Generators of Cyclotomic Subfields Thesis

Alexandra Sklyarova

Math 4961: Fall 2025

Abstract

A great man once said, "thou shall know algebraic numbers by their polynomials"

This simple phrase was meant to serve as a precursor to the beautiful world of Galois Theory and acts as the central motivation for this paper. More specifically, we will cover the theory of period polynomials, which are generators of unique subfields of cyclotomic fields. We will begin by explaining the theory and the construction of these polynomials as well as a brief history. We will then present existing Theorems related to the coefficients of period polynomials. Then, we will explain the methodology that was used to expand this study beyond what has been already proven. This section will be accompanied by several case studies and examples. Afterwards, we will present conjectures and give future directions to take beyond this paper. lastly, we will insert all of the Sage code that was used for the computation and include a brief explanation of how it works.

Contents

1 Theory of Period polynomials

1.1 Brief History

Cyclotomy refers to divisions of a circle:

Cyclo: Circle Tomo: Cut

This study certainly predates Gauss, but for the sake of our story, we will begin with his contributions. In his famous work Disquisitiones Arithmeticae, he proved the regular 17-gon is constructible and gave a sufficient condition for which other n-gons are constructible. The vertices of these regular n-gons live in cyclotomic fieldsRecall that the nth cyclotomic polynomial is defined by

$$\Phi_n(x) \;=\; \prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} \left(x - e^{2\pi i k/n}\right),$$

and it is the minimal polynomial of the primitive nth root of unity

$$\zeta_n = e^{2\pi i/n}.$$

Thus, instead of the equation

$$x^n - 1 = 0,$$

which has many non-primitive solutions, the polynomial $\Phi_n(x)$ isolates exactly the primitive ones. Therefore, we may refer to $\Phi_n(x)$ as *the* minimal polynomial of the algebraic number ζ_n.
It is natural to ask: what other subfields of $\mathbb{Q}(\zeta_n)$ exist besides the ones corresponding to regular n-gons?
Gauss answered this question fully for certain casesfor example, for cubic subfields of $\mathbb{Q}(\zeta_p)$ when $3 \mid (p-1)$ (a construction we will return to in a later section). However, as n grows, the subgroup structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ becomes increasingly complicated, and so does the structure of the intermediate fields of $\mathbb{Q}(\zeta_n)$.
While we will identify and explain several recurring patterns, determining all subfields of cyclotomic fields in general remains a deep and nontrivial problemwell beyond what one could hope to settle in an undergraduate thesis.

1.2 Galois Correspondence

First, recall one of the most important theorems from Galois Theory:

Galois Correspondence: Suppose we have a Galois extension E of field F. Let $\mathrm{Gal}(E/F)$ be the Galois group. Then there are mutually inverse bijections

$$\begin{array}{lcl} \{\text{subgroups } H < \mathrm{Gal}(E/F)\} & \longleftrightarrow & \{\text{intermediate fields } F \subset M \subset E\} \\ H & \longrightarrow & E^H \\ \mathrm{Aut}(E/M) & \longleftarrow & M \end{array}$$

Important Facts:

(a) $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ via the explicit isomorphism

$$\sigma_m(\zeta_n) = \zeta_n^m \qquad (m \in (\mathbb{Z}/n\mathbb{Z})^\times)$$

So, subfields K of $\mathbb{Q}(\zeta_n)$ correspond to a subgroup $H < (\mathbb{Z}/n\mathbb{Z})^\times$ according to the Galois Correspondence.

Also, we know

$$K = (\mathbb{Q}(\zeta_n))^H$$

and

$$[K : \mathbb{Q}] = \frac{\phi(n)}{|H|}$$

where $\phi(n)$ is Euler's Totient Function.

(b) Now, recall the Chinese Remainder Theorem allows us to decompose $(\mathbb{Z}/n\mathbb{Z})^\times$ into

$$(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{p|n} (\mathbb{Z}/p^e\mathbb{Z})^\times$$

where e is the power of p dividing n.

(c) Since each H corresponds to a subfield K_H with

$$[K_H : \mathbb{Q}] = \frac{\phi(n)}{|H|}$$

we can use the divisors of $\phi(n)$ to determine what our possible subfields can be.

Note: Also, note that we will be doing it for n where $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. This precisely occurs when $n = 2, 4, p^k, 2p^k$ (where p is an odd prime).

1.3 Explicit Construction using Gauss Sums

We will now give the explicit construction specifically when n is an odd prime p.
The group $\mathbb{F}_p^\times$ is cyclic of order $p-1$, so its subgroups correspond to divisors of $p-1$. Fix a divisor $d \mid (p-1)$ and let $H_d \leq \mathbb{F}_p^\times$ be the unique subgroup of index d. Then the fixed field $\mathbb{Q}(\zeta)^{H_d}$ is the unique subfield of $\mathbb{Q}(\zeta)$ of degree d over $\mathbb{Q}$. Moreover,

$$\mathbb{Q}(\zeta)^{H_d} = \mathbb{Q}(\alpha_d), \qquad \alpha_d := \sum_{h \in H_d} \zeta^h.$$

By the Galois correspondence, $\mathbb{Q}(\alpha_d) = \mathbb{Q}(\zeta)^J$ for a unique subgroup $J \leq \mathbb{F}_p^\times$. Since α_d is clearly H_d-invariant, we have $\mathbb{Q}(\zeta)^J \subseteq \mathbb{Q}(\zeta)^{H_d}$, hence $H_d \leq J$. It remains to show $J \leq H_d$. For any $s \in J$,

$$\sum_{h \in H_d} \zeta^h \;=\; \alpha_d \;=\; \sigma_s(\alpha_d) \;=\; \sum_{h \in H_d} \zeta^{hs}.$$

Here $\sigma_s \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ denotes the automorphism determined by

$$\sigma_s(\zeta) = \zeta^{\,s},$$

for $s \in (\mathbb{F}_p^\times) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. It acts on powers of ζ by $\sigma_s(\zeta^h) = \zeta^{hs}$.
Because $\{\zeta^k : k \in \mathbb{F}_p^\times\}$ forms a basis of $\mathbb{Q}(\zeta)$, it follows that $\zeta = \zeta^{hs}$ for some $h \in H_d$, so $hs \equiv 1 \pmod p$ and therefore $s \in H_d$. Thus $J \leq H_d$, proving $\mathbb{Q}(\alpha_d) = \mathbb{Q}(\zeta)^{H_d}$.
From this we get

$$[\mathbb{Q}(\alpha_d) : \mathbb{Q}] = [\mathbb{F}_p^\times : H_d] = d.$$

Gauss problem becomes: *find the minimal polynomial of α_d over $\mathbb{Q}$.*
Define

$$f_d(x) \;:=\; \prod_{k \in \mathbb{F}_p^\times / H_d} \big(x - \sigma_k(\alpha_d)\big).$$

Then $f_d(x)$ is invariant under the action of the Galois group, has α_d as a root, and $\deg f_d = d$. So, $f_d(x) \in [x]$ is the minimal monic polynomial of α_d. It remains to determine the coefficients of f_d.
Choose a generator g of the cyclic group $\mathbb{F}_p^\times$ and set $d' = (p-1)/d$. Then $H_d = \langle g^d \rangle$, and the choice of g yields an isomorphism

$$\mathbb{F}_p^\times \;\xrightarrow{\sim}\; \mathbb{Z}/(p-1)\mathbb{Z}, \qquad g^j \longmapsto j \pmod{p-1},$$

which sends H_d to the subgroup $\langle d \rangle$. Thus the partition of $\mathbb{F}_p^\times$ into right cosets of H_d corresponds to a partition

$$\mathbb{Z}/(p-1)\mathbb{Z} \;=\; \bigsqcup_{i=0}^{d-1} C_d(i), \qquad C_d(i) := \{\, dk + i :\; 0 \leq k \leq d' \,\}.$$

We have

$$\alpha_d \;=\; \sum_{k=1}^{d'} \zeta^{\,g^{dk}}, \qquad f_d(x) \;=\; \prod_{i=0}^{d-1} \big(x - \sigma_{g^i}(\alpha_d)\big),$$

and, for each i,

$$\sigma_{g^i}(\alpha_d) \;=\; \sum_{\ell \in C_d(i)} \zeta^{\,g^\ell}. \tag{1}$$

These sums are the *Gauss periods* (period polynomials) they are precisely the roots of f_d.

Define, with an indeterminate t,

$$A_i(t) \;:=\; \sum_{\ell \in C_d(i)} t^{\,g^\ell} \;\in\; \mathbb{Z}[t], \qquad 0 \leq i \leq d-1,$$

and

$$F_d(t,x) \;:=\; \prod_{i=0}^{d-1}\big(x - A_i(t)\big) \;\in\; R[x],$$

where $R = \mathbb{Z}[t]/\big(\Phi_p(t)\big)$. Evaluating $t = \zeta$ (equivalently, reducing modulo $\Phi_p(t)$) identifies $F_d(t,x)$ with $f_d(x)$.

1.4 Statements about Period Polynomials

Period Polynomials are irreducible
proof: Take $\sigma_m \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ which acts via $\sigma_m(\zeta) = \zeta^m$ for $m \in \mathbb{Z}/p\mathbb{Z}^\times$. So for all powers ζ^a, $a \in \mathbb{Z}$, we have $\sigma_m(\zeta^a) = \zeta^{am}$. Recall, we defined the roots to be

$$\alpha_i = \sum_{k=1}^{(p-1)/d} \zeta^{g^{dk+l}}$$

and we want to show that the Galois group acts transitively on these roots, i.e. there exists some element $\sigma_m \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that

$$\sigma_m\Big(\sum_{k=1}^{(p-1)/d} \zeta^{g^{dk+i}}\Big) = \sum_{k=1}^{(p-1)/d} \zeta^{g^{dk+j}}$$

for some $0 \le i, j < d$. Take $m = g^{j-i}$. Then we have

$$\sigma_{g^{j-i}}\Big(\sum_{k=1}^{(p-1)/d} \zeta^{g^{dk+i}}\Big) = \sigma_m\Big(\sum_{k=1}^{(p-1)/d} \zeta^{g^{dk+i}\cdot g^{j-i}}\Big) = \sigma_m\Big(\sum_{k=1}^{(p-1)/d} \zeta^{g^{dk+i+j-i}}\Big) = \sigma_m\Big(\sum_{k=1}^{(p-1)/d} \zeta^{g^{dk+j}}\Big)$$

So we can go from any one root to any other root, making the action on the period polynomials transitive. Over characteristic 0 field, the polynomial is separable, and if a Galois group acts transitively on its set of roots then the minimal polynomial of any root has all these roots, hence is irreducible. This directly means that these polynomials are irreducible over $\mathbb{Q}$.

Polynomials are independent of choice of generator
proof: Let g, g' be two generators of $\mathbb{F}_p^\times$. The generator g means that every element of $\mathbb{F}_p^\times$ can be written in the form $g^k \mod p$ for $0 \le k < p$. So say the other generator g' can be written as $g' = g^a$ if $gcd(a, p-1) = 1$. Now, as before let $d|p-1$ and define the cosets as we have previously. Since we have $g' = g^a$, we have $g'^k = g^{a^k}$. So for the two generators we have different cosets $\{g^{i+dk} \mod p : 0 \le k < d\}$ and $\{g^{a(i+dk)} \mod p : 0 \le k < d\}$.

Define a map

$$\kappa_a : \mathbb{F}_p^\times \to \mathbb{F}_p^\times, g^m \mapsto g^{am}$$

this is a group automorphism since $gcd(a, p-1) = 1$, which means it preserves cosets. So, $\{g^{i+dk} \mod p : 0 \le k < d\}$ contains the same elements as $\{g^{a(i+dk)} \mod p : 0 \le k < d\}$, but indices might differ.

So if we have

$$\alpha_i = \sum_{k=1}^{d-1} \zeta^{g^{dk+i}}$$

and

$$\alpha_i' = \sum_{k=1}^{d-1} \zeta^{g^{a(dk+i)}}$$

we will have

$$\prod_{i=0}^{d-1}(x - \sigma_{g^i}(\alpha_i)) = \prod_{i=0}^{d-1}(x - \sigma_{g^{ai}}(\alpha_i'))$$

so the period polynomials are the same regardless of generator.

Showing quadratic subfield of $\mathbb{Q}(\zeta_{p^r})$ is the same as that of $\mathbb{Q}(\zeta_p)$

proof: Let p be a prime and $r \geq 1$. Take a primitive p^r-th root of unity $\zeta_{p^r} = e^{2\pi i/p^r}$.
Once again, let p be an odd prime and $r \geq 1$. Take a primitive p^r-th root of unity $\zeta_{p^r} = e^{2\pi i/p^r}$. Then

$$\zeta_{p^r}^{p^{r-1}} = e^{2\pi i/p} = \zeta_p,$$

so $\zeta_p \in \mathbb{Q}(\zeta_{p^r})$ and hence

$$\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_{p^r}).$$

Since p is odd, Eulers totient function gives

$$[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \varphi(p^r) = p^{r-1}(p-1), \qquad [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

Therefore,

$$[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_p)] = \frac{p^{r-1}(p-1)}{p-1} = p^{r-1}.$$

Because $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield, namely

$$\mathbb{Q}\left(\sqrt{(-1)^{(p-1)/2}p}\right),$$

and this subfield is already contained in $\mathbb{Q}(\zeta_{p^r})$, the quadratic subfield of $\mathbb{Q}(\zeta_{p^r})$ is the same as that of $\mathbb{Q}(\zeta_p)$.

