(*February 15, 2024*)

Discussion 06

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

[06.1] Show that a *finite* integral domain (no zero divisors) is necessarily a *field*.

Discussion: Let R be the integral domain. The integral domain property can be immediately paraphrased as that for $0 \neq x \in R$ the map $y \to xy$ has trivial kernel (as R-module map of R to itself, for example). Thus, it is injective. Since R is a finite set, an injective map of it to itself is a bijection. Thus, there is $y \in R$ such that $xy = 1$, proving that x is invertible. ///

[06.2] Let $P(x) = x^3 + ax + b \in k[x]$. Suppose that $P(x)$ factors into linear polynomials $P(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Give a polynomial condition on a, b for the α_i to be distinct.

Discussion: (One might try to do this as a symmetric function computation, but it's a bit tedious.)

If $P(x) = x^3 + ax + b$ has a repeated factor, then it has a common factor with its derivative $P'(x) = 3x^2 + a$.

If the characteristic of the field is 3, then the derivative is the constant a. Thus, if $a \neq 0$, $\gcd(P, P') = a \in k^\times$ is never 0. If $a = 0$, then the derivative is 0, and all the α_i are the same.

Now suppose the characteristic is not 3. In effect applying the Euclidean algorithm to P and P',

$$\left(x^3 + ax + b\right) - \frac{x}{3} \cdot \left(3x^2 + a\right) = ax + b - \frac{x}{3} \cdot a = \frac{2}{3}ax + b$$

If $a = 0$ then the Euclidean algorithm has already terminated, and the condition for distinct roots or factors is $b \neq 0$. Also, possibly surprisingly, at this point we need to consider the possibility that the characteristic is 2. If so, then the remainder is b, so if $b \neq 0$ the roots are always distinct, and if $b = 0$

Now suppose that $a \neq 0$, and that the characteristic is not 2. Then we can divide by $2a$. Continue the algorithm

$$\left(3x^2 + a\right) - \frac{9x}{2a} \cdot \left(\frac{2}{3}ax + b\right) = a + \frac{27b^2}{4a^2}$$

Since $4a^2 \neq 0$, the condition that P have no repeated factor is

$$4a^3 + 27b^2 \neq 0$$

[06.3] The first three **elementary symmetric functions** in indeterminates $x_1, \ldots, x_n$ are

$$\sigma_1 = \sigma_1(x_1, \ldots, x_n) = x_1 + x_2 + \ldots + x_n = \sum_i x_i$$

$$\sigma_2 = \sigma_2(x_1, \ldots, x_n) = \sum_{i<j} x_i x_j$$

$$\sigma_3 = \sigma_3(x_1, \ldots, x_n) = \sum_{i<j<\ell} x_i x_j x_\ell$$

Express $x_1^3 + x_2^3 + \ldots + x_n^3$ in terms of $\sigma_1, \sigma_2, \sigma_3$.

Discussion: Execute the algorithm given in the proof of the theorem. Thus, since the degree is 3, if we can derive the right formula for just 3 indeterminates, the same expression in terms of elementary symmetric

polynomials will hold generally. Thus, consider $x^3+y^3+z^3$. To approach this we first take $y=0$ and $z=0$, and consider x^3. This is $s_1(x)^3 = x^3$. Thus, we next consider

$$\left(x^3+y^3\right) - s_1(x,y)^3 = 3x^2y + 3xy^2$$

As the algorithm assures, this is divisible by $s_2(x,y) = xy$. Indeed,

$$\left(x^3+y^3\right) - s_1(x,y)^3 = (3x+3y)s_2(x,y) = 3s_1(x,y)\,s_2(x,y)$$

Then consider

$$\left(x^3+y^3+z^3\right) - \left(s_1(x,y,z)^3 - 3\,s_2(x,y,z)\,s_1(x,y,z)\right) = 3xyz = 3s_3(x,y,z)$$

Thus, again, since the degree is 3, this formula for 3 variables gives the general one:

$$x_1^3 + \ldots + x_n^3 = s_1^3 - 3s_1s_2 + 3s_3$$

where $s_i = s_i(x_1,\ldots,x_n)$.

