$= \left((1+i)^2\right)^{(p-1)/2} \cdot i^{-(p-1)/2} = (1+i)^{p-1} \cdot i^{-(p-1)/2} \bmod p$$

Multiply both sides by $1+i$ to obtain, modulo p,

$$(1+i) \cdot \left(\frac{2}{p}\right)_2 = (1+i)^p \cdot i^{-(p-1)/2} = (1+i^p) \cdot i^{-(p-1)/2} \bmod p$$

The right-hand side depends only on p modulo 8, and the four cases given in the statement of the theorem can be computed directly. ///

The main part of quadratic reciprocity needs somewhat more preparation. Let p and q be distinct odd primes. Let $\zeta = \zeta_q$ be a primitive q^{th} root of unity. The **quadratic Gauss sum** mod q is

$$g = \sum_{b \bmod q} \zeta_q^b \cdot \left(\frac{b}{q}\right)_2$$

[22] Sometimes called a *supplementary* law of quadratic reciprocity.

[23] The expression of the value of the quadratic symbol as a power of -1 is just an interpolation of the values. That is, the expression $(p^2-1)/8$ does not present itself naturally in the argument.

[5.0.5] **Proposition:** Let q be an odd prime, ζ_q a primitive q^{th} root of unity. Then

$$g^2 = \left(\sum_{b \bmod q} \zeta_q^b \cdot \left(\frac{b}{q}\right)_2 \right)^2 = \left(\frac{-1}{q}\right)_2 \cdot q$$

That is, either $\sqrt{q}$ or $\sqrt{-q}$ is in $\mathbb{Q}(\zeta_q)$, depending upon whether q is 1 or 3 modulo 4.

Proof: Compute

$$g^2 = \sum_{a,b \bmod q} \zeta_q^{a+b} \cdot \left(\frac{ab}{q}\right)_2$$

from the multiplicativity of the quadratic symbol. And we may restrict the sum to a, b not 0 mod q. Then

$$g^2 = \sum_{a,b \bmod q} \zeta_q^{a+ab} \cdot \left(\frac{a^2 b}{q}\right)_2$$

by replacing b by ab mod q. Since $a \neq 0 \bmod q$ this is a bijection of $\mathbb{Z}/q$ to itself. Then

$$g^2 = \sum_{a \neq 0,\ b \neq 0} \zeta_q^{a+ab} \cdot \left(\frac{a^2}{q}\right)_2 \left(\frac{b}{q}\right)_2 = \sum_{a \neq 0,\ b \neq 0} \zeta_q^{a(1+b)} \cdot \left(\frac{b}{q}\right)_2$$

For fixed b, if $1 + b \neq 0 \bmod q$ then we can replace $a(1 + b)$ by a, since $1 + b$ is invertible mod q. With $1 + b \neq 0 \bmod q$, the inner sum over a is

$$\sum_{a \neq 0 \bmod q} \zeta_q^a = \left(\sum_{a \bmod q} \zeta_q^a \right) - 1 = 0 - 1 = -1$$

When $1 + b = 0 \bmod q$, the sum over a is $q - 1$. Thus, the whole is

$$g^2 = \sum_{b = -1 \bmod q} (q-1) \cdot \left(\frac{b}{q}\right)_2 - \sum_{b \neq 0, -1 \bmod q} \left(\frac{b}{q}\right)_2 = (q-1) \cdot \left(\frac{-1}{q}\right)_2 - \sum_{b \bmod q} \left(\frac{b}{q}\right)_2 + \left(\frac{-1}{q}\right)_2$$

Let c be a non-square mod q. Then $b \longrightarrow bc$ is a bijection of $\mathbb{Z}/q$ to itself, and so

$$\sum_{b \bmod q} \left(\frac{b}{q}\right)_2 = \sum_{b \bmod q} \left(\frac{bc}{q}\right)_2 = \left(\frac{c}{q}\right)_2 \cdot \sum_{b \bmod q} \left(\frac{b}{q}\right)_2 = - \sum_{b \bmod q} \left(\frac{b}{q}\right)_2$$

