CYCLOTOMIC INTERMEDIATE FIELDS: EXPLICIT COMPUTATIONS

JUSTIN KATZ

Fix an odd prime p, and let ζ be a primitive pth root of unity and let $K = \mathbb{Q}(\zeta)$ be the pth cyclotomic field.

The extension $K/\mathbb{Q}$ is Galois, with $\mathrm{Gal}(K/\mathbb{Q}) \approx (\mathbb{Z}/p\mathbb{Z})^\times$, the isomorphism being

$$(\zeta \mapsto \zeta^a) \mapsto a.$$

For each divisor m of $p-1 = |\,\mathrm{Gal}(K/\mathbb{Q})|$ there is a unique order m subgroup H_m of $\mathrm{Gal}(K/\mathbb{Q})$, which fixes the unique subfield K_m of K having degree m over $\mathbb{Q}$. The extension $K_m/\mathbb{Q}$ is also cyclic, but in general, to conclude that it is generated by an mth root of some element of $\mathbb{Q}$, we must be sure that K_m contains an mth root of unity.

We circumvent this concern by working in a different environment. Let ω be a primitive $p-1$st root of unity, and $F = Q(\omega)$, and define the compositum $L = FK = \mathbb{Q}(\zeta, \omega)$. Then L/F is Galois, and again $G = \mathrm{Gal}(L/F)$ is cyclic of order $p-1$ under the same isomorphism as above. The discussion above applies, and we may now conclude that the degree m intermediate field is generated by an mth root of an element in F.

The goal of this document is to explicitly determine the radical expression for generators of the intermediate fields for specific primes.

In the first section, some general theory is sketched:

- We construct elements of L that are equivariant under the action of G. Upon raising to a suitable power, equivariance dictates that these elements lie in the base field F, so are thus the roots we are searching for. The equivariant elements are particular *Gauss sums*, which are an instantiation of a more general construction: Lagrange resolvents.
- Since G is cyclic, so is its group of characters $\hat{G}$. We characterize a useful generator of the character group, the *Kummer character*, and prove its existence using Hensel's lemma.
- With the goal of factoring the power of Gauss sum that lies in F into primes ideals of $\mathcal{O}_F$, we factor the Gauss sum itself in the top field L. We have no need to explicitly determine the prime factors of the Gauss sum in $\mathcal{O}_L$ lying over those in $\mathcal{O}_F$, but the enlarged environment of the former allows for computation not accessible in the latter.
- Last, we specialize to the case that the prime factors of the power of the Gauss sum are *principal*, in which case the preceding computations determines the decomposition up to a unit, in fact a root of unity, which we identify.

This document is based on the writeup `http://people.reed.edu/~jerry/361/lectures/kummer.pdf` , which is in turn based on `http://www.math.umn.edu/~garrett/m/v/kummer_eis.pdf`.

1 Some algebraic number theory

1.1 Galois Equivariant elements: Gauss sums

Fix a character $\chi : G \to F^\times$, and symmetrize ζ viz

$$\tau(\chi) = \sum_{g\in G} \chi(g)g(\zeta) \in L.$$

Equivariance is built in, for any $g \in G$, changing variables in the sum and using multiplicitivity of χ, compute

$$g\tau(\chi) = \chi(g^{-1})\tau(\chi).$$

For nontrivial χ, this shows that $\tau(\chi)$ lies in a proper extension of K in L.

However, since G is finite cyclic, there is some minimal nonzero m (depending on χ) dividing $p-1$, the order of G, such that

$$g(\tau(\chi))^m = (\tau(\chi))^m \quad \text{for all } g \in G.$$

Since the extension $\mathrm{Gal}(L/F)$ is Galois, this shows that $\tau(\chi)^m \in F$. By standard Galois theory, the minimal polynomial for $\tau(\chi)$ over F is $x^m - \tau(\chi)^m \in F[x]$, which splits in the unique extension $F(\tau(\chi))$ of F, since F contains a primitive mth root of unity.