[06.4] Express $\sum_{i\neq j} x_i^2x_j$ as a polynomial in the elementary symmetric functions of $x_1,\ldots,x_n$.

Discussion: We could (as in the previous problem) execute the algorithm that proves the theorem asserting that every symmetric (that is, S_n-invariant) polynomial in $x_1,\ldots,x_n$ is a polynomial in the elementary symmetric functions.

But, also, sometimes *ad hoc* manipulations can yield short-cuts, depending on the context. Here,

$$\sum_{i\neq j} x_i^2x_j = \sum_{i,j} x_i^2x_j - \sum_{i=j} x_i^2x_j = \left(\sum_i x_i^2\right)\left(\sum_j x_j\right) - \sum_i x_i^3$$

An easier version of the previous exercise gives

$$\sum_i x_i^2 = s_1^2 - 2s_2$$

and the previous exercise itself gave

$$\sum_i x_i^3 = s_1^3 - 3s_1s_2 + 3s_3$$

Thus,

$$\sum_{i\neq j} x_i^2x_j = (s_1^2-2s_2)\,s_1 - \left(s_1^3 - 3s_1s_2 + 3s_3\right) = s_1^3 - 2s_1s_2 - s_1^3 + 3s_1s_2 - 3s_3 = s_1s_2 - 3s_3$$

[06.5] Suppose the characteristic of the field k does not divide n. Let $\ell > 2$. Show that

$$P(x_1,\ldots,x_n) = x_1^n + \ldots + x_\ell^n$$

is irreducible in $k[x_1,\ldots,x_\ell]$.

Discussion: First, treating the case $\ell = 2$, we claim that x^n+y^n is not a unit and has no repeated factors in $k(y)[x]$. (We take the field of rational functions in y so that the resulting polynomial ring in a single variable is Euclidean, and, thus, so that we understand the behavior of its irreducibles.) Indeed, if we start executing the Euclidean algorithm on x^n+y^n and its derivative nx^{n-1} in x, we have

$$(x^n+y^n) - \frac{x}{n}(nx^{n-1}) = y^n$$

Note that n is invertible in k by the characteristic hypothesis. Since y is invertible (being non-zero) in $k(y)$, this says that the *gcd* of the polynomial in x and its derivative is 1, so there is no repeated factor. And the degree in x is positive, so $x^n + y^n$ has *some* irreducible factor (due to the unique factorization in $k(y)[x]$, or, really, due indirectly to its Noetherian-ness).

Thus, our induction (on n) hypothesis is that $x_2^n + x_3^n + \ldots + x_\ell^n$ is a non-unit in $k[x_2, x_3, \ldots, x_n]$ and has no repeated factors. That is, it is divisible by some irreducible p in $k[x_2, x_3, \ldots, x_n]$. Then in

$$k[x_2, x_3, \ldots, x_n][x_1] \approx k[x_1, x_2, x_3, \ldots, x_n]$$

Eisenstein's criterion applied to $x_1^n + \ldots$ as a polynomial in x_1 with coefficients in $k[x_2, x_3, \ldots, x_n]$ and using the irreducible p yields the irreducibility.

[06.6] Find the determinant of the **circulant** matrix

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_{n-2} & x_{n-1} & x_n \\ x_n & x_1 & x_2 & \ldots & x_{n-2} & x_{n-1} \\ x_{n-1} & x_n & x_1 & x_2 & \ldots & x_{n-2} \\ \vdots & & & \ddots & & \vdots \\ x_3 & & & & x_1 & x_2 \\ x_2 & x_3 & \ldots & & x_n & x_1 \end{pmatrix}$$

(*Hint:* Let ζ be an n^{th} root of 1. If $x_{i+1} = \zeta \cdot x_i$ for all indices $i < n$, then the $(j+1)^{th}$ row is ζ times the j^{th}, and the determinant is 0.)