Since $A = -A$ implies $A = 0$ for integers A, we have

$$\sum_{b \bmod q} \left(\frac{b}{q}\right)_2 = 0$$

Then we have

$$g^2 = (q-1) \cdot \left(\frac{-1}{q}\right)_2 - \sum_{b \bmod q} \left(\frac{b}{q}\right)_2 + \left(\frac{-1}{q}\right)_2 = q \cdot \left(\frac{-1}{q}\right)_2$$

as claimed. ///

Now we can prove

[5.0.6] Theorem: *(Quadratic Reciprocity)* Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)_2 = (-1)^{(p-1)(q-1)/4} \cdot \left(\frac{q}{p}\right)_2$$

Proof: Using Euler's criterion and the previous proposition, modulo p in the ring $\mathbb{Z}[\zeta_q]$,

$$\left(\frac{q}{p}\right)_2 = q^{(p-1)/2} = \left(g^2 \left(\frac{-1}{q}\right)_2\right)^{(p-1)/2}$$

$$= g^{p-1}\left(\frac{-1}{q}\right)_2^{(p-1)/2} = g^{p-1}\left((-1)^{(q-1)/2}\right)^{(p-1)/2}$$

Multiply through by the Gauss sum g, to obtain

$$g \cdot \left(\frac{q}{p}\right)_2 = g^p \cdot (-1)^{(p-1)(q-1)/4} \bmod p$$

Since p divides the middle binomial coefficients, and since p is odd (so $(b/q)_2^p = (b/q)_2$ for all b),

$$g^p = \left(\sum_{b \bmod q} \zeta_q^b \cdot \left(\frac{b}{q}\right)_2\right)^p = \sum_{b \bmod q} \zeta_q^{bp} \cdot \left(\frac{b}{q}\right)_2 \bmod p$$

Since p is invertible modulo q, we can replace b by $bp^{-1} \bmod q$ to obtain

$$g^p = \sum_{b \bmod q} \zeta_q^b \cdot \left(\frac{bp^{-1}}{q}\right)_2 = \left(\frac{p^{-1}}{q}\right)_2 \cdot \sum_{b \bmod q} \zeta_q^b \cdot \left(\frac{b}{q}\right)_2 = \left(\frac{p}{q}\right)_2 \cdot g \bmod p$$

Putting this together,

$$g \cdot \left(\frac{q}{p}\right)_2 = \left(\frac{p}{q}\right)_2 \cdot g \cdot (-1)^{(p-1)(q-1)/4} \bmod p$$

We obviously want to cancel the factor of g, but we must be sure that it is invertible in $\mathbb{Z}[\zeta_q]$ modulo p. Indeed, since

$$g^2 = q \cdot \left(\frac{-1}{q}\right)_2$$

we could *multiply* both sides by g to obtain

$$q\left(\frac{-1}{q}\right)_2 \cdot \left(\frac{q}{p}\right)_2 \cdot q\left(\frac{-1}{q}\right)_2 = \left(\frac{p}{q}\right)_2 \cdot q\left(\frac{-1}{q}\right)_2 \cdot (-1)^{(p-1)(q-1)/4} \bmod p$$

Since $\pm q$ is invertible mod p, we cancel the $q(-1/q)_2$ to obtain

$$\left(\frac{q}{p}\right)_2 = \left(\frac{p}{q}\right)_2 \cdot (-1)^{(p-1)(q-1)/4} \bmod p$$

Both sides are ± 1 and $p > 2$, so we have an *equality* of integers

$$\left(\frac{q}{p}\right)_2 = \left(\frac{p}{q}\right)_2 \cdot (-1)^{(p-1)(q-1)/4}$$

which is the assertion of quadratic reciprocity. ///

6. *Worked examples*

[19.1] Let ζ be a primitive n^{th} root of unity in a field of characteristic 0. Let M be the n-by-n matrix with ij^{th} entry ζ^{ij}. Find the multiplicative inverse of M.

Some experimentation (and an exercise from the previous week) might eventually suggest consideration of the matrix A having ij^{th} entry $\frac{1}{n}\zeta^{-ij}$. Then the ij^{th} entry of MA is

$$(MA)_{ij} = \frac{1}{n}\sum_k \zeta^{ik-kj} = \frac{1}{n}\sum_k \zeta^{(i-j)k}$$

As an example of a *cancellation principle* we claim that

$$\sum_k \zeta^{(i-j)k} = \begin{cases} 0 & (\text{for } i-j \neq 0) \\ n & (\text{for } i-j = 0) \end{cases}$$