1.5 Discussion on Subfield Lattices

1.5 Discussion on Subfield Lattices

The lattice of intermediate fields of a cyclotomic extension $\mathbb{Q}(\zeta_n)$ is determined entirely by the subgroup lattice of the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \;\cong\; (\mathbb{Z}/n\mathbb{Z})^\times.$$

Period polynomials are useful for producing *explicit generators* of the corresponding subfields, but they are *not required* in order to determine the lattice structure itself.
The procedure below works whenever $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, namely for

$$n \in \{2,\ 4,\ p^k,\ 2p^k\} \quad \text{with } p \text{ an odd prime.}$$

In these cases one may choose a generator g of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, which allows for a clean coset description.

Computation Steps.

(a) Fix a subgroup $H_d < (\mathbb{Z}/n\mathbb{Z})^\times$ of index d. By the Galois correspondence,

$$[(\mathbb{Z}/n\mathbb{Z})^\times : H_d] = d \qquad \Longleftrightarrow \qquad [\mathbb{Q}(\zeta_n)^{H_d} : \mathbb{Q}] = d.$$

Since $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$, we also obtain

$$|H_d| = \frac{\varphi(n)}{d}.$$

(b) Choose coset representatives for the quotient

$$(\mathbb{Z}/n\mathbb{Z})^\times / H_d.$$

If g is a generator of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^\times$, then

$$\{\, 1, g, g^2, \ldots, g^{d-1} \,\}$$

is a complete set of coset representatives.

(c) For each $i = 0, \ldots, d-1$, define the coset

$$C_d(i) = \{\, g^{\,i+dk} \;:\; 0 \le k < |H_d| \,\} = \{\, g^{\,i+dk} \;:\; 0 \le k < \varphi(n)/d \,\}.$$

(Notice this replaces the special case $(p-1)/d$ used when $n = p$.)

(d) Define the corresponding Gaussian periods

$$\eta_i = \sum_{\ell \in C_d(i)} \zeta_n^{\ell}, \qquad i = 0, \ldots, d-1.$$

The d numbers $\eta_0, \ldots, \eta_{d-1}$ form the complete set of Galois conjugates of a generator of the intermediate field $\mathbb{Q}(\zeta_n)^{H_d}$, and hence their minimal polynomial is the degree-d period polynomial associated with H_d.

This construction produces explicit generators for all intermediate fields of $\mathbb{Q}(\zeta_n)$ in the cyclic cases listed above.

Interpreting the Polynomial Tables. For each divisor d of $\varphi(67)$, we obtain a Gaussian period

$$\alpha_d \;=\; \sum_{k \in C_d} \zeta_{67}^{k},$$

where C_d is the corresponding coset of H_d inside $(\mathbb{Z}/67\mathbb{Z})^{\times}$. In the notation used above, an expression such as $[k]_{67}$ simply means the power ζ_{67}^{k}.
Once the Gaussian period α_d is computed, we determine its minimal polynomial over $\mathbb{Q}$. The tables displayed for A (with $d = 6$) and B (with $d = 22$) are a compact way of writing these polynomials.

Each table has two rows:

- **The "exp" row** lists the exponents of x appearing in the polynomial.
- **The "coeff" row** lists the corresponding coefficients of x^{exp}.

For example, the table

exp	6	5	4	3	2	1	0
coeff	1	1	1	46	123	169	617

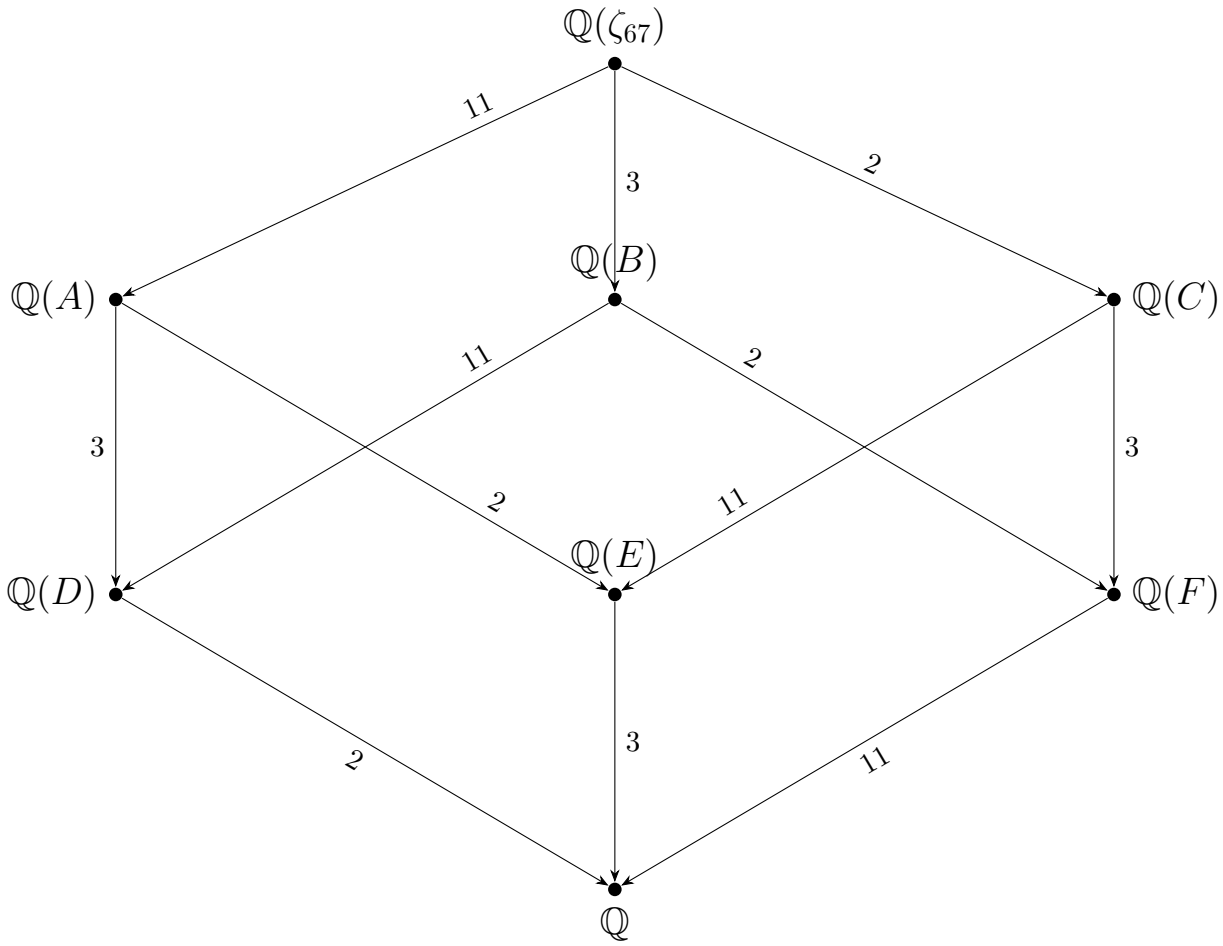
represents the polynomial

$$x^6 + x^5 + x^4 + 46x^3 + 123x^2 + 169x + 617,$$

which is the minimal polynomial of the period α_6.
Writing the coefficients in this table format mirrors the output produced by computer algebra systems and makes it easy to read off the polynomial without displaying a long expression. The same interpretation applies to the degree-22 polynomial associated with the period α_{22}.

Note: There are certain polynomials in this section that appear to have coefficients that vanish. The fact that all non-leading coefficients vanish in this case will be explained in a later section, where we discuss the phenomenon of vanishing period polynomials for prime-power moduli such as $81 = 3^4$.

Subfield lattice of ζ_{67}, a cyclic group of order 66



Notation note: ζ_{67}^k will be expressed as $[k]_{67}$

$$A \ \ (d = 6) \ : [1]_{67} + [4]_{67} + [14]_{67} + [15]_{67} + [22]_{67} + [24]_{67} + [25]_{67} + [40]_{67} + [59]_{67} + [62]_{67} + [64]_{67}$$

polynomial:

exp	6	5	4	3	2	1	0
coeff	1	1	6	46	123	169	617

$$B \ \ (d = 22) \ : [1]_{67} + [29]_{67} + [37]_{67}$$

polynomial:

exp	22	21	20	19	18	17	16	15	14	13	12	11
coeff	1	1	2	-40	-33	-59	535	361	574	-2902	-1439	-2088

exp	10	9	8	7	6	5	4	3	2	1	0
coeff	6412	3927	3984	-2341	-9804	-3508	355	5700	5006	-186	1073

$$C \ \ (d = 33) \ : [1]_{67} + [-1]_{67}$$

polynomial:

exp	33	32	31	30	29	28	27	26	25
coeff	1	1	-32	-31	465	435	4060	-3654	23751

exp	24	23	22	21	20	19	18	17	16
coeff	20475	-98280	80730	296010	230230	-657800	-480700	1081575	735471

exp	15	14	13	12	11	10	9	8	7
coeff	-1307504	-817190	1144066	646646	-705432	-352716	293930	125970	-77520

exp	6	5	4	3	2	1	0
coeff	-27132	11628	3060	-816	-136	17	1

$$D \ \ (d = 2) \ : \sqrt{-67}$$

polynomial:

exp	2	1	0
coeff	1	1	17

$$E \ \ (d = 3) \ : [1]_{67}+[3]_{67}+[5]_{67}+[8]_{67}+[9]_{67}+[14]_{67}+[15]_{67}+[22]_{67}+[24]_{67}+[25]_{67}+[27]_{67}+[40]_{67}+[42]_{67}+$$

$$[43]_{67} + [45]_{67} + [52]_{67} + [53]_{67} + [58]_{67} + [59]_{67} + [62]_{67} + [64]_{67} + [66]_{67}$$

polynomial:

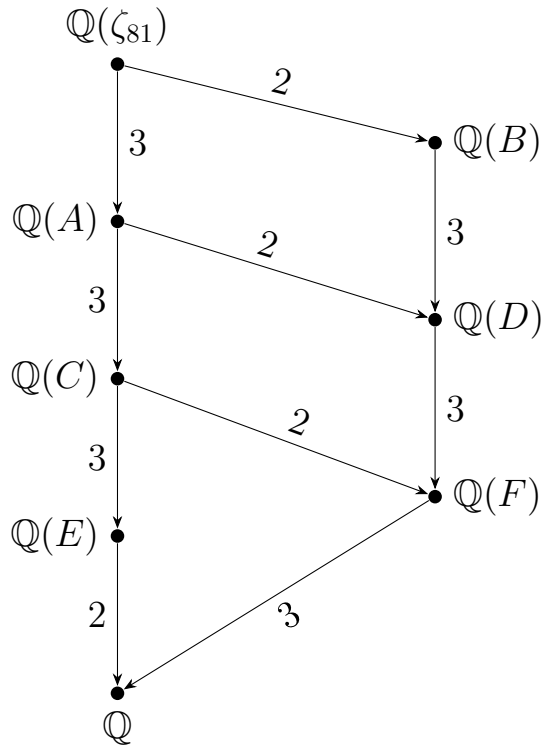
exp	3	2	1	0
coeff	1	1	-22	5

$$F \ \ (d = 11) \ = [1]_{67} + [29]_{67} + [30]_{67} + [37]_{67} + [38]_{67} + [66]_{67}$$

polynomial:

exp	11	10	9	8	7	6	5	4	3	2	1	0
coeff	1	1	-30	-63	220	698	-101	-1960	-1758	-35	243	-29

Subfield lattice of ζ_{81}, a cyclic group of order 54



$A \;\; (d = 18) \;\; : [1]_{81} + [28]_{81} + [55]_{81}$

polynomial:

exp	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
coeff	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

$B \;\; (d = 27) \;\; : [1]_{81} + [80]_{81}$

polynomial:

exp	27	26	25	24	23	22	21	20	19	18	17
coeff	1	0	-27	0	324	0	-2277	0	10395	0	-32319

exp	16	15	14	13	12	11	10	9	8	7
coeff	0	69768	0	104652	0	107406	0	-72930	0	30888

exp	6	5	4	3	2	1	0
coeff	0	-7371	0	819	0	-27	1

$C \;\; (d = 6) \;\; : [1]_{81} + [10]_{81} + [19]_{81} + [28]_{81} + [37]_{81} + [46]_{81} + [55]_{81} + [64]_{81} + [73]_{81}$

polynomial:

exp	6	5	4	3	2	1	0
coeff	1	0	0	0	0	0	0

$$D \ \ (d = 9) \ : [1]_{81} + [26]_{81} + [28]_{81} + [53]_{81} + [55]_{81} + [80]_{81}$$

polynomial:

exp	9	8	7	6	5	4	3	2	1	0
coeff	1	0	0	0	0	0	0	0	0	0

$$E \ \ (d = 2) \ : \sqrt{-3}$$

polynomial:

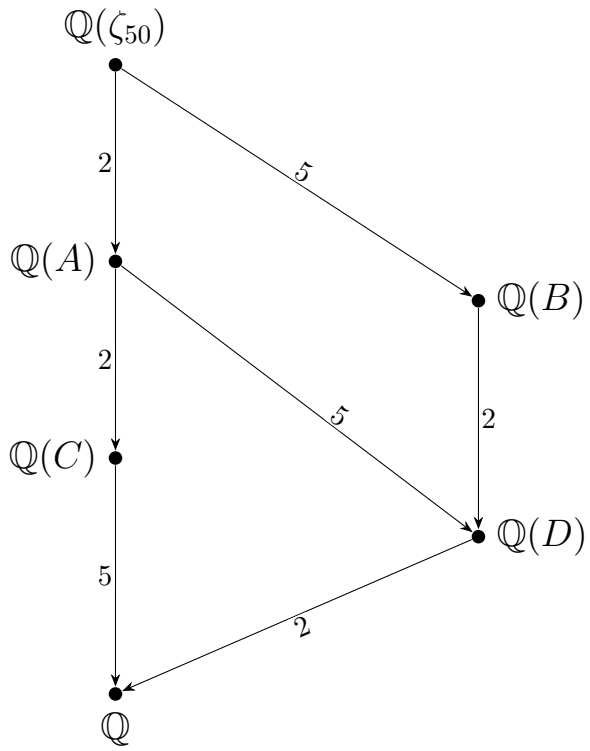
exp	2	0	0
coeff	1	0	0

$$F \ \ (d = 3) \ : [1]_{81}+[8]_{81}+[10]_{81}+[17]_{81}+[19]_{81}+[26]_{81}+[28]_{81}+[35]_{81}+[37]_{81}+[44]_{81}+[46]_{81}+[53]_{81}+[55]_{81}$$
$$+[62]_{81} + [64]_{81} + [71]_{81} + [73]_{81} + [80]_{81}$$

polynomial:

exp	3	2	1	0
coeff	1	0	0	0

Subfield lattice of ζ_{50}, a cyclic group of order 20



$A \ \ (d = 10) \ : [1]_{50} + [49]_{50}$

polynomial:

exp	10	9	8	7	6	5	4	3	2	1	0
coeff	1	-10	35	-1	-50	5	25	5	25	-5	-1

$B \ \ (d = 4) \ : [1]_{50} + [11]_{50} + [21]_{50} + [31]_{50} + [41]_{50}$

polynomial:

exp	4	3	2	1	0
coeff	1	0	0	0	0

$C \ \ (d = 5) \ : [1]_{50} + [7]_{50} + [43]_{50} + [49]_{50}$

polynomial:

exp	5	4	3	2	1	0
coeff	1	0	-10	-5	10	-1

$D \ \ (d = 2) \ : \sqrt{5}$

polynomial:

exp	2	1	0
coeff	1	0	0

2 Existing Theorems

2.1 Quadratic Extension

We can think about $\mathbb{Q}(\zeta)$ as being generated by $\sqrt{\varepsilon p}$, where $\varepsilon \in \{\pm 1\}$ is determined by $p \equiv \varepsilon \pmod 4$. Since our Galois group has a unique subgroup of index 2, namely there is a unique nontrivial homomorphism

$$\left(\tfrac{\cdot}{p}\right) \,:\, \mathbb{F}_p^\times \longrightarrow \{\pm 1\},$$

called the *Legendre symbol*, given by

$$\left(\tfrac{k}{p}\right) \;=\; \begin{cases} +1, & \text{if } k \in (\mathbb{F}_p^\times)^2, \\ -1, & \text{if } k \notin (\mathbb{F}_p^\times)^2. \end{cases}$$

It can be shown that the quadratic Gauss sum

$$G = \sum_{k \in \mathbb{F}_p^\times} \left(\tfrac{k}{p}\right) \zeta^k$$

satisfies

$$G^2 = \left(\tfrac{-1}{p}\right) p \;=\; \varepsilon\, p,$$

so the quadratic subfield is $\mathbb{Q}(\sqrt{\varepsilon p})$.
and the polynomial is of the form

$$f_2(x) = x^2 + x + \begin{cases} \frac{p+1}{4}, & \text{if } p \equiv 3 \mod 4, \\ \frac{1-p}{4}, & \text{if } p \equiv 1 \mod 4. \end{cases}$$

2.2 Degree $\frac{\phi(n)}{2}$ Extension

Consider the real subfield

$$\mathbb{R} \cap \mathbb{Q}(\zeta_n),$$

This is also the fixed field of complex conjugation on $\mathbb{Q}(\zeta_n)$. Since $\overline{\zeta_n} = \zeta_n^{-1}$, the corresponding subgroup (recall the Galois correspondence explained earlier) is $H = \{\pm 1\} \subset U_n$.
The real number

$$\gamma_n = \zeta_n + \zeta_n^{-1} = 2\cos\left(\frac{2\pi}{n}\right)$$

is fixed by H, hence $\mathbb{Q}(\gamma_n) \subset \mathbb{R} \cap \mathbb{Q}(\zeta_n)$.
Also, ζ_n is a root of the quadratic polynomial

$$f(x) \;=\; (x - \zeta_n)(x - \zeta_n^{-1}) \;=\; x^2 - \gamma_n x + 1 \;\in\; \mathbb{Q}(\gamma_n)[x].$$

Since f is quadratic with no real roots, it is irreducible over $\mathbb{Q}(\gamma_n)$. Therefore

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\gamma_n)] \;=\; 2,$$

and it follows that

$$F = \mathbb{Q}(\gamma_n).$$

Now, we will show how to calculate Ψ_n, the polynomial generating the degree $\frac{\phi(n)}{2}$ extension, from Φ_n. Let

$$\Phi_n(z) = \sum_{k=0}^{\varphi(n)} c_k\, z^k,$$

and let $m = \varphi(n)/2 = \deg \Psi_n$. Then

$$z^{-m}\Phi_n(z) = c_m + \sum_{k=1}^{m} c_k\, (z^k + z^{-k}).$$

Then we will have

$$z^{-m}\Phi_n(z) \;=\; c_m + \sum_{k=1}^{m} c_k\, Q_k(z + z^{-1}).$$

Evaluating both sides at $z = \zeta_n$ gives

$$0 = c_m + \sum_{k=1}^{m} c_k\, Q_k(\gamma_n),$$

and so

$$\Psi_n(x) = c_m + \sum_{k=1}^{m} c_k\, Q_k(x),$$

since the polynomial on the right is monic of degree m.

Constructing Q_k.
Define functions χ_k for integers $k \geq -1$ by

$$\chi_{-1} = 0, \qquad \chi_0 = 1, \qquad \chi_k(z) = z^k + z^{k-2} + \cdots + z^{2-k} + z^{-k} \quad (k \geq 1).$$

For $k \geq 1$ we have

$$z^k + z^{-k} = \chi_k(z) - \chi_{k-2}(z),$$

so it suffices to express $\chi_k(z)$ as a polynomial in $\chi_1 = z + z^{-1}$. The basic recursion is

$$\chi_1 \cdot \chi_k = \chi_{k+1} + \chi_{k-1}.$$

By induction on k this yields

$$\chi_k(z) \;=\; \sum_{j\geq 0}(-1)^j\binom{k-j}{j}\,\chi_1(z)^{\,k-2j},$$

(where $\binom{k-j}{j}=0$ if $k-j<j$). Therefore $\chi_k(z)=P_k(z+z^{-1})$, where the polynomials P_k for $k\geq -1$ are

$$P_{-1}=0, \qquad P_0=1, \qquad P_k(x)=\sum_{j\geq 0}(-1)^j\binom{k-j}{j}\,x^{k-2j}.$$

(The coefficients of P_k can be read off by moving northeast in Pascals triangle until zero and then alternating signs.)
Set

$$Q_k(x) \;=\; P_k(x)-P_{k-2}(x).$$

Then

$$Q_k(z+z^{-1}) \;=\; P_k(z+z^{-1})-P_{k-2}(z+z^{-1})=\chi_k(z)-\chi_{k-2}(z)=z^k+z^{-k}$$

Returning to $\Psi_n=\Psi_n(x)$, we get

$$\Psi_n(x) \;=\; c_m+\sum_{k=1}^{m}c_k\big(P_k(x)-P_{k-2}(x)\big).$$

If $n=p$ is prime, then $m=(p-1)/2$, all $c_k=1$, and the sum condenses to

$$\Psi_p(x) \;=\; P_m(x)+P_{m-1}(x).$$

2.3 Cubic Extension

This Theorem comes by way of Gauss (unsurprisingly).

Theorem on Cubic Extensions Let $p=1+3k$ be a prime with $p\equiv 1 \pmod 3$, and let $\zeta=e^{2\pi i/p}$. Then:

(a) There are unique integers A,B such that

$$4p \;=\; A^2+27B^2 \qquad \text{and} \qquad A\equiv 1 \pmod 3.$$

(b) The generator α_3 of the cubic subfield of $\mathbb{Q}(\zeta)$ has minimal polynomial

$$f_3(x) \;=\; x^3 + x^2 - k\,x - \frac{p(A+3)-1}{27},$$

whose discriminant is

$$D_{f_3} \;=\; (pB)^2.$$

(c) The number of points in $\mathbb{P}^2(\mathbb{F}_p)$ lying on the curve $X^3 + Y^3 + Z^3 = 0$ equals

$$p + 1 + A.$$

The proof for this is long and arduous and will thus be omitted. However, its connection to elliptic curves is fascinating. Part c of the statement involves discussing the number of solutions to the Fermat curve

$$x^3 + y^3 = 1$$

or the number of projective solutions to the homogeneous form of that equation. This interplay is something that will not be discussed here, but is certainly something worth looking into. The full details for this theorem can be seen in either Disquisitiones Arithmeticae by Gauss or Rational Points on Elliptic Curves by Silverman and Tate.

2.4 Quartic Extension

The methodology for computing the coefficients for quartic period polynomials comes from Gerald Myerson. The exact construction will be omitted but can be found in the paper titled "Period Polynomials and Gaussian Sums"

From the paper we get the following formula for the quartic period polynomial:

$$f_4(x) = \begin{cases} x^4 + x^3 - \frac{1}{8}(3q-3)x^2 + \frac{1}{16}((2s-3)q+1)x + \frac{1}{256}(q^2 - (4s^2-8s+6)q + 1), & \text{if f is even} \\ \\ x^4 + x^3 + \frac{1}{8}(q+3)x^2 + \frac{1}{16}((2s+1)q+1)x + \frac{1}{256}(9q^2 - (4s^2-8s-2)q + 1), & \text{if f is odd} \end{cases}$$

Discussion on the quartic Galois group and the cubic resolvent. Recall the classical quotient

$$S_4/D_2 \;\simeq\; S_3,$$

where

$$D_2 = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}.$$

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of our quartic

$$f(x) = \prod_{i=1}^{4}(x - \alpha_i).$$

The roots of the cubic resolvent are given by the well-known expressions

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \qquad \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \qquad \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Suppose now that the Galois group of the quartic is C_4, generated by the 4-cycle (1234). Its action on the β_i is

$$(1234): \qquad \{12\}\{34\} \longleftrightarrow \{14\}\{23\}, \qquad \{13\}\{24\} \text{ is fixed},$$

so exactly one of the β_i is fixed under the Galois action. Without loss of generality, assume it is β_3. Hence the resolvent polynomial $g(x)$ over $\mathbb{Q}$ factors as

$$g(x) = (x - \beta_3)\, h(x),$$

where $h(x)$ is a quadratic polynomial. Therefore the resolvent is reducible over $\mathbb{Q}$.

We use the following classical fact:
Fact. If the resolvent g has a rational root and its discriminant D_g is not a square in $\mathbb{Q}$, then the Galois group G_f of the quartic is either D_4 or C_4. Moreover,

$$G_f \simeq C_4 \quad \Longleftrightarrow \quad f \text{ is reducible over the subfield } M = \mathbb{Q}(\sqrt{D_f}),$$

where D_f is the discriminant of $f(x)$.
Here D_g is not a square means $D_g \notin \mathbb{Q}^2$, so the splitting field of g is a quadratic extension of $\mathbb{Q}$.

Explanation. If $G_f \not\simeq D_4$, then the only remaining possibility under the hypotheses above is $G_f \simeq C_4$. In this case, since g has a rational root (namely β_3), the remaining roots β_1, β_2 must lie in the unique quadratic subfield

$$M = \mathbb{Q}(\sqrt{D_f}).$$

Thus $g(x) = (x - \beta_3)\, h(x)$ with $h(x) \in M[x]$.
Under the Galois correspondence, the fixed field of the subgroup

$$\langle (12)(34) \rangle < S_4$$

is exactly M. Since $G_f \cong C_4$ is cyclic, it acts transitively on the four roots of f if and only if f is irreducible over M. But the polynomial $h(x)$ already has coefficients in M, so f cannot remain irreducible in $M[x]$. Therefore f *must* split over M, which is equivalent to the statement that f is reducible over M.

Converse. If f is reducible over $M = \mathbb{Q}(\sqrt{D_f})$ but irreducible over $\mathbb{Q}$, then the Galois group of f cannot act transitively over M, so it must be contained in a cyclic group of order 4. Under the hypotheses above on the resolvent, this forces $G_f \simeq C_4$.

3 Inductive Lattice Construction Conjecture

3.1 The Vanishing

While using the Sage code, one might have noticed that certain polynomials for ζ_n where n is not prime, have coefficients that are all 0. We will go through this for ζ_{81} and ζ_{54}. This is certainly unusual since when working with ζ_p where p is a prime, the polynomials are irreducible, so why are we getting period polynomials of the form

$$x^d + 0x^{d-1} + ... + 0 = x^d$$

The answer can be quite complicated, so we will first illustrate with some examples, highlighting the patterns that occur.