Last, use the isomorphism $(\zeta \mapsto \zeta^a) \mapsto a + p\mathbb{Z}$ to compute the identity $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)p$:

$$\begin{aligned}\tau(\chi)\tau(\overline{\chi}) &= \sum_{a,b} \chi(a)\chi(b^{-1})\zeta^{a-b} = \sum_{a,c} \chi(c^{-1})\zeta^{a(1+c)} \\ &= \sum_{c} \chi(c^{-1}) \sum_{a} \zeta^{a(1+c)} = \chi(-1)(p-1) + 1 = \chi(-1)p.\end{aligned}$$

In particular, observe that at the level of ideals, any prime dividing $\tau(\chi)$ in an extension of $\mathbb{Q}$ lies over p.

1.2 The Kummer character

Since $p = 1 \mod p-1$, the ideal $p\mathbb{Z}$ is unramified in $\mathcal{O}_F$, decomposing as a product of a prime $\mathfrak{q}$ and its Galois conjugates $\sigma\mathfrak{q}$ for $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. The residue field $\mathcal{O}_F/\mathfrak{q}$ has order p, and the projection $\mathcal{O}_F \to \mathcal{O}_F/\mathfrak{q} \approx \mathbb{Z}/p\mathbb{Z}$ restricts to a group homomorphism of multiplicative subgroups $(\mathcal{O}_F)^\times \to (\mathcal{O}_F/\mathfrak{q})^\times \approx (\mathbb{Z}/p\mathbb{Z})^\times$. The primitive $p-1$st root of unity ω generates a cyclic subgroup $\langle\omega\rangle$ in $\mathrm{O}_F^\times$ which is taken isomorphically to $(\mathcal{O}_F/\mathfrak{q})^\times \approx (\mathbb{Z}/p\mathbb{Z})^\times$, as shown in a moment.

Granting the isomorphism, we can define a unique character $\chi_\mathfrak{q} : \mathrm{Gal}(L/F) \to \mathcal{O}_F^\times$ satisfying

$$\chi_\mathfrak{q}(\zeta \mapsto \zeta^a) = a + \mathfrak{q} \qquad \text{for all } a \in (\mathbb{Z}/p\mathbb{Z})^\times.$$

This is the Kummer character, sometimes called the Teichmuller character.

We seek to demonstrate the existence and uniqueness of an element $\omega^k \in \mathcal{O}_F^\times$ such that $\omega^k = a \mod \mathfrak{q}$. Fix $x_1 = a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then x_1 satisfies the polynomial $f(x) = x^{p-1} - 1 \mod \mathfrak{q}$, and further since x_1 is nonzero mod $\mathfrak{q}$, it does not satisfy the derivative $f'(x) = (p-1)x^{p-2} \mod \mathfrak{q}$. By Hensel's lemma, x_1 lifts to a solution in the integral domain $\lim \mathcal{O}_F/\mathfrak{q}^n$. That said, the $p-1$

distinct powers of ω already comprise a full solution set to f, and are already in $\mathcal{O}_F^\times$. Thus, the character above is well defined.

Remark. As an example take $p = 5$, which factors as

$$5 = (2+i)(2-i) \in F = \mathbb{Q}(i).$$

In this case, $\mathfrak{q} = (2+i)\mathcal{O}_F$ is principal, and the Kummer character is characterized by

$$\chi_{\mathfrak{q}}(\zeta \mapsto \zeta^a) = a + (2+i)\mathcal{O}_F \in \langle i \rangle/(2+i)\mathcal{O}_F \subset \mathcal{O}_F^\times/\mathfrak{q}.$$

The automorphism $\zeta \mapsto \zeta^2$ generates $\mathrm{Gal}(L/F)$, and thus $\chi_{\mathfrak{q}}$ is determined by value there. We are looking for the element of $\langle i \rangle$ which is $2 \mod 2+i$. The unique such element is $-i$. Thus

$$\chi_{\mathfrak{q}}(\zeta \mapsto \zeta^{2^a}) = (-i)^a.$$

Returning to generality, since $\chi_{\mathfrak{q}}$ has order $p-1$, it generates the characters of $\mathrm{Gal}(L/F)$. Thus, the element $\tau(\chi_{\mathfrak{q}}^n)$ generates the unique subfield of $L = \mathbb{Q}(\zeta, \omega)$ of degree $|\chi_{\mathfrak{q}}^n| = (p-1)/\gcd(n, p-1)$ over $F = \mathbb{Q}(\omega)$.