The second assertion is clear, since we'd be summing n 1's in that case. For $i-j \neq 0$, we can change variables in the indexing, replacing k by $k+1 \bmod n$, since ζ^a is well-defined for $a \in \mathbb{Z}/n$. Thus,

$$\sum_k \zeta^{(i-j)k} = \sum_k \zeta^{(i-j)(k+1)} = \zeta^{i-j}\sum_k \zeta^{(i-j)k}$$

Subtracting,

$$(1-\zeta^{i-j})\sum_k \zeta^{(i-j)k} = 0$$

For $i-j \neq 0$, the leading factor is non-zero, so the sum must be zero, as claimed. ///

[19.2] Let $\mu = \alpha\beta^2+\beta\gamma^2+\gamma\alpha^2$ and $\nu = \alpha^2\beta+\beta^2\gamma+\gamma^2\alpha$. Show that these are the two roots of a quadratic equation with coefficients in $\mathbb{Z}[s_1, s_2, s_3]$ where the s_i are the elementary symmetric polynomials in α, β, γ.

Consider the quadratic polynomial

$$(x-\mu)(x-\nu) = x^2 - (\mu+\nu)x + \mu\nu$$

We will be done if we can show that $\mu+\nu$ and $\mu\nu$ are symmetric polynomials as indicated. The sum is

$$\mu+\nu = \alpha\beta^2+\beta\gamma^2+\gamma\alpha^2+\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha$$

$$= (\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha) - 3\alpha\beta\gamma = s_1s_2 - 3s_3$$

This expression is plausibly obtainable by a few trial-and-error guesses, and examples nearly identical to this were done earlier. The product, being of higher degree, is more daunting.

$$\mu\nu = (\alpha\beta^2+\beta\gamma^2+\gamma\alpha^2)(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)$$

$$= \alpha^3+\alpha\beta^4+\alpha^2\beta^2\gamma^2+\alpha^2\beta^2\gamma^2+\beta^3\gamma^3+\alpha\beta\gamma^4+\alpha^4\beta\gamma+\alpha^2\beta^2\gamma^2+\alpha^3\gamma^3$$

Following the symmetric polynomial algorithm, at $\gamma = 0$ this is $\alpha^3\beta^3 = s_2(\alpha,\beta)^3$, so we consider

$$\frac{\mu\nu - s_2^3}{s_3} = \alpha^3+\beta^3+\gamma^3 - 3s_3 - 3(\mu+\nu)$$

where we are lucky that the last 6 terms were $\mu + \nu$. We have earlier found the expression for the sum of cubes, and we have expressed $\mu + \nu$, so

$$\frac{\mu\nu - s_2^3}{s_3} = (s_1^3 - 3s_1s_2 + 3s_3) - 3s_3 - 3(s_1s_2 - 3s_3) = s_1^3 - 6s_1s_2 + 9s_3$$

and, thus,

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

Putting this together, μ and ν are the two roots of

$$x^2 - (s_1s_2 - 3s_3)x + (s_2^3 + s_1^3s_3 - 6s_1s_2s_3 + 9s_3^2) = 0$$

(One might also speculate on the relationship of μ and ν to solution of the general cubic equation.) ///

[19.3] The 5^{th} cyclotomic polynomial $\Phi_5(x)$ factors into two irreducible quadratic factors over $\mathbb{Q}(\sqrt{5})$. Find the two irreducible factors.

We have shown that $\sqrt{5}$ occurs inside $\mathbb{Q}(\zeta)$, where ζ is a primitive fifth root of unity. Indeed, the discussion of Gauss sums in the proof of quadratic reciprocity gives us the convenient

$$\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}$$

We also know that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, since $x^2 - 5$ is irreducible in $\mathbb{Q}[x]$ (Eisenstein and Gauss). And $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ since $\Phi_5(x)$ is irreducible in $\mathbb{Q}[x]$ of degree $5 - 1 = 4$ (again by Eisenstein and Gauss). Thus, by multiplicativity of degrees in towers of fields, $[\mathbb{Q}(\zeta) : \mathbb{Q}(\sqrt{5})] = 2$.