Using subfields of ζ_{81} as examples

The divisors with vanishing coefficients are

$$d = 2, 6, 9, 18$$

So we will compute the polynomials by hand and see what happens. Also, note that

$$\Phi_{81}(t) = t^{54} + t^{27} + 1$$

d=2: using our usual methodology for computing cosets, we get

$$A = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67, 70, 73, 76, 79\}$$

$$B = \{2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 56, 59, 62, 65, 68, 71, 74, 77, 80\}$$

Then our polynomial is

$$A = x - t^1 - t^4 - t^7 - t^{10} - t^{13} - t^{16} - t^{19} - t^{22} - t^{25} - t^{28} - t^{31} - t^{34} - t^{37} - t^{40} -$$
$$-t^{43} - t^{46} - t^{49} - t^{52} - t^{55} - t^{58} - t^{61} - t^{64} - t^{67} - t^{70} - t^{73} - t^{76} - t^{79}$$

$$B = x - t^2 - t^5 - t^8 - t^{11} - t^{14} - t^{17} - t^{20} - t^{23} - t^{26} - t^{29} - t^{32} - t^{35} - t^{38} - t^{41} -$$
$$-t^{44} - t^{47} - t^{50} - t^{53} - t^{56} - t^{59} - t^{62} - t^{65} - t^{68} - t^{71} - t^{74} - t^{77} - t^{80}$$

To understand what is happening, we reorganize the exponents in each coset using the shape of the cyclotomic polynomial

$$\Phi_{81}(t) = t^{54} + t^{27} + 1.$$

The exponents that appear here are $0, 27, 54$, which are all congruent modulo 27. More generally, for any integer a we have

$$t^a + t^{a+27} + t^{a+54} = t^a\big(1 + t^{27} + t^{54}\big),$$

and the three exponents $a, a+27, a+54$ are precisely the elements of a single equivalence class modulo 27 in $\mathbb{Z}/81\mathbb{Z}$.
Define an equivalence relation on $\mathbb{Z}/81\mathbb{Z}$ where each equivalence class has exactly three elements, of the form $\{a, a+27, a+54\}$. We now intersect the cosets A and B with these equivalence classes and group the exponents accordingly. This produces the partitions

$$\begin{aligned} A = &\{1,28,55\},\ \{4,31,58\},\ \{7,34,61\},\ \{10,37,64\},\ \{13,40,67\},\\ &\{16,43,70\},\ \{19,46,73\},\ \{22,49,76\},\ \{25,52,79\},\\ B = &\{2,29,56\},\ \{5,32,59\},\ \{8,35,62\},\ \{11,38,65\},\ \{14,41,68\},\\ &\{17,44,71\},\ \{20,47,74\},\ \{23,50,77\},\ \{26,53,80\}. \end{aligned}$$

In each triple $\{a, a+27, a+54\}$ we will later factor the corresponding sum $t^a + t^{a+27} + t^{a+54}$ as $t^a(1+t^{27}+t^{54})$, which is what ultimately leads to the vanishing of all non-leading coefficients after reduction modulo $\Phi_{81}(t)$.
Then rewriting in terms of t again but factoring out the power of t according to the congruence (i.e. if they are congruent modulo 3 then factor out t^3) we get:

$$\begin{aligned} A = x - t(1+t^{27}+t^{54}) - t^4(1+t^{27}+t^{54}) - t^7(1+t^{27}+t^{54}) - t^{10}(1+t^{27}+t^{54}) -\\ -t^{13}(1+t^{27}+t^{54}) - t^{16}(1+t^{27}+t^{54}) - t^{19}(1+t^{27}+t^{54}) - t^{22}(1+t^{27}+t^{54}) - t^{25}(1+t^{27}+t^{54}) \end{aligned}$$

$$\begin{aligned} B = x - t^2(1+t^{27}+t^{54}) - t^5(1+t^{27}+t^{54}) - t^8(1+t^{27}+t^{54}) - t^{11}(1+t^{27}+t^{54}) - t^{14}(1+t^{27}+t^{54}) -\\ -t^{17}(1+t^{27}+t^{54}) - t^{20}(1+t^{27}+t^{54}) - t^{23}(1+t^{27}+t^{54}) - t^{26}(1+t^{27}+t^{54}) \end{aligned}$$

We see that when we do this method of rearranging, we see that $\Phi_{81}(t)$ is in every term besides the leading x. This means that when we continue our process and reduce the polynomial modulo $\Phi_{81}(t)$, every term will be $\equiv 0 \mod \Phi_{81}(t)$ except x. Therefore, our final polynomial will be

$$f_2(x) = x^2$$

d=6: Cosets are

$$\begin{aligned} A &= \{1,10,19,28,37,46,55,64,73\}, \quad B = \{2,11,20,29,38,47,56,65,74\}\\ C &= \{4,13,22,31,40,49,58,67,76\}, \quad D = \{5,14,23,32,41,50,59,68,77\}\\ E &= \{7,16,25,34,43,52,61,70,79\} \quad F = \{8,17,26,35,44,53,62,71,80\} \end{aligned}$$

Split into partitions

$$\begin{aligned} A &= \{1,28,55\},\{10,37,64\},\{19,46,73\} \quad B = \{2,29,56\},\{11,38,65\},\{20,47,74\}\\ C &= \{4,31,58\},\{13,40,67\},\{22,49,76\} \quad D = \{5,32,59\},\{14,41,68\},\{23,50,77\}\\ E &= \{7,34,61\},\{16,43,70\},\{25,52,79\} \quad F = \{8,35,62\},\{17,44,71\},\{26,53,80\} \end{aligned}$$

Grouping polynomials again, we get

$$A : x - t(1 + t^{27} + t^{54}) - t^{10}(1 + t^{27} + t^{54}) - t^{19}(1 + t^{27} + t^{54})$$
$$B : x - t^{2}(1 + t^{27} + t^{54}) - t^{11}(1 + t^{27} + t^{54}) - t^{20}(1 + t^{27} + t^{54})$$
$$C : x - t^{4}(1 + t^{27} + t^{54}) - t^{13}(1 + t^{27} + t^{54}) - t^{22}(1 + t^{27} + t^{54})$$
$$D : x - t^{5}(1 + t^{27} + t^{54}) - t^{14}(1 + t^{27} + t^{54}) - t^{23}(1 + t^{27} + t^{54})$$
$$E : x - t^{7}(1 + t^{27} + t^{54}) - t^{16}(1 + t^{27} + t^{54}) - t^{25}(1 + t^{27} + t^{54})$$
$$F : x - t^{8}(1 + t^{27} + t^{54}) - t^{17}(1 + t^{27} + t^{54}) - t^{26}(1 + t^{27} + t^{54})$$

Again, we see that every term except x will get reduced to 0 modulo Φ, so the polynomial will just be

$$f_6(x) = x^6$$

d=9: Cosets are

$$A = \{1, 26, 28, 53, 55, 80\}, B = \{2, 25, 29, 52, 56, 79\}, C = \{4, 23, 31, 50, 58, 77\}$$
$$D = \{5, 22, 32, 49, 59, 76\}, E = \{7, 20, 34, 47, 61, 74\}, F = \{8, 19, 35, 46, 62, 73\}$$
$$G = \{10, 17, 37, 44, 64, 71\}, H = \{11, 16, 38, 43, 65, 70\}, I = \{13, 14, 40, 41, 67, 68\}$$

Split into partitions

$$A = \{1, 28, 55\}, \{26, 53, 80\} \quad B = \{2, 29, 56\}, \{25, 52, 79\} \quad C = \{4, 31, 58\}, \{23, 50, 77\}$$
$$D = \{5, 32, 59\}, \{22, 49, 76\} \quad E = \{7, 34, 61\}, \{20, 47, 74\} \quad F = \{8, 35, 62\}, \{19, 46, 73\}$$
$$G = \{10, 37, 64\}, \{17, 44, 71\} \quad H = \{11, 38, 65\}, \{16, 43, 70\} \quad I = \{13, 40, 67\}, \{14, 41, 68\}$$

Grouping polynomials

$$A : x - t(1 + t^{27} + t^{54}) - t^{26}(1 + t^{27} + t^{54}) \quad B : x - t^{2}(1 + t^{27} + t^{54}) - t^{25}(1 + t^{27} + t^{54})$$
$$C : x - t^{4}(1 + t^{27} + t^{54}) - t^{23}(1 + t^{27} + t^{54}) \quad D : x - t^{5}(1 + t^{27} + t^{54}) - t^{22}(1 + t^{27} + t^{54})$$
$$E : x - t^{7}(1 + t^{27} + t^{54}) - t^{20}(1 + t^{27} + t^{54}) \quad F : x - t^{8}(1 + t^{27} + t^{54}) - t^{19}(1 + t^{27} + t^{54})$$
$$G : x - t^{10}(1 + t^{27} + t^{54}) - t^{17}(1 + t^{27} + t^{54}) \quad H : x - t^{11}(1 + t^{27} + t^{54}) - t^{16}(1 + t^{27} + t^{54})$$
$$I : x - t^{13}(1 + t^{27} + t^{54}) - t^{14}(1 + t^{27} + t^{54})$$

Which then means

$$f_9(x) = x^9$$

d=18: Cosets are

$$\{1, 28, 55\}, \{2, 29, 56\}, \{4, 31, 58\}, \{5, 32, 59\}, \{7, 34, 61\}, \{8, 35, 62\}$$

$$\{10, 37, 64\}, \{11, 38, 65\}, \{13, 40, 67\}\{14, 41, 68\}, \{16, 43, 70\}, \{17, 44, 71\}$$
$$\{19, 46, 73\}, \{20, 47, 74\}, \{22, 49, 76\}, \{23, 50, 77\}, \{25, 52, 79\}, \{26, 53, 80\}$$

These are already partitioned in the way we need (reader can check this fact), so the polynomial will then become

$$f_{18}(x) = x^{18}$$

It turns out that the Gauss sums method results in not linearly independent ζ sums, which causes the coefficients to vanish when reduced by Φ_n. So, it is imperative that we try to find a different construction at least where $n = p^r$ (some power of a prime).

3.2 Inductive Construction

In the previous section we observed a vanishing phenomenon when constructing periods for $\mathbb{Q}(\zeta_n)$ in the prime case $n = p$. When $n = p^r$ is a prime power, we would like to extend the same construction. To do this, we must work with the multiplicative groups

$$(\mathbb{Z}/p\mathbb{Z})^\times, \qquad (\mathbb{Z}/p^2\mathbb{Z})^\times, \qquad \dots \qquad (\mathbb{Z}/p^r\mathbb{Z})^\times,$$

and in particular we need a generator that lifts from level p to all higher powers of p.
The following classical result provides exactly what we need.

Lemma: Lifting of primitive roots; cf. Ireland–Rosen, Theorem 2.5 Let p be an odd prime. Suppose g is a primitive root modulo p and satisfies

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Then g is a primitive root modulo p^k for every $k \geq 1$. In particular, g generates both $(\mathbb{Z}/p\mathbb{Z})^\times$ and $(\mathbb{Z}/p^k\mathbb{Z})^\times$ simultaneously.
proof: Let g generate $(\mathbb{Z}/p\mathbb{Z})^\times$. From the binomial theorem we know

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2},$$

we have $(g+p)^{p-1} \not\equiv g^{p-1} \pmod{p^2}$, so

$$g^{p-1} \not\equiv 1 \pmod{p^2} \quad \text{or} \quad (g+p)^{p-1} \not\equiv 1 \pmod{p^2}.$$

Assume $g^{p-1} \not\equiv 1 \pmod{p^2}$, since that would mean g has an order less than $\phi(p^2) = p(p-1)$. Then

$$g^{p-1} \equiv 1 + k_1 p, \quad p \nmid k_1.$$

Using the binomial theorem once again we get,

$$\begin{aligned} g^{p(p-1)} =& \equiv (1+k_1p)^p \equiv 1 + pk_1p + \sum_{j=2}^{p-1} \binom{p}{j} k_1^j p^j + k_1^p p^p \\ &\equiv 1 + k_2 p^2, \quad p \nmid k_2. \end{aligned}$$

The last equality comes from the fact that the terms in the sum and the term $k_1^p p^p$ are multiples of p^3.
Then we can do it again and get

$$g^{p^2(p-1)} \equiv 1 + k_3 p^3, \quad p \nmid k_3,$$

because terms are multiples of p^4
Then we can keep repeating up to

$$g^{p^{r-2}(p-1)} \equiv 1 + k_{r-1} p^{r-1}, \quad p \nmid k_{r-1}.$$

So,

$$g^{p^{r-2}(p-1)} \not\equiv 1 \pmod{p^r}.$$

We know that the order so g must divide $p^{r-1}(p-1)$. So suppose for a contradiction that the order of g is of the form p^{r-d} with $d > 1$ and $d|p-1$. By Fermat's Little Theorem, we know

$$g^{p^r d} \equiv 1 \mod p^r \Rightarrow g^d \equiv 1 \mod p$$

However, this means that the order of g would divide d, which contradicts the initial assumption that g is a generator for $(\mathbb{Z}/p\mathbb{Z})^\times$. the order of g in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ takes the form $p^{r-1}(p-1)$ where $e \leq r-1$.

Definition Let p be an odd prime and $r \geq 1$. Set $\zeta_{p^r} = e^{2\pi i/p^r}$ and

$$K_r = \mathbb{Q}(\zeta_{p^r}).$$

Then $K_r/\mathbb{Q}$ is Galois with

$$\mathrm{Gal}(K_r/\mathbb{Q}) \cong (\mathbb{Z}/p^r\mathbb{Z})^\times,$$

a cyclic group of order $\varphi(p^r) = p^{r-1}(p-1)$.

Note Fix g as in the Lemma. Then $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^i})/\mathbb{Q}(\zeta_{p^{i-1}}))$ is generated by $g^{p^{i-2}(p-1)}$.

3.3 Conjecture Statement

Inductive construction of subfield generators for $n = p^r$.
Let p be an odd prime and $n = p^r$. For every intermediate field F with $\mathbb{Q} \subseteq F \simeq \mathbb{Q}(\zeta_{p^r})$ corresponding to a subgroup $H \leq (\mathbb{Z}/p^r\mathbb{Z})^\times$, there exists an explicit generator G_H (ex. a rational linear combination of roots of unity) such that:

(a) **Base step:** For $r = 1$ (i.e. $n = p$), generators G_H are given by Gaussian periods / period-polynomial constructions determined by the cosets of H in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) **Inductive step:** Suppose generators $G_{H'}$ are fixed for all subfields of $\mathbb{Q}(\zeta_{p^r})$. For each subgroup $H \leq (\mathbb{Z}/p^{r+1}\mathbb{Z})^\times$, choose coset representatives lifting those used at level r (via the natural reduction $(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \to (\mathbb{Z}/p^r\mathbb{Z})^\times$). Then a generator G_H for the corresponding subfield of $\mathbb{Q}(\zeta_{p^{r+1}})$ can be constructed by the *same* period-polynomial rule applied to these lifted cosets. In other words, for those subfields that already existed in $\mathbb{Q}(\zeta_{p^r})$, their generators and corresponding polynomials do not change when viewed inside $\mathbb{Q}(\zeta_{p^{r+1}})$.