Discussion: Let C_{ij} be the ij^{th} entry of the circulant matrix C. The expression for the determinant

$$\det C = \sum_{p \in S_n} \sigma(p)\, C_{1,p(1)} \ldots C_{n,p(n)}$$

where $\sigma(p)$ is the sign of p shows that the determinant is a polynomial in the entries C_{ij} with integer coefficients. This is the most universal viewpoint that could be taken. However, with some hindsight, some intermediate manipulations suggest or require enlarging the 'constants' to include n^{th} roots of unity ω. Since we do not know that $\mathbb{Z}[\omega]$ is a UFD (and, indeed, it is not, in general), we must adapt. A reasonable adaptation is to work over $\mathbb{Q}(\omega)$. Thus, we will prove an identity in $\mathbb{Q}(\omega)[x_1, \ldots, x_n]$.

Add ω^{i-1} times the i^{th} row to the first row, for $i \geq 2$. The new first row has entries, from left to right,

$$x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{n-1} x_n$$

$$x_2 + \omega x_3 + \omega^2 x_4 + \ldots + \omega^{n-1} x_{n-1}$$

$$x_3 + \omega x_4 + \omega^2 x_5 + \ldots + \omega^{n-1} x_{n-2}$$

$$x_4 + \omega x_5 + \omega^2 x_6 + \ldots + \omega^{n-1} x_{n-3}$$

$$\ldots$$

$$x_2 + \omega x_3 + \omega^2 x_4 + \ldots + \omega^{n-1} x_1$$

The t^{th} of these is

$$\omega^{-t} \cdot (x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{n-1} x_n)$$

since $\omega^n = 1$. Thus, in the ring $\mathbb{Q}(\omega)[x_1, \ldots, x_n]$,

$$x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{n-1} x_n)$$

divides this new top row. Therefore, from the explicit formula, for example, this quantity divides the determinant.

Since the characteristic is 0, the n roots of $x^n - 1 = 0$ are distinct (for example, by the usual computation of *gcd* of $x^n - 1$ with its derivative). Thus, there are n superficially-different linear expressions which divide $\det C$. Since the expressions are linear, they are *irreducible* elements. If we prove that they are *non-associate* (do not differ merely by units), then their product must divide $\det C$. Indeed, viewing these linear expressions in the larger ring

$$\mathbb{Q}(\omega)(x_2, \ldots, x_n)[x_1]$$

we see that they are distinct linear monic polynomials in x_1, so are non-associate.

Thus, for some $c \in \mathbb{Q}(\omega)$,

$$\det C = c \cdot \prod_{1 \le \ell \le n} \left(x_1 + \omega^\ell x_2 + \omega^{2\ell} x_3 + \omega^{3\ell} x_4 + \ldots + \omega^{(n-1)\ell} x_n \right)$$

Looking at the coefficient of x_1^n on both sides, we see that $c = 1$.

(One might also observe that the product, when expanded, will have coefficients in $\mathbb{Z}$.)

[06.7] Let $f(x)$ be a monic polynomial with integer coefficients. Show that f is irreducible in $\mathbb{Q}[x]$ if it is irreducible in $(\mathbb{Z}/p)[x]$ for some p.

Discussion: First, claim that if $f(x)$ is irreducible in some $(\mathbb{Z}/p)[x]$, then it is irreducible in $\mathbb{Z}[x]$. A factorization $f(x) = g(x) \cdot h(x)$ in $\mathbb{Z}[x]$ maps, under the natural $\mathbb{Z}$-algebra homomorphism to $(\mathbb{Z}/p)[x]$, to the corresponding factorization $f(x) = g(x) \cdot h(x)$ in $(\mathbb{Z}/p)[x]$. (There's little reason to invent a notation for the reduction modulo p of polynomials as long as we are clear what we're doing.) A critical point is that since f is monic both g and h can be taken to be monic also (multiplying by -1 if necessary), since the highest-degree coefficient of a product is simply the product of the highest-degree coefficients of the factors. The irreducibility over $\mathbb{Z}/p$ implies that the degree of one of g and h modulo p is 0. Since they are monic, reduction modulo p does not alter their degrees. Since f is monic, its content is 1, so, by Gauss' lemma, the factorization in $\mathbb{Z}[x]$ is not proper, in the sense that either g or h is just ± 1.