Thus, since none of the 4 primitive fifth roots of 1 lie in $\mathbb{Q}(\sqrt{5})$, each is necessarily quadratic over $\mathbb{Q}(\sqrt{5})$, so has minimal polynomial over $\mathbb{Q}(\sqrt{5})$ which is quadratic, in contrast to the minimal polynomial $\Phi_5(x)$ over $\mathbb{Q}$. Thus, the 4 primitive fifth roots break up into two (disjoint) bunches of 2, grouped by being the 2 roots of the same quadratic over $\mathbb{Q}(\sqrt{5})$. That is, the fifth cyclotomic polynomial factors as the product of those two minimal polynomials (which are necessarily irreducible over $\mathbb{Q}(\sqrt{5})$).

In fact, we have a trick to determine the two quadratic polynomials. Since

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$$

divide through by ζ^2 to obtain

$$\zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = 0$$

Thus, regrouping,

$$\left(\zeta + \frac{1}{\zeta}\right)^2 + \left(\zeta + \frac{1}{\zeta}\right)^2 - 1 = 0$$

Thus, $\xi = \zeta + \zeta^{-1}$ satisfies the equation

$$x^2 + x - 1 = 0$$

and $\xi = (-1 \pm \sqrt{5})/2$. Then, from

$$\zeta + \frac{1}{\zeta} = (-1 \pm \sqrt{5})/2$$

multiply through by ζ and rearrange to

$$\zeta^2 - \frac{-1 \pm \sqrt{5}}{2}\,\zeta + 1 = 0$$

Thus,

$$x^4 + x^3 + x^2 + x + 1 = \left(x^2 - \frac{-1 + \sqrt{5}}{2}\,x + 1\right)\left(x^2 - \frac{-1 - \sqrt{5}}{2}\,x + 1\right)$$

Alternatively, to see what can be done similarly in more general situations, we recall that $\mathbb{Q}(\sqrt{5})$ is the subfield of $\mathbb{Q}(\zeta)$ fixed pointwise by the automorphism $\zeta \longrightarrow \zeta^{-1}$. Thus, the 4 primitive fifth roots of unity should be paired up into the orbits of this automorphism. Thus, the two (irreducible in $\mathbb{Q}(\sqrt{5})[x]$) quadratics are

$$(x-\zeta)(x-\zeta^{-1}) = x^2 - (\zeta+\zeta^{-1})x + 1$$
$$(x-\zeta^2)(x-\zeta^{-2}) = x^2 - (\zeta^2+\zeta^{-2})x + 1$$

Again, without imbedding things into the complex numbers, etc., there is no canonical one of the two square roots of 5, so the $\pm\sqrt{5}$ just means that whichever one we pick first the other one is its negative. Similarly, there is no distinguished one among the 4 primitive fifth roots unless we imbed them into the complex numbers. There is no need to do this. Rather, specify one ζ, and specify a $\sqrt{5}$ by

$$\zeta + \zeta^{-1} = \frac{-1+\sqrt{5}}{2}$$

Then necessarily

$$\zeta^2 + \zeta^{-2} = \frac{-1-\sqrt{5}}{2}$$

And we find the same two quadratic equations again. Since they are necessarily the minimal polynomials of ζ and of ζ^2 over $\mathbb{Q}(\sqrt{5})$ (by the degree considerations) they are irreducible in $\mathbb{Q}(\sqrt{5})[x]$. ///

[19.4] The 7^{th} cyclotomic polynomial $\Phi_7(x)$ factors into two irreducible cubic factors over $\mathbb{Q}(\sqrt{-7}$. Find the two irreducible factors.

Let ζ be a primitive 7^{th} root of unity. Let $H = \langle\tau\rangle$ be the order 3 subgroup of the automorphism group $G \approx (\mathbb{Z}/7)^\times$ of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$, where $\tau = \sigma_2$ is the automorphism $\tau(\zeta) = \zeta^2$, which has order 3. We have seen that $\mathbb{Q}(\sqrt{-7})$ is the subfield fixed pointwise by H. In particular, $\alpha = \zeta + \zeta^2 + \zeta^4$ should be at most quadratic over $\mathbb{Q}$. Recapitulating the earlier discussion, α is a zero of the quadratic polynomial

$$(x - (\zeta + \zeta^2 + \zeta^4))(x - (\zeta^3 + \zeta^6 + \zeta^5))$$

which will have coefficients in $\mathbb{Q}$, since we have arranged that the coefficients are G-invariant. Multiplying out and simplifying, this is

$$x^2 + x + 2$$

with zeros $(-1 \pm \sqrt{-7})/2$.