(c) **New subfields appearing at level $r+1$.** The group $(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times$ contains strictly more subgroups than $(\mathbb{Z}/p^r\mathbb{Z})^\times$, and therefore $\mathbb{Q}(\zeta_{p^{r+1}})$ contains subfields that do not occur at level r. For any such "new subgroup $H \leq (\mathbb{Z}/p^{r+1}\mathbb{Z})^\times$ whose image under the reduction map

$$(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times$$

is *not* a subgroup of the latter, one obtains a genuinely new intermediate field of $\mathbb{Q}(\zeta_{p^{r+1}})$.

For these new subfields, we conjecture the existence of a polynomial

$$f_p(x) \in \mathbb{Q}[x],$$

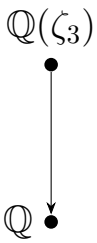
depending only on the prime p, such that the minimal polynomials of their generators can be constructed uniformly from $f_p(x)$ by applying the same period polynomial or Chebyshev-type transformations used in the base case $r = 1$.

In other words, once a generator at level p is known, the minimal polynomials of generators for *all* new subfields at each higher level p^{r+1} can be obtained via a fixed transformation rule involving $f_p(x)$.

3.4 Examples

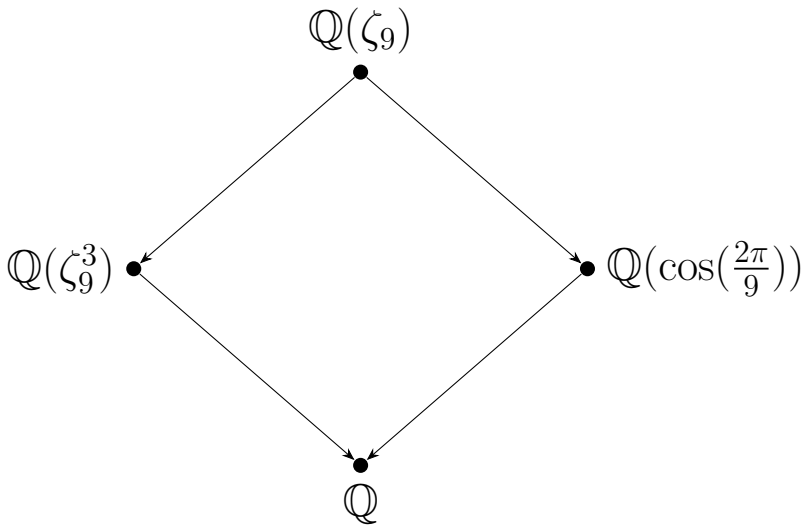
This will become clear with an example. So take $p = 3$ and lets describe the lattice structure for the following fields $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\zeta_{3^2})$, $\mathbb{Q}(\zeta_{3^3})$, $\mathbb{Q}(\zeta_{3^4})$.
We begin by describing the lattice structure of $\mathbb{Q}(\zeta_3)$

Subfield lattice of ζ_3, a cyclic group of order 2



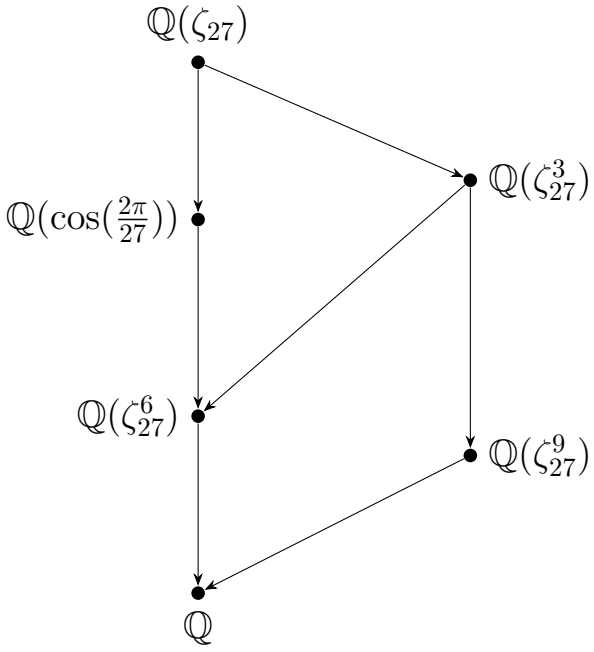
The only generator we need here is the one for $\mathbb{Q}(\zeta_3)$, since this is just the cyclotomic extenstion, we always know this polyonomial. In this case, it's $x^2 + x + 1$.
Next, we will give the lattice for $\mathbb{Q}(\zeta_9)$

Subgroup lattice of ζ_9



We already know one of the field extensions, $\mathbb{Q}(\zeta_9^3)$ from our previous construction. So we need to compute $\mathbb{Q}(\zeta_9^2)$ as well as $\mathbb{Q}(\zeta_9)$. the latter is simply the cyclotomic field, so we can easily get the generator $x^6 + x^3 + 1$. Then since $\mathbb{Q}(\zeta_9^2)$ is an $\frac{\phi(n)}{2}$ extension, we can use the method we previously described, which ends up being $x^3 - 3x + 1$.
Next, we compute $\mathbb{Q}(\zeta_{3^3})$

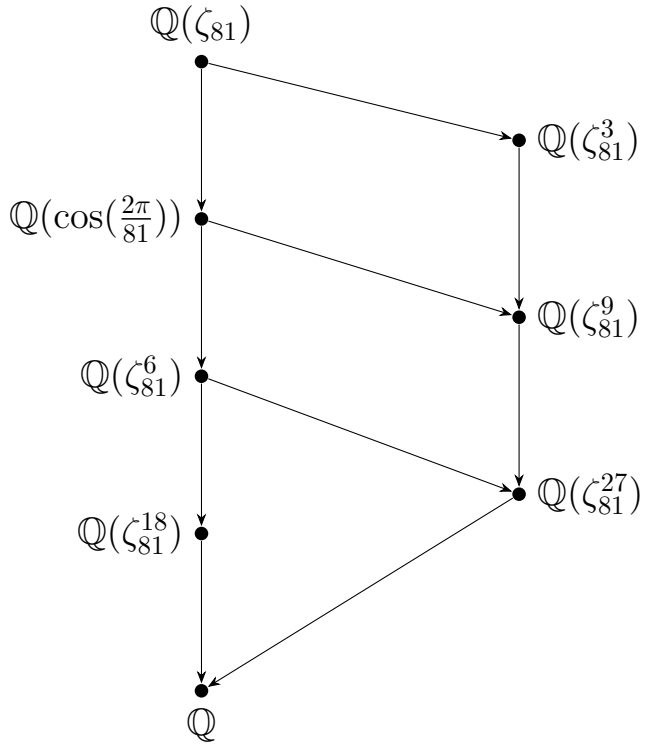
Subgroup lattice of $\mathbb{Q}(\zeta_{27})$



Again, we have two new fields $\mathbb{Q}(\zeta_{27}^2)$ and $\mathbb{Q}(\zeta_{27})$. Again, the latter is a cyclotomic field so the corresponding polynomial is $x^{18} + x^9 + 1$. Then we can use the same method as above to compute the generator for $\mathbb{Q}(\zeta_{27}^2)$, which ends up being $x^9 - 9x^7 + 27x^5 - 30x^3 + 9x + 1$

Then recall the lattice for $\mathbb{Q}(\zeta_{3^4})$

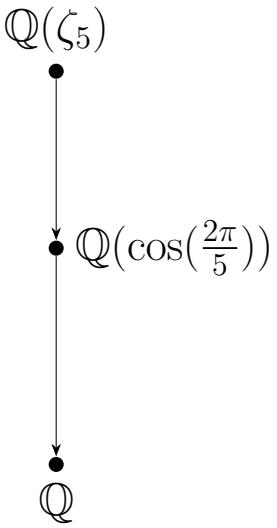
Subfield lattice of ζ_{81}, a cyclic group of order 54



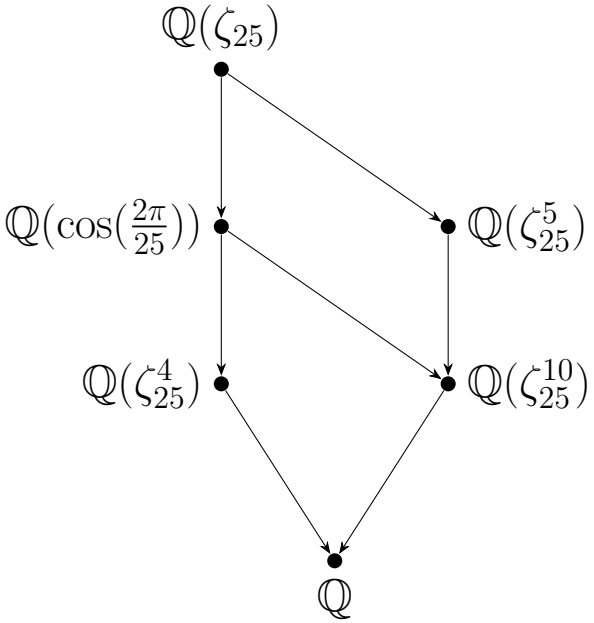
Here, we add the fields $\mathbb{Q}(\zeta_{81})$, $\mathbb{Q}(\zeta_{81}^2)$. Once again, for the cyclotomic, we have the generator $x^{54}+x^{27}+1$. Then for the degree $\phi(n)/2$ field, we get the generator
$x^{27}-27x^{25}+324x^{23}-2277x^{21}+10395x^{19}-32319x^{17}+69768x^{15}-104652x^{13}+107406x^{11}-72930x^9+30888x^7-7371x^5+819x^3-27x+1$
Now that we have an idea of what the inductive construction can look like for $p=3$, we can look at other primes.

Now take $p = 5$. We will only look at $n = 5$ and $n = 5^2$.

Subgroup lattice of ζ_5



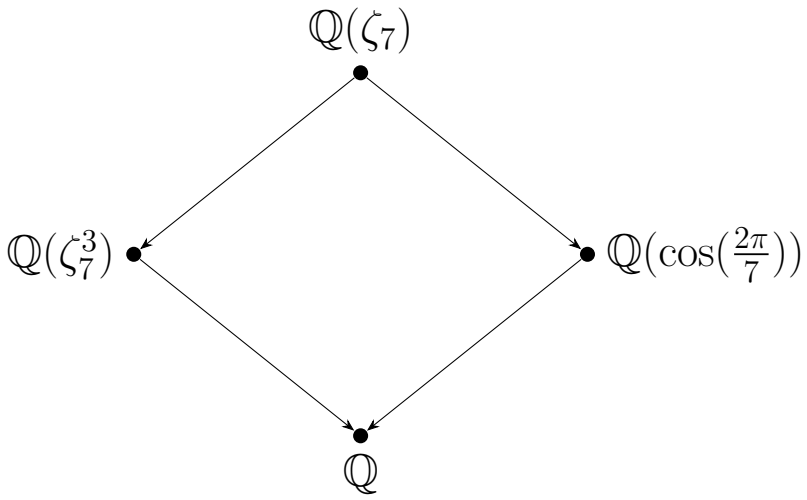
Subgroup lattice of ζ_{25}



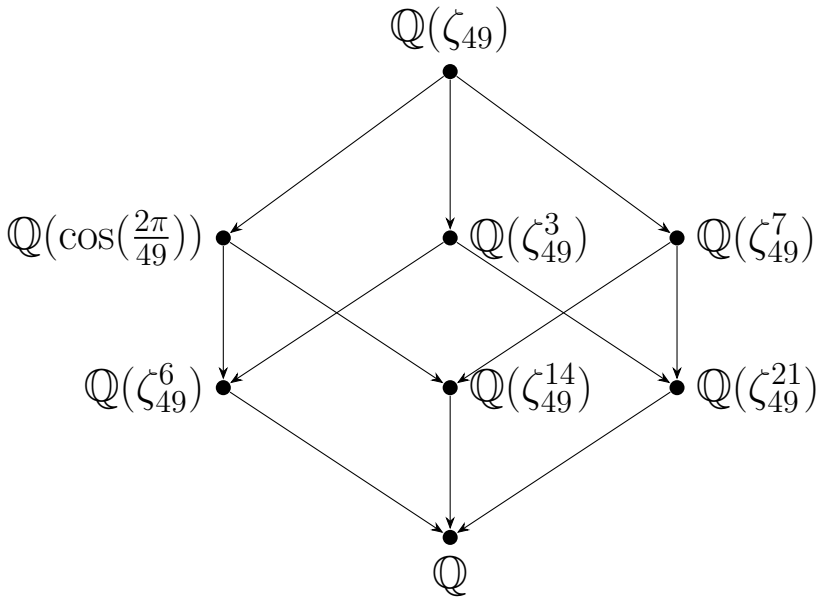
We have three new fields for the lattice of $\mathbb{Q}(\zeta_{25})$. As before, one of them is the big cyclotomic field which has a formula $x^{20}+x^{15}+x^{10}+x^5+1$. Next, we can compute $\mathbb{Q}(\zeta_{25}^2)$ in the same way as above and we get $x^{10}-10x^8+35x^6+x^5-50x^4-5x^3+25x^2+5x-1$. However, we still have one more field $\mathbb{Q}(\zeta_{25}^4)$ which has degree 5 over $\mathbb{Q}$. Interestingly, it seems we can use our Gauss sums method to compute its polynomial without vanishing. We get that the generator is $x^5-10x^3+5x^2+10x+1$.