That is, f is irreducible in the ring $\mathbb{Z}[x]$. Again by Gauss' lemma, this implies that f is irreducible in $\mathbb{Q}[x]$.

[06.8] Let n be a positive integer such that $(\mathbb{Z}/n)^\times$ is *not* cyclic. Show that the n^{th} cyclotomic polynomial $\Phi_n(x)$ factors properly in $\mathbb{F}_p[x]$ for any prime p not dividing n.

Discussion: (See subsequent text for systematic treatment of the case that p divides n.) Let d be a positive integer such that $p^d - 1 = 0 \bmod n$. Since we know that $\mathbb{F}_{p^d}^\times$ is cyclic, $\Phi_n(x) = 0$ has a root in $\mathbb{F}_{p^d}$ when $p^d - 1 = 0 \bmod n$. For $\Phi_n(x)$ to be irreducible in $\mathbb{F}_p[x]$, it must be that $d = \varphi(n)$ (Euler's totient function φ) is the smallest exponent which achieves this. That is, $\Phi_n(x)$ will be irreducible in $\mathbb{F}_p[x]$ only if $p^{\varphi(n)} = 1 \bmod n$ but no smaller positive exponent achieves this effect. That is, $\Phi_n(x)$ is irreducible in $\mathbb{F}_p[x]$ only if p is of order $\varphi(n)$ in the group $(\mathbb{Z}/n)^\times$. We know that the order of this group is $\varphi(n)$, so any such p would be a generator for the group $(\mathbb{Z}/n)^\times$. That is, the group would be cyclic.

[06.9] Show that the 15^{th} cyclotomic polynomial $\Phi_{15}(x)$ is irreducible in $\mathbb{Q}[x]$, despite being reducible in $\mathbb{F}_p[x]$ for every prime p.

Discussion: First, by Sun-Ze

$$(\mathbb{Z}/15)^\times \approx (\mathbb{Z}/3)^\times \times (\mathbb{Z}/5)^\times \approx \mathbb{Z}/2 \oplus \mathbb{Z}/4$$

This is not cyclic (there is no element of order 8, as the maximal order is 4). Thus, by the previous problem, there is no prime p such that $\Phi_{15}(x)$ is irreducible in $\mathbb{F}_p[x]$.

To prove that Φ_{15} is irreducible in $\mathbb{Q}[x]$, it suffices to show that the field extension $\mathbb{Q}(\zeta)$ of $\mathbb{Q}$ generated by any root ζ of $\Phi_{15}(x) = 0$ (in some algebraic closure of $\mathbb{Q}$, if one likes) is of degree equal to the degree of the polynomial Φ_{15}, namely $\varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$. We already know that Φ_3 and Φ_5 are irreducible. And one notes that, given a primitive 15^{th} root of unity ζ, $\eta = \zeta^3$ is a primitive 5^{th} root of unity and $\omega = \zeta^5$ is a primitive third root of unity. And, given a primitive cube root of unity ω and a primitive 5^{th} root of unity η, $\zeta = \omega^2 \cdot \eta^{-3}$ is a primitive 15^{th} root of unity: in fact, if ω and η are produced from ζ, then this formula recovers ζ, since

$$2 \cdot 5 - 3 \cdot 3 = 1$$

Thus,

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)(\eta)$$

By the multiplicativity of degrees in towers of fields

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\omega)] \cdot [\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\omega)] \cdot 2 = [\mathbb{Q}(\omega, \eta) : \mathbb{Q}(\omega)] \cdot 2$$

Thus, it would suffice to show that $[\mathbb{Q}(\omega, \eta) : \mathbb{Q}(\omega)] = 4$.