The coefficients of the polynomial

$$(x-\zeta)(x-\tau(\zeta))(x-\tau^2(\zeta)) = (x-\zeta)(x-\zeta^2)(x-\zeta^4)$$

will be H-invariant and therefore will lie in $\mathbb{Q}(\sqrt{-7})$. In parallel, taking the primitive 7^{th} root of unity ζ^3 which is not in the H-orbit of ζ, the cubic

$$(x-\zeta^3)(x-\tau(\zeta^3))(x-\tau^2(\zeta^3)) = (x-\zeta^3)(x-\zeta^6)(x-\zeta^5)$$

will also have coefficients in $\mathbb{Q}(\sqrt{-7})$. It is no coincidence that the exponents of ζ occuring in the two cubics are disjoint and exhaust the list $1, 2, 3, 4, 5, 6$.

Multiplying out the first cubic, it is

$$(x-\zeta)(x-\zeta^2)(x-\zeta^4) = x^3 - (\zeta+\zeta^2+\zeta^4)x^2 + (\zeta^3+\zeta^5+\zeta^6)x - 1$$
$$= x^3 - \left(\frac{-1+\sqrt{-7}}{2}\right)x^2 + \left(\frac{-1-\sqrt{-7}}{2}\right)x - 1$$

for a choice of ordering of the square roots. (Necessarily!) the other cubic has the roles of the two square roots reversed, so is

$$(x-\zeta^3)(x-\zeta^6)(x-\zeta^2) = x^3 - (\zeta^3+\zeta^5+\zeta^6)x + (\zeta+\zeta^2+\zeta^4)x - 1$$

$$= x^3 - \left(\frac{-1-\sqrt{-7}}{2}\right)x^2 + \left(\frac{-1+\sqrt{-7}}{2}\right)x - 1$$

Since the minimal polynomials of primitive 7^{th} roots of unity are of degree 3 over $\mathbb{Q}(\sqrt{-7})$ (by multiplicativity of degrees in towers), these cubics are irreducible over $\mathbb{Q}(\sqrt{-7})$. Their product is $\Phi_7(x)$, since the set of all 6 roots is all the primitive 7^{th} roots of unity, and there is no overlap between the two sets of roots. ///

[19.5] Let ζ be a primitive 13^{th} root of unity in an algebraic closure of $\mathbb{Q}$. Find an element α in $\mathbb{Q}(\zeta)$ which satisfies an irreducible cubic with rational coefficients. Find an element β in $\mathbb{Q}(\zeta)$ which satisfies an irreducible quartic with rational coefficients. Determine the cubic and the quartic explicitly.

Again use the fact that the automorphism group G of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/13)^\times$ by $a \longrightarrow \sigma_a$ where $\sigma_a(\zeta) = \zeta^a$. The unique subgroup A of order 4 is generated by $\mu = \sigma_5$. From above, an element $\alpha \in \mathbb{Q}(\zeta)$ fixed by A is of degree at most $|G|/|A| = 12/4 = 3$ over $\mathbb{Q}$. Thus, try symmetrizing/averaging ζ itself over the subgroup A by

$$\alpha = \zeta + \mu(\zeta) + \mu^2(\zeta) + \mu^3(\zeta) = \zeta + \zeta^5 + \zeta^{12} + \zeta^8$$

The unique subgroup B of order 3 in G is generated by $\nu = \sigma_3$. Thus, necessarily the coefficients of

$$(x-\alpha)(x-\nu(\alpha))(x-\nu^2(\alpha))$$

are in $\mathbb{Q}$. Also, one can see directly (because the ζ^i with $1 \le i \le 12$ are linearly independent over $\mathbb{Q}$) that the images $\alpha, \nu(\alpha), \nu^2(\alpha)$ are distinct, assuring that the cubic is irreducible over $\mathbb{Q}$.