1.3 Factoring $\tau(\chi_{\mathfrak{q}}^{-n})$ in $\mathcal{O}_L$

Knowing that $\tau(\chi_{\mathfrak{q}}^{-n})^{|\chi_{\mathfrak{q}}^{-n}|} \in \mathcal{O}_F$ we seek a formula for its prime factors in $\mathcal{O}_F$, so that we can describe the relevant extension of F as a radical expression. To do so, we first work in the top field L and its ring of integers $\mathcal{O}_L$.

In $\mathcal{O}_L$ we have the factorization

$$p\mathcal{O}_L = \prod_{g \in \mathrm{Gal}(L/K)} (g\mathfrak{P})^{p-1}, \quad \mathfrak{P} \text{ prime in } \mathcal{O}_L, \text{ lying over } p\mathbb{Z}.$$

Thus, to factor $\tau(\chi_{\mathfrak{q}}^{-n})\mathcal{O}_L$, we wish to determine the valuations

$$\mathrm{ord}_{g\mathfrak{P}}(\tau(\chi^{-n})), \quad \text{for each } g \in \mathrm{Gal}(L/F).$$

A useful fact in the following computation is that the ideal $\mathfrak{P}$ lies over the ideal $(1-\zeta)\,\mathrm{O}_K$, with no ramification.

Start with $n = 1$, then compute using the last observation,

$$\begin{aligned}
\tau(\chi_{\mathfrak{q}}^{-1}) + \mathfrak{P}^2 &= \sum_{a \in \mathbb{Z}/p\mathbb{Z}^\times} \chi_{\mathfrak{q}}^{-1}(a)(1+\zeta-1)^a + \mathfrak{P}^2 \\
&= \sum_{a \in \mathbb{Z}/p\mathbb{Z}^\times} \chi_{\mathfrak{q}}^{-1}(a)(1+a(\zeta-1)) + \mathfrak{P}^2 \\
&= (\zeta-1) \sum_{a \in \mathbb{Z}/p\mathbb{Z}^\times} \chi_{\mathfrak{q}}^{-1}(a)a + \mathfrak{P}^2.
\end{aligned}$$

Then, dividing through by $\zeta - 1$ using that $\zeta - 1$ is unramified in $\mathcal{O}_L$, the characterization $\chi_{\mathfrak{q}}^{-1}(a) = a^{-1} \mod \mathfrak{q}$, and that $\mathfrak{P}|\mathfrak{q}|p\,\mathrm{O}_L$, see

$$\frac{\tau(\chi_{\mathfrak{q}}^{-1})}{\zeta-1} + \mathfrak{P} = p - 1 + \mathfrak{P} = -1 + \mathfrak{P}.$$

Next, use the Jacobi sum identity

$$\tau(\chi_{\mathfrak{q}}^{-n}) = \frac{\tau(\chi_{\mathfrak{q}}^{-1})\tau(\chi_{\mathfrak{q}}^{-(n-1)})}{J(\chi_{\mathfrak{q}}^{-1}, \chi_{\mathfrak{q}}^{-(n-1)})}$$

to prove by induction the identity for $n \in \{1, ..., p-2\}$

$$\frac{\tau(\chi_{\mathfrak{q}}^{-1})}{(\zeta - 1)^n} + \mathfrak{P} = \frac{-1}{n!} + \mathfrak{P}.$$