We should not forget that we have shown that $\mathbb{Z}[\omega]$ is Euclidean, hence a PID, hence a UFD. Thus, we are entitled to use Eisenstein's criterion and Gauss' lemma. Thus, it would suffice to prove irreducibility of $\Phi_5(x)$ in $\mathbb{Z}[\omega][x]$. As in the discussion of $\Phi_p(x)$ over $\mathbb{Z}$ with p prime, consider $f(x) = \Phi_5(x+1)$. All its coefficients are divisible by 5, and the constant coefficient is exactly 5 (in particular, not divisible by 5^2). We can apply Eisenstein's criterion and Gauss' lemma if we know, for example, that 5 is a prime in $\mathbb{Z}[\omega]$. (There are other ways to succeed, but this would be simplest.)

To prove that 5 is prime in $\mathbb{Z}[\omega]$, recall the *norm*

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

already used in discussing the Euclidean-ness of $\mathbb{Z}[\omega]$. One proves that the norm takes non-negative integer values, is 0 only when evaluated at 0, is *multiplicative* in the sense that $N(\alpha\beta) = N(\alpha)N(\beta)$, and $N(\alpha) = 1$ if and only if α is a unit in $\mathbb{Z}[\omega]$. Thus, if 5 were to factor $5 = \alpha\beta$ in $\mathbb{Z}[\omega]$, then

$$25 = N(5) = N(\alpha) \cdot N(\beta)$$

For a proper factorization, meaning that neither α nor β is a unit, neither $N(\alpha)$ nor $N(\beta)$ can be 1. Thus, both must be 5. However, the equation

$$5 = N(a + b\omega) = a^2 - ab + b^2 = (a - \frac{b}{2})^2 + \frac{3}{4}b^2 = \frac{1}{4}\left((2a-b)^2 + 3b^2\right)$$

has no solution in integers a, b. Indeed, looking at this equation mod 5, since 3 is not a square mod 5 it must be that $b = 0 \bmod 5$. Then, further, $4a^2 = 0 \bmod 5$, so $a = 0 \bmod 5$. That is, 5 divides both a and b. But then 25 divides the norm $N(a + b\omega) = a^2 - ab + b^2$, so it cannot be 5.

Thus, in summary, 5 is prime in $\mathbb{Z}[\omega]$, so we can apply Eisenstein's criterion to $\Phi_5(x+1)$ to see that it is irreducible in $\mathbb{Z}[\omega][x]$. By Gauss' lemma, it is irreducible in $\mathbb{Q}(\omega)[x]$, so $[\mathbb{Q}(\omega, \eta) : \mathbb{Q}(\omega)] = \varphi(5) = 4$. And this proves that $[\mathbb{Q}(\zeta) : \mathbb{Q})] = 8$, so $\Phi_{15}(x)$ is irreducible over $\mathbb{Q}$.

[06.10] Let p be a prime. Show that every degree d irreducible in $\mathbb{F}_p[x]$ is a factor of $x^{p^d-1} - 1$. Show that that the $(p^d - 1)^{th}$ cyclotomic polynomial's irreducible factors in $\mathbb{F}_p[x]$ are all of degree d.

Discussion: Let $f(x)$ be a degree d irreducible in $\mathbb{F}_p[x]$. For a linear factor $x - \alpha$ with α in some field extension of $\mathbb{F}_p$, we know that

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \text{ degree of minimal poly of } \alpha = \deg f = d$$

Since there is a unique (up to isomorphism) field extension of degree d of $\mathbb{F}_p$, *all* roots of $f(x) = 0$ lie in that field extension $\mathbb{F}_{p^d}$. Since the order of the multiplicative group $\mathbb{F}_{p^d}^\times$ is $p^d - 1$, by Lagrange the order of any non-zero element α of $\mathbb{F}_{p^d}$ is a divisor of $p^d - 1$. That is, α is a root of $x^{p^d-1} - 1 = 0$, so $x - \alpha$ divides $x^{p^d-1} - 1 = 0$. Since f is irreducible, f has no repeated factors, so $f(x) = 0$ has no repeated roots. By unique factorization (these linear factors are mutually distinct irreducibles whose least common multiple is their product), the product of all the $x - \alpha$ divides $x^{p^d-1} - 1$.