To multiply out the cubic and determine the coefficients as rational numbers it is wise to be as economical as possible in the computation. Since we know *a priori* that the coefficients are rational, we need not drag along all the powers of ζ which appear, since there will necessarily be cancellation. Precisely, we compute in terms of the $\mathbb{Q}$-basis

$$1,\ \zeta,\ \zeta^2,\ \ldots,\ \zeta^{10},\ \zeta^{11}$$

Given ζ^n appearing in a sum, reduce the exponent n modulo 13. If the result is 0, add 1 to the sum. If the result is 12, add -1 to the sum, since

$$\zeta^{12} = -(1+\zeta+\zeta^2+\ldots+\zeta^{11})$$

expresses ζ^{12} in terms of our basis. If the reduction mod 13 is anything else, drop that term (since we know it will cancel). And we can go through the monomial summand in lexicographic order. Using this bookkeeping strategy, the cubic is

$$\left(x-(\zeta+\zeta^5+\zeta^{12}+\zeta^8)\right)\left(x-(\zeta^3+\zeta^2+\zeta^{10}+\zeta^{11})\right)\left(x-(\zeta^9+\zeta^6+\zeta^4+\zeta^7)\right)$$

$$= x^3 - (-1)x^2 + (-4)x - (-1) = x^3 + x^2 - 4x + 1$$

Yes, there are $3{\cdot}4^2$ terms to sum for the coefficient of x, and 4^3 for the constant term. Most give a contribution of 0 in our bookkeeping system, so the workload is not completely unreasonable. (A numerical computation offers a different sort of check.) Note that Eisenstein's criterion (and Gauss' lemma) gives another proof of the irreducibility, by replacing x by $x+4$ to obtain

$$x^3 + 13x^2 + 52x + 65$$

and noting that the prime 13 fits into the Eisenstein criterion here. This is yet another check on the computation.

For the quartic, reverse the roles of μ and ν above, so put

$$\beta = \zeta + \nu(\zeta) + \nu^2(\zeta) = \zeta + \zeta^3 + \zeta^9$$

and compute the coefficients of the quartic polynomial

$$(x-\beta)(x-\mu(\beta))(x-\mu^2(\beta))(x-\mu^3(\beta))$$

$$= \left(x - (\zeta+\zeta^3+\zeta^9)\right)\left(x - (\zeta^5+\zeta^2+\zeta^6)\right)\left(x - (\zeta^{12}+\zeta^{10}+\zeta^4)\right)\left(x - (\zeta^8+\zeta^{11}+\zeta^7)\right)$$

Use the same bookkeeping approach as earlier, to allow a running tally for each coefficient. The sum of the 4 triples is -1. For the other terms some writing-out seems necessary. For example, to compute the constant coefficient, we have the product

$$(\zeta+\zeta^3+\zeta^9)(\zeta^5+\zeta^2+\zeta^6)(\zeta^{12}+\zeta^{10}+\zeta^4)(\zeta^8+\zeta^{11}+\zeta^7)$$

which would seem to involve 81 summands. We can lighten the burden by writing only the exponents which appear, rather than recopying zetas. Further, multiply the first two factors and the third and fourth, leaving a multiplication of two 9-term factors (again, retaining only the exponents)

$$(\,6\quad 3\quad 7\quad 8\quad 5\quad 9\quad 1\quad 11\quad 2\,)(\,7\quad 10\quad 6\quad 5\quad 8\quad 4\quad 12\quad 2\quad 11\,)$$

As remarked above, a combination of an exponent from the first list of nine with an exponent from the second list will give a non-zero contribution only if the sum (reduced modulo 13) is either 0 or 12, contributing 1 or -1 respectively. For each element of the first list, we can keep a running tally of the contributions from each of the 9 elements from the second list. Thus, grouping by the elements of the first list, the contributions are, respectively,

$$(1-1)+(1)+(1-1)+(1-1)+(-1+1)+(1)+(1-1)+(1)(-1+1) = 3$$

The third symmetric function is a sum of 4 terms, which we group into two, writing in the same style

$$(\,1\quad 3\quad 9\quad 5\quad 2\quad 6\,)(\,7\quad 10\quad 6\quad 5\quad 8\quad 4\quad 12\quad 2\quad 11\,)$$

$$+(\,6\quad 3\quad 7\quad 8\quad 5\quad 9\quad 1\quad 11\quad 2\,)(\,12\quad 10\quad 4\quad 8\quad 11\quad 7\,)$$