Then, since $\zeta - 1$ is unramified in $\mathfrak{P}$, this yields the formula for such n:

$$\mathrm{ord}_{\mathfrak{P}}(\tau(\chi_{\mathfrak{q}}^{-n})) = n.$$

To determine the valuation for the Galois conjugates $g\mathfrak{P}$, recall that the definition of the Kummer character $\chi_{\mathfrak{q}}$ is subordinate to a choice of any prime $\mathfrak{q}$ in $\mathcal{O}_F$ over p, and $\mathfrak{P}$ is the prime in $\mathcal{O}_L$ over $\mathfrak{q}$. These choices are eliminated by noting that $\mathrm{Gal}(L/K) \approx \mathrm{Gal}(F/\mathbb{Q})$ acts transitively on such primes, and thus for any $g \in \mathrm{Gal}(L/K) \approx \mathrm{Gal}(F/\mathbb{Q}) \approx (\mathbb{Z}/(p-1)\mathbb{Z})^\times$ we have

$$\mathrm{ord}_{g\mathfrak{P}}(\tau(\chi_{g\mathfrak{q}}^{-n})) = n.$$

Next, recall that $g \in \mathrm{Gal}(L/K) \approx \mathrm{Gal}(K/\mathbb{Q})$ acts by raising ω to a power, and the Kummer character takes its values in the subgroup $\langle\omega\rangle$. Employing the isomorphism $\sigma_b = (\omega \mapsto \omega^b) \mapsto b + (p-1)\mathbb{Z}$, we see

$$\sigma_b \chi_{\mathfrak{q}}^{-n} = \chi_{\mathfrak{q}}^{-nb}.$$

On the other hand, $\chi_{\mathfrak{q}}^{-n}$ is characterized by $\chi_{\mathfrak{q}}^{-n}(\zeta \mapsto \zeta^a) = a^{-n} + \mathfrak{q}$, so

$$\sigma_b \chi_{\mathfrak{q}}^{-n}(\zeta \mapsto \zeta^a) = a^{-n} + \sigma_b(\mathfrak{q}) = \chi_{\sigma_b\mathfrak{q}}^{-n}(\zeta \mapsto \zeta^a).$$

Combining the two displays, we see $\chi_{\mathfrak{q}}^{-nb} = \chi_{\sigma_b\mathfrak{q}}^{-n}$ and thus $\chi_{\mathfrak{q}}^{-n} = \chi_{\sigma_b\mathfrak{q}}^{-nb^{-1}}$, where the inverse b^{-1} is taken in $(\mathbb{Z}/(p-1)\mathbb{Z})^\times$. Thus, applying the valuation formula above, we see

$$\mathrm{ord}_{\sigma_b\mathfrak{P}}(\tau(\chi_{\mathfrak{q}}^{-n})) = nb^{-1} \in \{1, .., p-2\}.$$

We have just determined the factorization, for $n \in \{1, ..., p-2\}$

$$\tau(\chi_{\mathfrak{q}}^{-n})\mathcal{O}_L = \prod_{\sigma_b \in \mathrm{Gal}(L/K)} (\sigma_b\mathfrak{P})^{nb^{-1}}$$

1.4 Factorization of $\tau(\chi_{\mathfrak{q}}^{-n})^m$ in a subring of $\mathcal{O}_F$

For the remainder, assume $n | p-1$.

By construction, for any character $\chi : \mathrm{Gal}(L/F) \to F^\times$, the power $\tau(\chi)^{p-1}$ of the Gauss sum is fixed by $\mathrm{Gal}(L/F)$, and thus lies in F. Letting $m = |\chi_{\mathfrak{q}}^{-n}| = (p-1)/n$, observe that $\tau(\chi_{\mathfrak{q}}^{-n})^m$ is still fixed by $\mathrm{Gal}(L/F)$, and thus still lies in F, but is also fixed by the subgroup in $\mathrm{Gal}(K/\mathbb{Q})$ of order m, and thus, letting $\omega_m = e^{2\pi i/m}$, lies in the proper subfield $F_m = \mathbb{Q}(\omega_m)$ of F.