Next, we will do this for for the prime $p = 7$ in the cases that $n = 7$ and $n = 7^2$.

Subgroup lattice of ζ_7



Subgroup lattice of $\mathbb{Q}(\zeta_{49})$



We have four new fields to analyze. First, the big cyclomtoic is $\mathbb{Q}(\zeta_{49})$ and has generator $x^{42} + x^{35} + x^{28} + x^{21} + x^{14} + x^7 + 1$. Next, $\mathbb{Q}(\zeta_{49}^2)$, and using the same method, we get the generator

$$x^{21} - 21x^{19} + 189x^{17} - 952x^{15} + x^{14} + 2940x^{13} - 14x^{12} - 5733x^{11} + 77x^{10}$$

$$+7007x^9 - 210x^8 - 5147x^7 + 294x^6 + 2072x^5 - 196x^4 - 371x^3 + 49x^2 + 14x - 1$$

Next, we will look at the field $\mathbb{Q}(\zeta_{49}^3)$ which has degree 14 over $\mathbb{Q}$. It appears it also doesn't vanish using the Gauss sums method and we get $x^{14} - 28x^{11} + 7x^{10} + 14x^9 + 189x^8 - 90x^7 - 98x^6 - 196x^5 + 427x^4 - 217x^3 - 140x^2 + 11x + 79$ as the generator. Lastly we need to look at $\mathbb{Q}(\zeta_{49}^6)$ with degree 7 over $\mathbb{Q}$. Its corresponding generator is $x^7 - 21x^5 - 21x^4 + 91x^3 + 112x^2 - 84x - 97$.

3.5 Proof Sketch

It might be early to conclude, but it seems like with every new power of p, we will be able to find a generator for every field in our subfield lattice, which means the inductive construction will allow us to obtain all of the generators of subfields of $\mathbb{Q}(\zeta_{p^r})$.

Idea for proof of Conjecture 3.3a:
The idea for this proof comes from Section I.

Idea for proof of Conjecture 3.3b:
Assume that for all subfields of $K_r = \mathbb{Q}(\zeta_{p^r})$ corresponding to subgroups $H' \leq (\mathbb{Z}/p^r\mathbb{Z})^\times$, we have fixed explicit generators $G_{H'}$ constructed via Gaussian periods (or rational linear combinations of roots of unity) determined by their coset decompositions in $(\mathbb{Z}/p^r\mathbb{Z})^\times$.
Consider the natural reduction map

$$\pi : (\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times, \quad k \mapsto k \bmod p^r,$$

which is surjective, with kernel

$$\ker(\pi) = 1 + p^r\mathbb{Z}/p^{r+1}\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}.$$

Via the isomorphism

$$\mathrm{Gal}(K_m/\mathbb{Q}) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$$

this map π corresponds to restriction of automorphisms

$$\mathrm{Gal}(K_{r+1}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K_r/\mathbb{Q})$$

Given a subgroup $H' \leq (\mathbb{Z}/p^r\mathbb{Z})^\times$, its inverse image

$$H := \pi^{-1}(H') \leq (\mathbb{Z}/p^{r+1}\mathbb{Z})^\times$$

corresponds to the same subfield $K_r^{H'}$ now viewed inside K_{r+1}. In particular,

$$K_{r+1}^{H} = K_r^{H'}.$$

Let

$$(\mathbb{Z}/p^r\mathbb{Z})^\times = C_1' \sqcup \cdots \sqcup C_d'$$

be the coset decomposition of H' in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ used to define $G_{H'}$. Lift each coset C_j' to a coset

$$C_j = \pi^{-1}(C_j') \subset (\mathbb{Z}/p^{r+1}\mathbb{Z})^\times,$$

and choose representatives $a \in C_j$ satisfying $a \equiv a' \pmod{p^r}$ for each $a' \in C_j'$.
Then from our explicit construction we have,

$$G_H = \sum_{a \in C_1} \zeta_{p^{r+1}}^a,$$

constructed by the same rule as in level r, but using the lifted cosets C_j.
Since the elements of $(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times$ act by multiplication on exponents, the stabilizer of G_H is precisely H, and therefore

$$\mathbb{Q}(G_H) = K_{r+1}^H = K_r^{H'} = \mathbb{Q}(G_{H'}).$$

Thus the subfield and its minimal polynomial do not change when passing from level r to $r+1$; the inductive construction simply recovers the same generator inside the larger cyclotomic field.

Idea for proof of Conjecture 3.3c: For $n = p^r$ where p is an odd prime, the n-th cyclotomic polynomial has the form

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}.$$

Thus, $\Phi_{p^r}(x)$ is a geometric series with exactly p nonzero terms, all with coefficient $+1$.
The length of the coset is $\phi(n)/d$ so if length is greater than $\phi(n)/d$ cosets won't vanish. So we want

$$p > \phi(n)/d \;\Rightarrow\; p > \frac{(p-1)p^{r-1}}{d} \;\Rightarrow\; d > (p-1)p^{r-2}$$

where $p > 2$ and $r > 2$
Now we will create a lower bound for the degree of the extension for the "new fields" when we go from $\mathbb{Q}(\zeta_{p^{r-1}})$ to $\mathbb{Q}(\zeta_{p^r})$.
For $\mathbb{Q}(\zeta_{p^{r-1}})$, the maximum degree over $\mathbb{Q}$ is

$$|\mathbb{Z}/p^{r-1}\mathbb{Z}|$$

So when we construct subfields of $\mathbb{Q}(\zeta_{p^r})$ from those of $\mathbb{Q}(\zeta_{p^{r-1}})$, the degree of extension over $\mathbb{Q}$ *must* be greater than the maximum degree of $\mathbb{Q}(\zeta_{p^{r-1}})$, i.e. greater than $|\mathbb{Z}/p^{r-1}\mathbb{Z}|$ which equals

$$(p-1)p^{r-2}$$

This is exactly what we wanted in terms of a bound. In other words, the degree of the extension for all "new fields" is great enough to allow us to always use Gauss sums to construct the period polynomials.

4 Coefficient Conjecture

4.1 Coefficient Generation Approach

In this section, we explain how the large coefficient dataset used in our visualizations was produced. For a fixed divisor d of $p-1$, the period polynomial associated to $\mathbb{Q}(\zeta_p)$ and the subgroup $H_d \subset (\mathbb{Z}/p\mathbb{Z})^\times$ has degree d and can be written in the form

$$P_{p,d}(x) = x^d + a_{d-1}(p)x^{d-1} + \cdots + a_1(p)x + a_0(p).$$

Thus for each prime p we obtain a family of coefficients $\{a_i(p)\}_{i=0}^{d-1}$. Our goal is to study how these coefficients vary as the prime p changes.

The data-generation routine proceeds as follows:

1. **Fix a divisor d of $p-1$.** Using Sage, we run the script Looped Polynomial, which constructs the degree-d period polynomial $P_{p,d}(x)$ for the first 1000 primes with $d \mid (p-1)$.
2. **Export the coefficients.** For each such prime, Sage outputs the vector of coefficients $(a_{d-1}(p), \ldots, a_0(p))$, which we save as a `.csv` file.
3. **Visualization.** In Colab we load the data and, for a fixed index i, we plot

$$p \longmapsto a_i(p)$$

using Altair and Pandas. The horizontal axis is the prime p, and the vertical axis shows the value of the coefficient $a_i(p)$.
4. **Pattern detection.** Each chart displays the behavior of a single coefficient family $a_i(p)$ as p varies, allowing us to identify congruence-dependent patterns and other regularities.

Note: The polynomials are monic, so the leading coefficient is always 1. Therefore our visualizations focus on the remaining coefficients, which vary nontrivially with the prime p.

4.2 Examples

Note: The first two leading coefficients are always equal to 1, so the visualizations will focus on coefficients that are not always the same.

d=2:

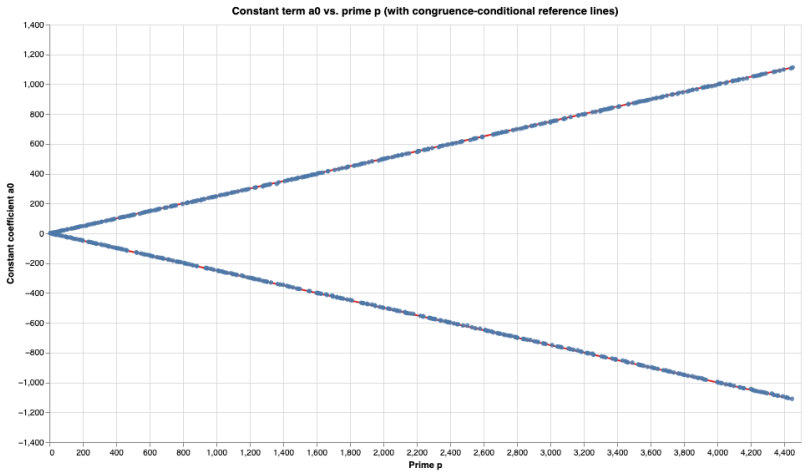


Figure 1: a_0 coefficient of degree 2 period polyonmials

From Gauss, the coefficients are of the form

$$a_0(p) = \begin{cases} \frac{p+1}{4}, & \text{if } p \equiv 3 \mod 4, \\ \frac{1-p}{4}, & \text{if } p \equiv 1 \mod 4. \end{cases}$$

One can observe that this coefficient is a linear function depending on the prime, which will become a clearer pattern as we move forward.

d = 3:

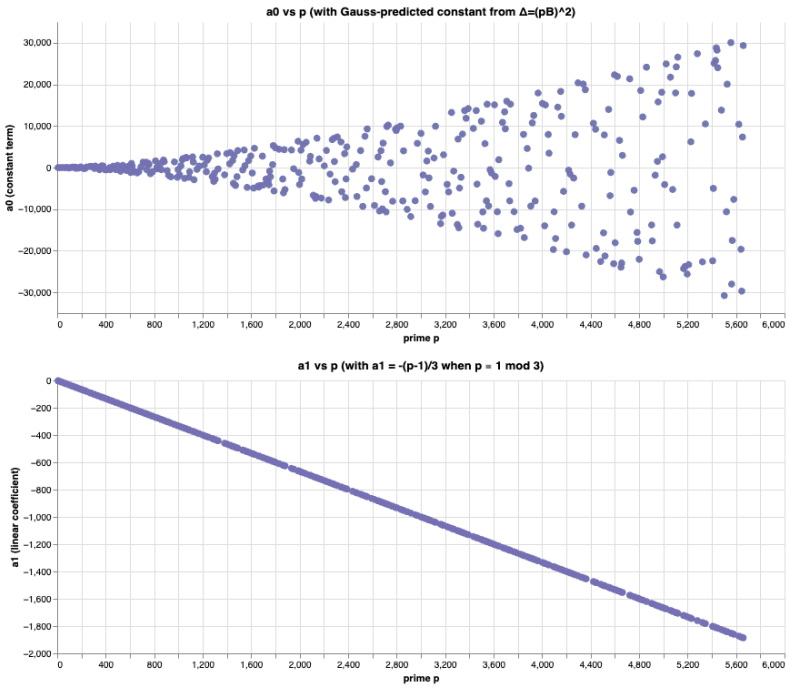


Figure 2: a_0 (top) and a_1 (bottom) coefficients of degree 3 period polynomials

For the case $d = 3$, the behavior of the coefficients is particularly well understood thanks to a classical theorem of Gauss. In his analysis of cubic Gauss sums, Gauss proved exact closed-form expressions for all of the coefficients of the degree3 period polynomial. In particular, when $p \equiv 1 \pmod 3$, the linear coefficient is given by

$$a_1(p) = -\frac{p-1}{3}.$$

Thus the coefficient a_1 is not merely observed to be linear in our data, but is known a priori to be exactly linear by Gauss's theorem.
Our plot of $a_1(p)$ versus p is included not to discover this formula, but to provide a numerical verification that the Sage computations reproduce Gauss's theoretically predicted values. The perfect alignment of the plotted points along the line confirms that our computational pipeline is consistent with the classical theory. For our purposes we simply restated the formula for the coefficient that behaves linearly (a_1) to verify the computation.
d=4:

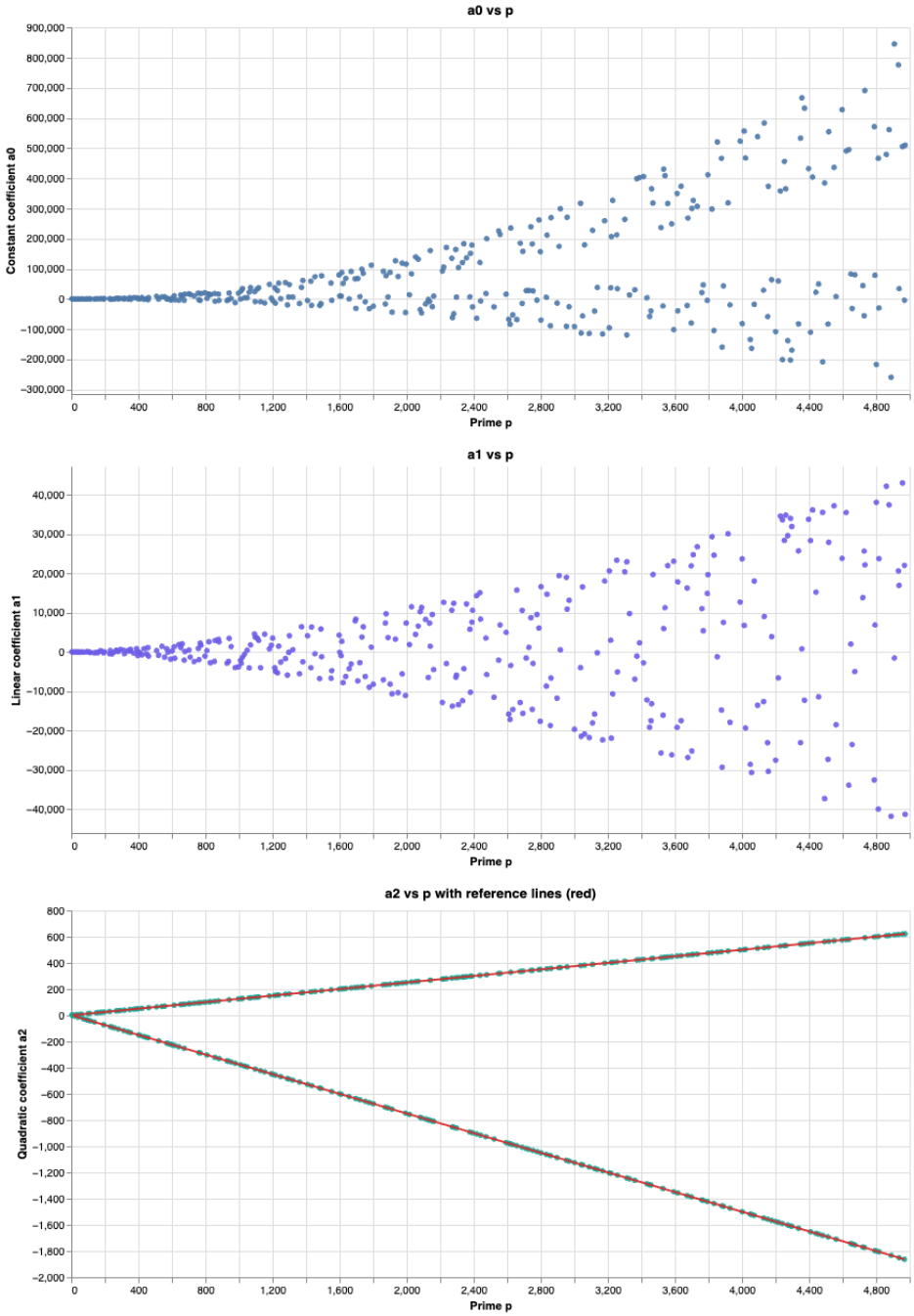


Figure 3: a_0 (top) and a_1 (middle) and a_2 (bottom) coefficients of degree 4 period polynomials

Again, we will focus on the coefficient behaving linearly. From Figure 3 (bottom), we have that the a_2 coefficient depends on the prime p in the following way

$$a_2(p) = \begin{cases} \dfrac{(3-3p)}{8}, & p \equiv 1 \mod 8 \\ \dfrac{3+p}{8}, & p \equiv 5 \mod 8 \end{cases}$$

d=5:
Here, I will only include the visualization for the coefficient $a_3(p)$.

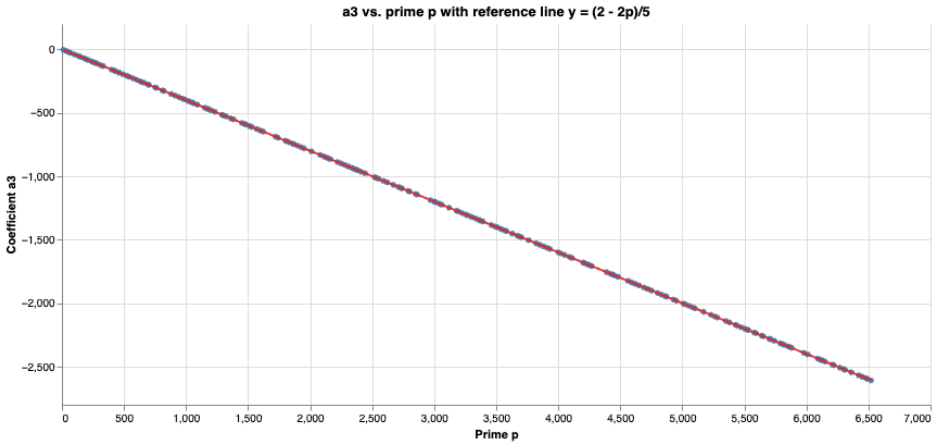


Figure 4: a_3 coefficients of degree 5 period polynomials

To identify a possible closed form for the coefficient $a_3(p)$, we plotted the computed values of a_3 for the first 1000 primes satisfying $p \equiv 1 \pmod 5$. The resulting scatterplot showed the points lying almost perfectly on the line $y = (2-2p)/5$, and by overlaying this reference line in the visualization, we verified that the Sage-generated coefficients agree exactly with the following linear formula:

$$a_3(p) = \frac{2-2p}{5}$$

This process was repeated for degree $6, 7, 8, 9, 16$ and similar patterns with the linearly behaving coefficients appeared, which allows us to make a potential conjecture.

4.3 Conjecture Statement

Motivation and Evidence for the Conjecture. This conjecture arose from a large-scale computational experiment carried out for first 1000 primes and all divisors $d \mid (p-1)$. For each such pair (p, d), we computed the degree-d period polynomial

$$P_{p,d}(x) = x^d + a_{d-1}(p)x^{d-1} + a_{d-2}(p)x^{d-2} + \cdots + a_0(p)$$

using the Sage routine described earlier. When the resulting families of coefficients were plotted as functions of p (using Altair/Pandas visualizations), a striking pattern emerged: *among all the coefficients, the first nontrivial term $a_{d-2}(p)$ always lay exactly on a straight line.*

More precisely, for fixed d, the points $\{(p, a_{d-2}(p))\}$ fall onto one of two linear functions of p, with the choice of branch determined solely by the residue class of p modulo $2d$. This behavior is visible even for small d (e.g. $d = 3$ and $d = 5$), where the graphs of $a_1(p)$ and $a_3(p)$ line up perfectly with the known theoretical formulas, such as

$$a_1(p) = -\frac{p-1}{3} \qquad \text{for } d = 3, \quad a_3(p) = \frac{2-2p}{5} \qquad \text{for } d = 5.$$

For larger d, where no closed formulas are known, the same linearity persists without exception in the entire computed dataset.
Based on this numerical evidence, we conjecture that the first nontrivial coefficient $a_{d-2}(p)$ is a linear function of p whose slope and intercept depend only on d and on the congruence class of p modulo $2d$. The explicit expressions written above are exactly the two linear branches that fit all observed data.

Line Equation Compution
Naive Approach
In many cases the plots strongly suggested that the coefficient $a_{d-2}(p)$ is not merely approximately linear in p, but in fact *exactly* linear . To verify this, I used a direct algebraic method to recover the linear formula from the data without appealing to statistical regression.
The values $a_{d-2}(p)$ for different primes were observed to lie on a perfect straight line. Therefore, any two data points $(p_1, a_{d-2}(p_1))$ and $(p_2, a_{d-2}(p_2))$ in that class determine the line exactly. The slope is computed by the elementary difference quotient

$$m = \frac{a_{d-2}(p_2) - a_{d-2}(p_1)}{p_2 - p_1},$$

and substituting either point yields the intercept

$$b = a_{d-2}(p_1) - m\, p_1.$$

Because the data lies exactly on a line (not merely approximately), this two point extraction recovers the true closed formula for $a_{d-2}(p)$ on each residue class.

Rigorous Approach:
This is the method I will utilize in the future.
For each fixed divisor d and each residue class $r \pmod{2d}$, we can collect all data points $(p, a_{d-2}(p))$. Given such a set of points (p_i, a_i), we can compute the leastsquares line

$$y = m_r p + b_r$$

by minimizing $\sum_i (a_i - (mp_i + b))^2$. The closed form expressions

$$m_r = \frac{n\sum_i p_i a_i - (\sum_i p_i)(\sum_i a_i)}{n\sum_i p_i^2 - (\sum_i p_i)^2}, \qquad b_r = \frac{1}{n}\Big(\sum_i a_i - m_r \sum_i p_i\Big),$$

will be evaluated numerically in Python (via `numpy.polyfit`) and the resulting slopes and intercepts will then be simplified to rational numbers. In every case, the data points will still lay exactly on the corresponding line $y = m_r p + b_r$, yielding our formulas and more generally the piecewise linear expressions for $a_{d-2}(p)$ stated in the conjecture below.

First Nontrivial Coefficient Conjecture Let p be an odd prime, and let $d \mid |\mathbb{F}_p^\times| = p - 1$. Consider the degree-$d$ period polynomial associated to the subgroup of index d of $(\mathbb{Z}/p\mathbb{Z})^\times$,

$$P_{d,p}(x) \;=\; \prod_{a \in C_0} (x - \zeta_p^a) \;=\; x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_0,$$

Then the coefficient a_{d-2} (the first genuinely new coefficient after the trace term) is explicitly determined by the residue class of p modulo $2d$.
If d is even, then:

$$a_{d-2}(p) \;=\; \begin{cases} \dfrac{(d-1) - (d-1)p}{2d} & \text{if } p \equiv 1 \pmod{2d}, \\ \dfrac{(d-1) + p}{2d} & \text{if } p \equiv d+1 \pmod{2d}. \end{cases}$$

Equivalently, a_{d-2} is a linear function of p, determined entirely by $p \bmod 2d$.

if d is odd, then: (d=2k+1):

$$a_{d-2}(p) = \frac{k - kp}{d}$$

Note: this statement comes exclusively from the examples that were computed. Larger scale models/ more coefficient generation would result in clearer patterns and validation. I found this by computing line of best fit

5 Further Research

5.1 Inductive Lattice Construction Conjecture

Note on the Proof
While we provided a sketch of a proof, we still need to define a rigorous construction for the inductive lattice perspective.

Generalization(s)
1) Use existing literature or develop a new proof of which Gauss sums vanish under certain conditions. In other words, we need to see when they fail to be linearly independent in order to rule out any vanishing sums for "new fields" when we go from $\mathbb{Q}(\zeta_{p^r})$ to $\mathbb{Q}(\zeta_{p^{r+1}})$.
2) Potentially extend the inductive construction to more general fields i.e. those of the form $\mathbb{Q}(\zeta_{p_1^{r_1} \cdot p_2^{r_2}})$ and $\mathbb{Q}(\zeta_{2 \cdot p_1^{r_1}})$. These will require significantly more work to see how fields are preserved and which new fields are added.

Suggestions
Use Sage and some other computation tools to generate lattices with all relevant subfields and test out if inductive conjectures are possible. Potentially use data modeling to detect any patterns.

5.2 Coefficient Conjecture

Note on the Proof
We have no current proof or even sketch of a proof for this conjecture. So more research is necessary to see if there is a way to prove this claim.

Generalization(s)
1) Extending this to the next coefficient i.e. for the $d-3$ coefficient (where d is the degree of the period polynomial)
2) Gauss connected the cubic period polynomials to elliptic curves, so perhaps there is another connection to other algebraic varieties

Suggestions
1) Use a better compiler to generate data for more than just 1000 primes
2) Write a machine learning algorithm and train it on existing data to get it to predict coefficients

6 Computation Methodology and Code

6.1 Sage Code Explanation

The step by step construction that we gave in the first section are luckily very easily to replicate in Sage. I will give a brief explanation of how the code was written and how it can be used. Note, I will include the actual pasteable code in the appendix. The first two pieces of code will be explained step by step because they were utilized the most during this thesis. The other two are included as a bonus to give the reader more tools to play around with.

Single Polynomial

1) Set your parameters: prime p, divisor, degree of extension: d, and generator g. (this is the only step that the user has to manually set)
2) Set the polynomial rings that will be used later in computation. One is over $\mathbb{Q}$, the other is the ring $R[t]$ we defined above. The last is defined so we can reduce the computed polynomial modulo the larger cyclotomic polynomial Φ_n
3) Next, the code checks if the user entered a valid divisor, i.e. d must divide the order of the unit group
4) Computes the set of coset representatives by taking powers of the generator for $\mathbb{F}_p^\times/H_d$ and then sorts them. This gets printed.
5) Creates an empty list called Cosets and loops through numbers less than the divisor and computes the powers of dummy variable t corresponding to the cosets. This gets printed as well.
6) Computes values for α_d. This also gets printed
7) Multiplies the linear products using $x-$(the powers of t). This gets printed too.
8)Reduces the coefficients modulo Φ_n and prints the final result.