In each of these two products, for each item in the lists of 9, we tally the contributions of the 6 items in the other list, obtaining,

$$(0+0-1+0+1+1+1+0+0)+(1+1+0-1+0+1+0+0+0) = 4$$

The computation of the second elementary symmetric function is, similarly, the sum

$$(\,1\quad 3\quad 9\,)(\,5\quad 2\quad 6\quad 12\quad 10\quad 4\quad 8\quad 11\quad 7\,)$$

$$+(\,5\quad 2\quad 6\,)(\,12\quad 10\quad 4\quad 8\quad 11\quad 7\,)+(\,12\quad 10\quad 4\,)(\,8\quad 11\quad 7\,)$$

Grouping the contributions for each element in the lists $1,3,9$ and $5,2,6$ and $12,10,4$, this gives

$$[(1-1)+(1)+(1)]+[(1-1)+(-1+1)+(1)]+[0+0+(-1)] = 2$$

Thus, in summary, we have

$$x^4+x^3+2\,x^2-4x+3$$

Again, replacing x by $x+3$ gives

$$x^4 + 13x^3 + 65x^2 + 143x + 117$$

All the lower coefficients are divisible by 13, but not by 13^2, so Eisenstein proves irreducibility. This again gives a sort of verification of the correctness of the numerical computation. ///

[19.6] Let $f(x) = x^8 + x^6 + x^4 + x^2 + 1$. Show that f factors into two irreducible quartics in $\mathbb{Q}[x]$. Show that

$$x^8 + 5x^6 + 25x^4 + 125x^2 + 625$$

also factors into two irreducible quartics in $\mathbb{Q}[x]$.

The first assertion can be verified by an elementary trick, namely

$$x^8 + x^6 + x^4 + x^2 + 1 = \frac{x^{10} - 1}{x^2 - 1} = \frac{\Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)}{\Phi_1(x)\Phi_2(x)}$$

$$= \Phi_5(x)\Phi_{10}(x) = (x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$$

But we do learn something from this, namely that the factorization of the first octic into linear factors naturally has the eight linear factors occurring in two bunches of four, namely the primitive 5^{th} roots of unity and the primitive 10^{th} roots of unity. Let ζ be a primitive 5^{th} root of unity. Then $-\zeta$ is a primitive 10^{th}. Thus, the 8 zeros of the *second* polynomial will be $\sqrt{5}$ times primitive 5^{th} and 10^{th} roots of unity. The question is how to group them together in two bunches of four so as to obtain rational coefficients of the resulting two quartics.

The automorphism group G of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/10)^\times$, which is generated by $\tau(\zeta) = \zeta^3$. That is, taking a product of linear factors whose zeros range over an orbit of ζ under the automorphism group G,

$$x^4 + x^3 + x^2 + x + 1 = (x - \zeta)(x - \zeta^3)(x - \zeta^9)(x - \zeta^7)$$

has coefficients in $\mathbb{Q}$ and is the minimal polynomial for ζ over $\mathbb{Q}$. Similarly looking at the orbit of $-\zeta$ under the automorphism group G, we see that

$$x^4 - x^3 + x^2 - x + 1 = (x + \zeta)(x + \zeta^3)(x + \zeta^9)(x + \zeta^7)$$

has coefficients in $\mathbb{Q}$ and is the minimal polynomial for $-\zeta$ over $\mathbb{Q}$.

The discussion of Gauss sums in the proof of quadratic reciprocity gives us the convenient

$$\zeta - \zeta^2 - \zeta^3 + \zeta^4 = \sqrt{5}$$

Note that this expression allows us to see what effect the automorphism $\sigma_a(\zeta) = \zeta^a$ has on $\sqrt{5}$

$$\sigma_a(\sqrt{5}) = \sigma_a(\zeta - \zeta^2 - \zeta^3 + \zeta^4) = \begin{cases} \sqrt{5} & (\text{for } a = 1, 9) \\ -\sqrt{5} & (\text{for } a = 3, 7) \end{cases}$$