In F_m, there is a prime ideal $\mathfrak{p} \subset \mathcal{O}_{F_m}$ over p, and under $\mathfrak{q}$ so that

$$p\mathcal{O}_{F_m} = \prod_{g \in \mathrm{Gal}(F_m/\mathbb{Q})} g\mathfrak{p}.$$

Since the Gauss sum lies over p, its power in F_m lies over a power of p. Thus, to factor the power of the Gauss sum, we seek a formula for the quantities

$$\operatorname{ord}_{g\mathfrak{p}}(\tau(\chi_{\mathfrak{q}}^{-n})^m) \quad \text{for each } g \in \operatorname{Gal}(F_m/\mathbb{Q}) \approx (\mathbb{Z}/m\mathbb{Z})^\times.$$

To compute these, note that the automorphisms in $\operatorname{Gal}(F_m/\mathbb{Q})$ act by $\omega_m \mapsto \omega_m^\beta$ for some $\beta \in (\mathbb{Z}/m\mathbb{Z})^\times$. From the definition of ω and ω_m, each such automorphisms arises as the restriction of the automorphisms of the form $\omega \mapsto \omega^b$ where $b+m\mathbb{Z} = \beta+m\mathbb{Z}$. For any β, there are $\varphi(p-1)/\varphi(m)$ equally viable choices for b. Furthermore, we have the decomposition in the top field L,

$$\sigma_\beta \mathfrak{p}\, \mathrm{O}_L = \prod_{b=\beta \mod m} (\sigma_b \mathfrak{P})^{p-1}.$$

Thus, for every power of $\sigma_\beta\mathfrak{p}$ dividing $\tau(\chi_{\mathfrak{q}}^{-n})^m$ in $\mathcal{O}_{F_m}$, that power of $(\sigma_\beta\mathfrak{P})^{(p-1)/m}$ does too, and conversely. This gives

$$\operatorname{ord}_{\sigma_\beta\mathfrak{p}}(\tau(\chi_{\mathfrak{q}}^{-n})^m) = \frac{m}{p-1} \operatorname{ord}_{\sigma_b\mathfrak{P}}(\tau(\chi_{\mathfrak{q}}^{-n})).$$

We computed valuation on the right side to be nb^{-1}. Last, since $m = |\chi_{\mathfrak{q}}^{-n}| = (p-1)/n$, the display above becomes

$$\operatorname{ord}_{\sigma_\beta\mathfrak{p}}(\tau(\chi_{\mathfrak{q}}^{-n})^m) = \beta^{-1}$$

where β^{-1} is interpreted modulo m.

This shows the factorization in $\mathcal{O}_{F_m}$

$$\tau(\chi_{\mathfrak{q}}^{-n})^m \mathcal{O}_{F_m} = \prod_{\beta \in (\mathbb{Z}/m\mathbb{Z})^\times} (\sigma_\beta \mathfrak{p})^{\beta^{-1}}$$

1.5 Specializing to $\mathfrak{p}$ principal

When the prime $\mathfrak{p}$ (and thereby its Galois conjugates) dividing $\tau(\chi_{\mathfrak{q}}^{-n})^m\mathcal{O}_{F_m}$ is principal, say $\mathfrak{p} = \pi\mathcal{O}_{F_m}$ the last display determines the factorization of $\tau(\chi_{\mathfrak{q}}^{-n})^m$ up to a unit $u \in \mathcal{O}_{F_m}^\times$,

$$\tau(\chi_{\mathfrak{q}}^{-n})^m = u \prod_{\beta \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_\beta \pi^{\beta^{-1}}.$$

Note that this factorization does not require that the primes lying over π be principal.

In the source writeups, a theorem due to Kronecker is used to show that the unit $u \in \mathcal{O}_{F_m}^\times$ is actually a root of unity. Further, some (cyclotomic) polynomial arithmetic combined with Kummer's estimate, from the third section, shows that the root of unity u is characterized by the congruence

$$\frac{u \prod \sigma_\beta \pi^{\beta^{-1}}}{-p} + \pi\mathcal{O}_{F_m} = \left(\frac{-1}{n!}\right)^m + \pi\mathcal{O}_{F_m}.$$

This expression simplifies in noting that the Galois norm of π over $\mathbb{Q}$ is $\prod_{g \in \operatorname{Gal}(F_m/\mathbb{Q})} g\pi = p$, so that the characterization of u is

$$-u \prod_{\beta \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_\beta \pi^{\beta^{-1}-1} + \pi\mathcal{O}_{F_m} = \left(\frac{-1}{n!}\right)^m + \pi\mathcal{O}_{F_m}.$$

A derivation of these characterizations are in the source writeups, both of which deal with the case that n does not divide $p-1$. Since the goal is to compute the radical expressions for generators of intermediate fields, such generality is not needed.