Sage Code Looped Polynomial:
This code loops over first 1000 primes and outputs the coefficients for some divisor that the user specifies. It outputs them along with the corresponding prime in a .csv format
1) The first part is a helper function that computes the smallest generator for each prime so the user doesn't have to manually do it for each cyclic group
2) As before, we define our rings
3) the user inputs a divisor d=... and the program computes the order of the corresponding unit group and checks if d divides that.
4) As in the previous code, it computes the cosets, the corresponding powers, and reduces the polynomial so it has integer coefficients
5) Code uses a dictionary to store coefficients and returns them
6) The it actually loops over all of the primes and does a check if it can actually return coefficients
7) the code formats the coefficients in a clean way that prints them as a .csv (comma separated values)
Note: the reader would have to edit several lines of code if they wanted to change the value of d. Every time there is a variable like c1,c2,c3... or s1,s2,s3... it would have to be edited

6.2 Sage Code

Sage Code Single Polynomial

```
#  Parameters
p = 13
d = 4
g = 2

#  Rings
Rt.<t> = PolynomialRing(QQ)
Rx.<x> = PolynomialRing(Rt)
Phi = Rt(cyclotomic_polynomial(p, 't'))

#  Group data
order = ZZ(p - 1)
if order % d != 0:
    raise ValueError( d must divide p-1 )

# H_d = < g^d >
Hd = sorted({pow(g, (j*d) % order, p) for j in range(order // d)})

# Cosets g^i * H_d
cosets = []
for i in range(d):
    gi = pow(g, i, p)
    Ci = sorted({(gi * h) % p for h in Hd})
    Ci = [a for a in Ci if a != 0]
    cosets.append(Ci)

print( H_d = , Hd)
print( Cosets = , cosets)

# Period sums in QQ[t]
S = [sum(t**a for a in C) for C in cosets]
print( S_i(t) = , S)

# F_d(t,x) in (QQ[t])[x]
F = prod(x - Si for Si in S)
print( F_d(t,x) = , F)

# Reduce coefficients mod Phi_p(t)
def reduce_coeffs_mod_phi(F, Phi):
    return Rx({k: (c % Phi) for k, c in F.dict().items()})

F_red = reduce_coeffs_mod_phi(F, Phi)
print( F_d(t,x) mod Phi_p(t) = , F_red)
```

Sage Code Looped Polynomial

```
def smallest_generator(p):
    # Find the smallest primitive root modulo prime p
    for g in range(2, p):
        if Mod(g, p).multiplicative_order() == p - 1:
            return g
    raise ValueError(f No primitive root found for p={p} )

def coeffs_for_prime(p):
    # Rings
    Rt.<t> = PolynomialRing(QQ)
    Rx.<x> = PolynomialRing(Rt)
    Phi = Rt(cyclotomic_polynomial(p, 't'))

    d = 16
    order = ZZ(p - 1)
    if order % d != 0:
        return None  # (only excludes p=2)

    g = smallest_generator(p)

    # H_d = < g^d >
    Hd = sorted({pow(g, (j*d) % order, p) for j in range(order // d)})

    # Cosets g^i * H_d (nonzero automatically for prime modulus)
    cosets = []
    for i in range(d):
        gi = pow(g, i, p)
        Ci = sorted({(gi * h) % p for h in Hd})
        cosets.append(Ci)

    # Period sums S_i(t)
    S = [sum(t**a for a in C) for C in cosets]

    # F_d(t,x) =    (x - S_i)
    F = prod(x - Si for Si in S)

    # Reduce coefficients mod Phi_p(t)
    def reduce_coeffs_mod_phi(F_poly, Phi_poly):
        return Rx({k: (Rt(c) % Phi_poly) for k, c in F_poly.dict().items()})

    F_red = reduce_coeffs_mod_phi(F, Phi)


    Fd = F_red.dict()
    c16 = Rt(Fd.get(16, 0)) % Phi
    c15 = Rt(Fd.get(15, 0)) % Phi
    c14 = Rt(Fd.get(14, 0)) % Phi
    c13 = Rt(Fd.get(13, 0)) % Phi
    c12 = Rt(Fd.get(12, 0)) % Phi
    c11 = Rt(Fd.get(11, 0)) % Phi
    c10 = Rt(Fd.get(10, 0)) % Phi
```

```
    c9 = Rt(Fd.get(9, 0)) % Phi
    c8 = Rt(Fd.get(8, 0)) % Phi
    c7 = Rt(Fd.get(7, 0)) % Phi
    c6 = Rt(Fd.get(6, 0)) % Phi
    c5 = Rt(Fd.get(5, 0)) % Phi
    c4 = Rt(Fd.get(4, 0)) % Phi
    c3 = Rt(Fd.get(3, 0)) % Phi
    c2 = Rt(Fd.get(2, 0)) % Phi
    c1 = Rt(Fd.get(1, 0)) % Phi
    c0 = Rt(Fd.get(0, 0)) % Phi

    return (c16, c15, c14, c13, c12, c11, c10, c9, c8, c7, c6, c5, c4, c3,c2,
                                                c1, c0)

# Main loop over first 1000 primes
from sage.all import primes_first_n
primes = primes_first_n(1000)



for p in primes:
    if p == 2:
        continue
    triple = coeffs_for_prime(p)
    if triple is None:
        continue
    c16, c15, c14, c13, c12, c11, c10, c9, c8, c7, c6, c5, c4, c3, c2, c1, c0 =
                                                  triple
    # Remove spaces so spreadsheet cells are clean
    s16 = str(c16).replace(   ,   )
    s15 = str(c15).replace(   ,   )
    s14 = str(c14).replace(   ,   )
    s13 = str(c13).replace(   ,   )
    s12 = str(c12).replace(   ,   )
    s11 = str(c11).replace(   ,   )
    s10 = str(c10).replace(   ,   )
    s9 = str(c9).replace(   ,   )
    s8 = str(c8).replace(   ,   )
    s7 = str(c7).replace(   ,   )
    s6 = str(c6).replace(   ,   )
    s5 = str(c5).replace(   ,   )
    s4 = str(c4).replace(   ,   )
    s3 = str(c3).replace(   ,   )
    s2 = str(c2).replace(   ,   )
    s1 = str(c1).replace(   ,   )
    s0 = str(c0).replace(   ,   )
    print(f {p},{s16},{s15},{s14},{s13},{s12},{s11},{s10},{s9},{s8},{s7},{s6},{
                                                  s5},{s4},{s3},{s2},{s1},{s0} )
```

Sage Code Looped Large Prime Polynomial

```
# Parameters (set the prime)
p = 104729

from sage.all import primitive_root, ComplexField, PolynomialRing, ZZ, divisors
                                        , exp, pi, I
g = primitive_root(p)                  primitive root

PREC = 200
ONLY_D = None

# Complex setup and root of unity
CC = ComplexField(PREC)
zeta = CC(exp(2*pi*I / p))

# Precompute zeta^a table for a=0..p-1 (O(p))
Z = [CC(1)] * p
for a in range(1, p):
    Z[a] = zeta * Z[a-1]

# ZZ[x] for final integer polynomials
Rx.<x> = PolynomialRing(ZZ)

def gaussian_periods_for_d(d):

    Return the d Gaussian periods (complex numbers) for divisor d | (p-1),
    using multiplicative generation of H_d = <g^d>     (Z/pZ)^  .

    m = (p - 1) // d
    h = pow(g, d, p)

    # Build H_d = {h^0, h^1, ..., h^(m-1)} modulo p
    Hd = [1]
    cur = 1
    for _ in range(1, m):
        cur = (cur * h) % p
        Hd.append(cur)

    # Period sums over the cosets g^i * H_d
    periods = []
    gi = 1
    for _ in range(d):
        s = CC(0)
        for hv in Hd:
            a = (gi * hv) % p
            s += Z[a]
        periods.append(s)
        gi = (gi * g) % p
    return periods

def integer_period_polynomial(periods):
```

```
    Build F_d(x) =     (x - period_i) in CC[x], then round coefficients to ZZ[x
                                                ].

    RCx.<xC> = PolynomialRing(CC)
    FC = RCx(1)
    for eta in periods:
        FC *= (xC - CC(eta))

    # Round real parts to nearest integers
    coeffs = [ZZ((c.real()).round()) for c in FC.list()]
    # FC.list() returns coefficients from constant term up; Rx takes same order
                                                .
    return Rx(coeffs)

# Divisors to process
all_divs = sorted(d for d in divisors(p-1) if d > 1)
divs = all_divs if ONLY_D is None else [d for d in all_divs if d in ONLY_D]

#  Compute and print (compact, one line per polynomial)
for d in divs:
    periods = gaussian_periods_for_d(d)
    Fd = integer_period_polynomial(periods)
    # One compact line (good for copy/paste into Sheets)
    print(f d={d}: {str(Fd).replace(' ', '')} )
```

Sage Code Singe Polynomial for any $n \in \mathbb{N}$

```
    #  Any n: Gaussian periods via concrete units in Z/nZ

# Parameters
n =50
d = 2  # desired index of subgroup H     (Z/nZ)^*, must divide   (n)

# Polynomial rings and  _n(t)
Rt.<t> = PolynomialRing(QQ)
Rx.<x> = PolynomialRing(Rt)
Phi = Rt(cyclotomic_polynomial(n, 't'))   #  _n(t) in QQ[t]
R = Integers(n)

# Helpers

def prime_power_unit_generators(p, e):

    Return generators (as integers modulo p^e) and their orders for (Z/p^e Z)
                                                ^*.
    For odd p: cyclic of order    = p^{e-1}(p-1) -> one generator.
    For p=2:
       e=1: trivial (skip)
       e=2: cyclic C2 -> generator 3
       e>=3: C2    C_{2^{e-2}} -> generators -1 (order 2) and 5 (order 2^{e-2})

    mod = p**e
    if p == 2:
        if e == 1:
            return [], []  # order 1, no generator
        if e == 2:
            return [3 % mod], [2]
        # e >= 3
        return [(-1) % mod, 5 % mod], [2, 2**(e-2)]
    else:
        phi = euler_phi(mod)
        # find a primitive root mod p^e (exists for odd p)
        for a in range(2, mod):
            if gcd(a, mod) != 1:
                continue
            if Mod(a, mod).multiplicative_order() == phi:
                return [a % mod], [phi]
        raise RuntimeError(f No generator found for (Z/{mod}Z)^* (unexpected) )

def lift_to_mod_n(residues, moduli):
       Lift (CRT) residues modulo moduli to a single residue modulo n.
    return ZZ(crt(residues, moduli))

def crt_embed_generators(n):

    Build a set of global generators g_i     (Z/nZ)^* and their orders m_i by
    combining per-prime-power generators via CRT.

    fac = factor(n)
    moduli = [p**e for (p, e) in fac]
```

```
    gens_global = []
    orders = []

    for idx, (p, e) in enumerate(fac):
        loc_gens, loc_orders = prime_power_unit_generators(p, e)
        for g_loc, m_loc in zip(loc_gens, loc_orders):
            residues = [1]*len(moduli)
            residues[idx] = g_loc
            g_glob = lift_to_mod_n(residues, moduli) % n
            gens_global.append(R(g_glob))
            orders.append(m_loc)
    return gens_global, orders  # lists of equal length

def subgroup_H_of_index_d(n, d):

    Construct a subgroup H     (Z/nZ)^* of index d using global generators g_i
                                of orders m_i.
    We pick divisors t_i | m_i so that     (m_i / t_i) = d, then set H = < g_i
                                ^(m_i / t_i) >.

    gens_global, orders = crt_embed_generators(n)
    m_total = 1
    for m in orders:
        m_total *= m
    if d < 1 or (m_total % d) != 0:
        raise ValueError(f Index d={d} must divide |(Z/{n}Z)^*| = {m_total} (
                                                ({n})={euler_phi(n)}). )

    # distribute prime-power factors of d across the cyclic components
    from sage.arith.misc import valuation
    t = orders[:]  # desired orders inside H's generators
    for q, e in factor(d):
        for _ in range(e):
            # choose a component with largest q-valuation available
            i_best = max(range(len(t)), key=lambda i: valuation(t[i], q))
            if valuation(t[i_best], q) == 0:
                raise ValueError(f Cannot realize index {d} with components {
                                                    orders}. )
            t[i_best] //= q

    # H generators: h_i = g_i^(orders[i] / t[i])
    hgens = [g ** (orders[i] // t[i]) for i, g in enumerate(gens_global)]

    # BFS closure to enumerate H
    H = {R(1)}
    frontier = [R(1)]
    while frontier:
        new_frontier = []
        for a in frontier:
            for h in hgens:
                b = a * h
                if b not in H:
                    H.add(b)
                    new_frontier.append(b)
```

```
        frontier = new_frontier

    # sanity check index
    U_size = euler_phi(n)
    if U_size // len(H) != d:
        raise RuntimeError(f Constructed H has wrong index: |U|/|H| = {U_size}/
                                                    {len(H)}     {d} )
    return H

def cosets_of_H(n, H):
       Return cosets of H in (Z/nZ)^* as lists of integers in 0..n-1.
    U = [R(a) for a in range(n) if gcd(a, n) == 1]
    U_set = set(U)
    cosets = []
    while U_set:
        g = next(iter(U_set))
        coset = {g * h for h in H}
        cosets.append(sorted(ZZ(u.lift()) for u in coset))
        U_set -= coset
    return cosets

#  Run / print
H = subgroup_H_of_index_d(n, d)
cosets = cosets_of_H(n, H)

print(f (Z/{n}Z)^* has   (n) = {euler_phi(n)} units )
print(f Chosen H has size {len(H)}; index = {euler_phi(n) // len(H)} (target d=
                                        {d}) )
print(f Cosets (as unit exponents 0..{n-1}): {cosets} )

# Period sums and period polynomial
S = [sum(t**a for a in C) % Phi for C in cosets]
print( S_i(t) = , S)

F = prod(x - Si for Si in S)
F_red = Rx({k: (c % Phi) for k, c in F.dict().items()})
print(f F_{d}(t, x) = , F)
print(f F_{d}(t, x) mod   _{n}(t) = , F_red)
```

7 Citations

References

[1] Mark Reeder, *Notes on Galois Theory*, December 29, 2023.

[2] G. Myerson, "Period Polynomials and Gaussian Sums," *Math. Comp.* 48 (1987), 5363.

[3] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*, 2nd ed., Springer, Undergraduate Texts in Mathematics, Cham, 2015.

[4] J. Shurman, "Lecture 7: Unit-Group Structure," Reed College, 2024. Available at `https://people.reed.edu/~jerry/361/lectures/lec07.pdf`.

[5] T. Y. Lam and K. H. Leung, "On Vanishing Sums of Roots of Unity," *Journal of Algebra* 224 (2000), 91109.

[6] A. Cafure, "A Story About Cyclotomic Polynomials: The Minimal Polynomial of $\zeta_n + \zeta_n^{-1}$ and Its Constant Term," *Mathematics Magazine* 94 (2021), no. 5, 325338. doi:10.1080/0025570X.2021.1977537.