Thus, the orbit of $\sqrt{5}\zeta$ under G is

$$\sqrt{5}\zeta,\ \tau(\sqrt{5}\zeta) = -\sqrt{5}\zeta^3,\ \tau^2(\sqrt{5}\zeta) = \sqrt{5}\zeta^4,\ \tau^3(\sqrt{5}\zeta) = -\sqrt{5}\zeta^2$$

giving quartic polynomial

$$(x - \sqrt{5}\zeta)(x + \sqrt{5}\zeta^3)(x - \sqrt{5}\zeta^4)(x + \sqrt{5}\zeta^2)$$

$$= x^4 - \sqrt{5}(\zeta - \zeta^2 - \zeta^3 + \zeta^4)x^3 + 5(-\zeta^4 + 1 - \zeta^3 - \zeta^2 + 1 - \zeta)x^2 - 5\sqrt{5}(\zeta^4 - \zeta^2 + \zeta - \zeta^3)x + 25$$

$$= x^4 - 5x^3 + 15x^2 - 25x + 25$$

We might anticipate what happens with the other bunch of four zeros, but we can also compute directly (confirming the suspicion). The orbit of $-\sqrt{5}\zeta$ under G is

$$-\sqrt{5}\zeta,\ \tau(-\sqrt{5}\zeta) = \sqrt{5}\zeta^3,\ \tau^2(-\sqrt{5}\zeta) = -\sqrt{5}\zeta^4,\ \tau^3(-\sqrt{5}\zeta) = \sqrt{5}\zeta^2$$

giving quartic polynomial

$$(x+\sqrt{5}\zeta)(x-\sqrt{5}\zeta^3)(x+\sqrt{5}\zeta^4)(x-\sqrt{5}\zeta^2)$$
$$= x^4 + \sqrt{5}(\zeta - \zeta^2 - \zeta^3 + \zeta^4)x^3 + 5(-\zeta^4 + 1 - \zeta^3 - \zeta^2 + 1 - \zeta)x^2 + 5\sqrt{5}(\zeta^4 - \zeta^2 + \zeta - \zeta^3)x + 25$$
$$= x^4 + 5x^3 + 15x^2 + 25x + 25$$

Thus, we expect that

$$x^8 + 5x^6 + 25x^4 + 125x^2 + 625 = (x^4 - 5x^3 + 15x^2 - 25x + 25)\cdot(x^4 + 5x^3 + 15x^2 + 25x + 25)$$

Because of the sign flips in the odd-degree terms in the quartics, the octic is also

$$x^8 + 5x^6 + 25x^4 + 125x^2 + 625 = (x^4 + 15x^2 + 25)^2 - 25(x^3 + 5x)^2$$

(This factorization of an altered product of two cyclotomic polynomials is an *Aurifeuille-LeLasseur* factorization, after two amateur mathematicians who studied them, brought to wider attention by E. Lucas in the late 19th century.)

[19.7] Let p be a prime not dividing m. Show that in $\mathbb{F}_p[x]$

$$\Phi_{mp}(x) = \Phi_m(x)^{p-1}$$

From the recursive definition,

$$\Phi_{pm}(x) = \frac{x^{pm}-1}{\prod_{d|m}\Phi_{p^e d}(x)\cdot\prod_{d|m,\ d<m}\Phi_{pd}(x)}$$

In characteristic p, the numerator is $(x^m-1)^p$. The first product factor in the denominator is x^m-1. Thus, the whole is

$$\Phi_{pm}(x) = \frac{(x^m-1)^p}{(x^m-1)\cdot\prod_{d|m,\ d<m}\Phi_{pd}(x)}$$

By induction on $d<m$, in the last product in the denominator has factors

$$\Phi_{pd}(x) = \Phi_d(x)^{p-1}$$

Cancelling,

$$\Phi_{pm}(x) = \frac{(x^m-1)^p}{(x^m-1)\cdot\prod_{d|m,\ d<m}\Phi_d(x)^{p-1}} = \frac{(x^m-1)^{p-1}}{\prod_{d|m,\ d<m}\Phi_d(x)^{p-1}}$$
$$= \left(\frac{x^m-1}{\prod_{d|m,\ d<m}\Phi_d(x)}\right)^{p-1}$$

which gives $\Phi_m(x)^{p-1}$ as claimed, by the recursive definition. ///

Exercises

19.[6.0.1] Find two fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{11})$, where ζ_{11} is a primitive 11^{th} root of unity.

19.[6.0.2] The 5^{th} cyclotomic polynomial factors into two irreducibles in $\mathbb{F}_{19}[x]$. Find these two irreducibles.

19.[6.0.3] The 8^{th} cyclotomic polynomial factors into two irreducibles in $\mathbb{F}_7[x]$. Find these two irreducibles.

19.[6.0.4] The 8^{th} cyclotomic polynomial factors into two irreducible quadratics in $\mathbb{Q}(\sqrt{2})[x]$. Find these two irreducibles.