2 Application of generalities: computing generators

2.1 One more generality: the quadratic subfield

Let p be any odd prime, so that $p-1$ is divisible by 2. Take $n=(p-1)/2$, so that $m=2$. The field F_2 is just $\mathbb{Q}$, so $\mathcal{O}_{F_2}=\mathbb{Z}$.

The nth power of the Kummer character is quadratic, meaning $\chi_{\mathfrak{q}}^{-n}=\overline{\chi}_{\mathfrak{q}}^{-n}$, and thus $\chi_{\mathfrak{q}}^{-n}=(\cdot/p)$, where the latter expression is the Legendre symbol. In this case, the Gauss sum identity from above becomes $\tau^2=(-1/p)p$. Certainly p is prime in $\mathcal{O}_{F_2}=\mathbb{Z}$, and $(-1/p)\in\{\pm 1\}$ is a 2nd root of unity.

Thus, without having to bring the machinery developed above to bear, we find that the unique subfield of L of degree 2 over F is $\mathbb{Q}(\omega,\sqrt{(-1/p)p})$.

Remark. The characterization of the unit, knowing that when $n=(p-1)/2$ the unit is $(-1/p)$ shows (noting that $\mathrm{Gal}(F_m/\mathbb{Q})=\mathrm{Gal}(\mathbb{Q}/\mathbb{Q})=\{1\}$)

$$-\left(\frac{-1}{p}\right)+p\mathbb{Z}=\left(\frac{p-1}{2}!\right)^{-2}+p\mathbb{Z}.$$

There is a clear indication of some relationship with a special case of quadratic reciprocity, using Gauss' lemma, but I do not have time to explore this.

2.2 Working at specific p

Set $p=5$: Take $n=1$ so $m=4$. Compute in $\mathcal{O}_{F_4}=\mathbb{Z}[i]$

$$5=(2+i)(2-i)=\pi\cdot\sigma_3\pi.$$

By the formula for the power of the Gauss sum, we have

$$\tau(\chi_\pi^{-1})^4=u\cdot\pi\cdot\sigma_3\pi^3=u5(3+4i)$$

and the unit is characterized by

$$u\sigma_3\pi^2+\pi\mathcal{O}_{F_4}=1+\pi\mathcal{O}_{F_4}.$$

Working mod π, we see that $u+\pi\mathcal{O}_{F_4}=-1+\pi\mathcal{O}_{F_4}$, and thus $u=-1$. Consequently, we have an alternate expression for L (being the 'unique subfield of L of degree 6 over F')

$$L=\mathbb{Q}\left(i,\sqrt[4]{-5(3-4i)}\right)$$

Set $p=7$: Take $n=2$ so $m=3$. Let $\omega_3=\omega^2$, a primitive third root of unity, so $F_3=\mathbb{Q}(\omega_3)$. Then we can factor p in $\mathcal{O}_{F_3}$ by hand,

$$7=(2-\omega_3)(3+\omega_3)=\pi\cdot\sigma_2\pi,\quad \text{where } \sigma_2:\omega_3\mapsto\omega_3^2=-\omega-1.$$

Then from our formula for the prime decomposition of the power of the Gauss sum,

$$\tau(\chi_\pi^{-2})^3=u\pi\cdot\sigma_2\pi^2,\quad \text{for some root of unity } u\in\mathcal{O}_{F_3}^\times.$$

The unit u is characterized by

$$-u\cdot\pi^0\cdot\sigma_2\pi^1+\pi\mathcal{O}_{F_3}=\left(\frac{-1}{2!}\right)^3+\pi\mathcal{O}_{F_3}.$$