For the second part, similarly, look at the linear factors $x-\alpha$ of $\Phi_{p^d-1}(x)$ in a sufficiently large field extension of $\mathbb{F}_p$. Since p does not divide $n = p^d - 1$ there are no repeated factors. The multiplicative group of the field $\mathbb{F}_{p^d}$ is *cyclic*, so contains exactly $\varphi(p^d - 1)$ elements of (maximal possible) order $p^d - 1$, which are roots of $\Phi_{p^d-1}(x) = 0$. The degree of Φ_{p^d-1} is $\varphi(p^d - 1)$, so there are no *other* roots. No proper subfield $\mathbb{F}_{p^e}$ of $\mathbb{F}_{p^d}$ contains *any* elements of order $p^d - 1$, since we know that $e|d$ and the multiplicative group $\mathbb{F}_{p^e}^\times$ is of order $p^e - 1 < p^d - 1$. Thus, any linear factor $x - \alpha$ of $\Phi_{p^d-1}(x)$ has $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = d$, so the minimal polynomial $f(x)$ of α over $\mathbb{F}_p$ is necessarily of degree d. We claim that f divides Φ_{p^d-1}. Write

$$\Phi_{p^d-1} = q \cdot f + r$$

where q, r are in $\mathbb{F}_p[x]$ and $\deg r < \deg f$. Evaluate both sides to find $r(\alpha) = 0$. Since f was minimal over $\mathbb{F}_p$ for α, necessarily $r = 0$ and f divides the cyclotomic polynomial.

That is, any linear factor of Φ_{p^d-1} (over a field extension) is a factor of a degree d irreducible polynomial in $\mathbb{F}_p[x]$. That is, that cyclotomic polynomial factors into degree d irreducibles in $\mathbb{F}_p[x]$.

[06.11] Fix a prime p, and let ζ be a primitive p^{th} root of 1 (that is, $\zeta^p = 1$ and no smaller exponent will do). Let

$$V = \det \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \dots & \zeta^{p-1} \\ 1 & \zeta^2 & (\zeta^2)^2 & (\zeta^2)^3 & \dots & (\zeta^2)^{p-1} \\ 1 & \zeta^3 & (\zeta^3)^2 & (\zeta^3)^3 & \dots & (\zeta^3)^{p-1} \\ 1 & \zeta^4 & (\zeta^4)^2 & (\zeta^4)^3 & \dots & (\zeta^4)^{p-1} \\ \vdots & & & & & \vdots \\ 1 & \zeta^{p-1} & (\zeta^{p-1})^2 & (\zeta^{p-1})^3 & \dots & (\zeta^{p-1})^{p-1} \end{pmatrix}$$

Compute the rational number V^2.

Discussion: There are other possibly more natural approaches as well, but the following trick is worth noting. The ij^{th} entry of V is $\zeta^{(i-1)(j-1)}$. Thus, the ij^{th} entry of the square V^2 is

$$\sum_\ell \zeta^{(i-1)(\ell-1)} \cdot \zeta^{(\ell-1)(j-1)} = \sum_\ell \zeta^{(i-1+j-1)(\ell-1)} = \begin{cases} 0 & \text{if } (i-1)+(j-1) \neq 0 \bmod p \\ p & \text{if } (i-1)+(j-1) = 0 \bmod p \end{cases}$$

since

$$\sum_{0 \leq \ell < p} \omega^\ell = 0$$

for any p^{th} root of unity ω other than 1. Thus,

$$V^2 = \begin{pmatrix} p & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & p \\ 0 & 0 & 0 & \dots & p & 0 \\ & & & \iddots & & \\ 0 & 0 & p & \dots & 0 & 0 \\ 0 & p & 0 & \dots & 0 & 0 \end{pmatrix}$$

That is, there is a p in the upper left corner, and p's along the anti-diagonal in the lower right $(n-1)$-by-$(n-1)$ block. Thus, granting that the determinant squared is the square of the determinant,

$$(\det V)^2 = \det(V^2) = p^p \cdot (-1)^{(p-1)(p-2)/2}$$

Note that this did not, in fact, depend upon p being prime.