Since $2^3 + \pi\mathcal{O}_{F_3} = \omega_3^3 + \pi\mathcal{O}_{F_3} = 1 + \pi\mathcal{O}_{F_3}$, the congruence is

$$u(3+\omega_3) + \pi\mathcal{O}_{F_3} = 1 + \pi\mathcal{O}_{F_3},$$

which simplifies to $5u + \pi\mathcal{O}_{F_3} = 1 + \pi\mathcal{O}_{F_3}$. Thus $u + \pi\mathcal{O}_{F_3} = 3 + \mathcal{O}_{F_3} = -\omega_3^2 + \pi\mathcal{O}_{F_3}$. Since u is a root of unity, the formermost and lattermost elements are equal, showing that $\tau(\chi_\pi^{-2})^3 = -\omega_3^2\pi\sigma_2\pi^2 = \omega_3^2 7(3+\omega_3)$. Thus, the unique cubic extension of F in L is

$$\mathbb{Q}\left(\omega, \sqrt[3]{-7\omega_3^2(3+\omega_3)}\right).$$

Next, take $n = 1$ so $m = 6$. Note $\omega_3^2 = -\omega_6 = -\omega$ and already $\omega_3 \in F_6 = F$. Thus $F_3 = F_6 = F$. Thus, the factorization

$$7 = (2-\omega_3)(3+\omega_3)$$

is still sensible in $\mathcal{O}_{F_6}$. However, since 2 is not invertible mod 6, we must use the Galois automorphism $\sigma_5 = \omega_6 \mapsto \omega_6^5$. Again, letting $\pi = 2 - \omega_3$, the factorization is

$$7 = \pi \cdot \sigma_5\pi.$$

Consequently, the factorization of the power of the Gauss sum is (for some root of unity u)

$$\tau(\chi_\pi^{-1})^6 = u \cdot \pi \cdot \sigma_5\pi^5 = u \cdot 7 \cdot \sigma_5\pi^4.$$

The root of unity u is characterized by

$$-u(\sigma_5\pi)^4 + \pi\mathcal{O}_F = (-1/1!)^6 + \pi\mathcal{O}_F.$$

This congruence is $-u(-2)^4 + \pi\mathcal{O}_F = 1\pi\mathcal{O}_F$, again giving $5u + \pi\mathcal{O}_F = 1 + \pi\mathcal{O}_F$, which we know means $u = -\omega_3^2$. This determines an alternate expression for L,

$$L = \mathbb{Q}(\omega, \zeta) = \mathbb{Q}(\omega, \sqrt[6]{-7\omega_3^2(3+\omega_3)^4})$$

Set $p = 11$ Take $n = 2$ so $m = 5$. Compute

$$11 = \frac{-33}{-3} = \frac{(-2)^5 - 1}{-2-1} = \sum_{i=1}^{4} 2^i = \prod_{i=1}^{4}(2+\omega_5^i).$$

Set $\pi = 2 + \omega_5$, so that the formula for the power of the Gauss sum is

$$\tau(\chi_\pi^{-2})^5 = u\pi \cdot \omega_2\pi^3 \cdot \omega_3\pi^2 \cdot \omega_4\pi^4.$$

The unit u is characterized by the congruence

$$-u\sigma_2\pi^2 \cdot \sigma_3\pi \cdot \sigma_4\pi^3 + \pi\mathcal{O}_{F_5} = -1/2^5 + \pi\mathcal{O}_{F_5}.$$

From the congruence $2 + \pi\mathcal{O}_{F_5} = \omega_5 + \pi\mathcal{O}_{F_5}$, the congruence is

$$-u(2+4)^2(2-2^3)(2+2^4)^3 + \pi\mathcal{O}_{F_5} = -1 + \pi\mathcal{O}_{F_5},$$

which reduces to $u + \pi\mathcal{O}_{F_5} = 4 + \pi\mathcal{O}_{F_5} = \omega_5^2 + \mathcal{O}_{F_5}$ showing equality of the former and the latter. Thus, the quintic extension of F in L is

$$\mathbb{Q}\left(\omega, \sqrt[5]{11\omega_5^2(2+\omega_5^2)^2(2+\omega_5)(2+\omega_5^4)^3}\right).$$