[06.12] Let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive 15^{th} root of unity. Find 4 fields k strictly between $\mathbb{Q}$ and K.

Discussion: Let ζ be a primitive 15^{th} root of unity. Then $\omega = \zeta^5$ is a primitive cube root of unity, and $\eta = \zeta^3$ is a primitive fifth root of unity. And $\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)(\eta)$.

Thus, $\mathbb{Q}(\omega)$ is one intermediate field, of degree 2 over $\mathbb{Q}$. And $\mathbb{Q}(\eta)$ is an intermediate field, of degree 4 over $\mathbb{Q}$ (so certainly distinct from $\mathbb{Q}(\omega)$.)

By now we know that $\sqrt{5} \in \mathbb{Q}(\eta)$, so $\mathbb{Q}(\sqrt{5})$ suggests itself as a third intermediate field. But one must be sure that $\mathbb{Q}(\omega) \neq \mathbb{Q}(\sqrt{5})$. We can try a direct computational approach in this simple case: suppose $(a+b\omega)^2 = 5$ with rational a, b. Then

$$5 = a^2 + 2ab\omega + b^2\omega^2 = a^2 + 2ab\omega - b^2 - b^2\omega = (a^2 - b^2) + \omega(2ab - b^2)$$

Thus, $2ab - b^2 = 0$. This requires either $b = 0$ or $2a - b = 0$. Certainly b cannot be 0, or 5 would be the square of a rational number (which we have long ago seen impossible). Try $2a = b$. Then, supposedly,

$$5 = a^2 - 2(2a)^2 = -3a^2$$

which is impossible. Thus, $\mathbb{Q}(\sqrt{5})$ is distinct from $\mathbb{Q}(\omega)$.

We know that $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. This might suggest

$$\mathbb{Q}(\sqrt{-3} \cdot \sqrt{5}) = \mathbb{Q}(\sqrt{-15})$$

as the fourth intermediate field. We must show that it is distinct from $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{5})$. If it were equal to either of these, then that field would also contain $\sqrt{5}$ and $\sqrt{-3}$, but we have already checked that (in effect) there is no quadratic field extension of $\mathbb{Q}$ containing both these.

Thus, there are (at least) intermediate fields $\mathbb{Q}(\eta)$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5}$, and $\mathbb{Q}(\sqrt{-15})$.

[06.13] 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.

Discussion: 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. ///

[06.14] 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.

Discussion: 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

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

$$= (\alpha + \beta + \gamma)(\alpha\beta + \beta\gamma + \gamma\alpha) - 3\alpha\beta\gamma = s_1 s_2 - 3s_3$$

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

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

and, thus,

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

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

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

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

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

Discussion: 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 lies 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 $\zeta \to \zeta^{-1}$. 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 $\mathbb{Q}(\sqrt{5})[x]$. ///

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

Discussion: 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

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

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

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

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. ///

[06.17] 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.

Discussion: Again use the fact that the automorphism group G of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/13)^\times$ by $a \to \sigma_a$ 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 notating 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. ///

[06.18] 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 $\mathbb{Q}[x]$.

Discussion: 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 8 linear factors occurring in two bunches of 4, 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 already be able to anticipate what happens with the other bunch of four zeros, but we can also compute directly (perhaps confirming a 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

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

Note that because of the sign flips in the odd-degree terms in the quartics, the octic can also be written as

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

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