SKW

Xavier Roblot

October 29, 2026

Chapter 1

Setup

1.1 The fields and the primes

Let p be a prime number and f a positive integer. Set $q = p^f$. Let $L = \mathbb{Q}(\zeta_{p(q-1)})$ be the $p(q-1)$-th cyclotomic field. Inside L, we consider the subfields $K = \mathbb{Q}(\zeta_{q-1})$ and $F = \mathbb{Q}(\zeta_p)$, and we fix a primitive p-th root of unity $\zeta_p \in \mathcal{O}_F$. We fix a maximal ideal P of $\mathcal{O}_K$ lying above p and a maximal ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying above P. Since the order of p modulo $q-1$ is f, the residue field $\mathcal{O}_K/P$ has q elements.

Remark 1. In the formalization, most results of Chapters 1 to 3 are proved for an arbitrary integer $n \geq 1$ in place of $q-1$, with $K = \mathbb{Q}(\zeta_n)$, any number field L containing K and F, and the hypothesis that P has Teichmüller lifts of order n (1). Some of them then carry hypotheses such as $1 < n$, $e(\mathfrak{P} \mid P) \geq 2$ or $\zeta_p - 1 \notin \mathfrak{P}^2$, which all hold in the setting above. The case $n = q-1$ is obtained with 2.

1.2 The Teichmüller character

Definition 1. Let R be a commutative ring, I an ideal of R and n a positive integer. The ideal I *has Teichmüller lifts of order* n if the reduction map $\mu_n(R) \to (R/I)^\times$ is bijective.

Lemma 2. *The ideal P has Teichmüller lifts of order $q-1$.*

Proof. The ring $\mathcal{O}_K$ contains $q-1$ distinct $(q-1)$-th roots of unity, and the integer $q-1$ is not in P. Hence these roots stay distinct modulo P, so the reduction map is injective, and it is bijective since $(\mathcal{O}_K/P)^\times$ has $q-1$ elements. □

Definition 3. Assume that P has Teichmüller lifts of order $q-1$ (2). The *Teichmüller character* $\omega : \mathcal{O}_K/P \to \mathcal{O}_K$ is the multiplicative character whose restriction to $(\mathcal{O}_K/P)^\times$ is the inverse of the reduction map $\mu_{q-1}(\mathcal{O}_K) \xrightarrow{\sim} (\mathcal{O}_K/P)^\times$, extended by $\omega(0) = 0$.

Lemma 4. *For all $x \in \mathcal{O}_K/P$, we have $\omega(x) \equiv x \pmod{P}$.*

Proof. This is the definition for $x \neq 0$, and both sides vanish for $x = 0$. □

Lemma 5. *The order of ω as a multiplicative character is $q-1$.*

Proof. The values of ω on units are $(q-1)$-th roots of unity, so $\omega^{q-1} = 1$. The value of ω at the reduction of a primitive $(q-1)$-th root of unity is that root, so no smaller power of ω is trivial. □

Lemma 6. *Let $a \in \mathbb{Z}$ with $(q-1) \nmid a$. The character ω^{-a}, viewed with values in $\mathcal{O}_L$, is nontrivial. In particular,*

$$\sum_{x \in \mathcal{O}_K/P} \omega(x)^{-a} = 0.$$

Proof. The character ω^{-a} is nontrivial by 5, and stays nontrivial after composing with the injection $\mathcal{O}_K \to \mathcal{O}_L$. The vanishing of the sum is then `MulChar.sum_eq_zero_of_ne_one`. □

Lemma 7. *Let R be a ring containing $\mathcal{O}_K$ and let σ be a ring endomorphism of R such that $\sigma(\zeta_{q-1}) = \zeta_{q-1}^m$ for some $m \in \mathbb{N}$. Then $\sigma(\omega(x)^a) = \omega(x)^{am}$ for all $x \in \mathcal{O}_K/P$ and $a \in \mathbb{Z}$.*

Proof. For $x \neq 0$, the value $\omega(x)^a$ is a power ζ_{q-1}^k, so $\sigma(\omega(x)^a) = \zeta_{q-1}^{mk} = \omega(x)^{am}$. Both sides vanish for $x = 0$. □

1.3 The additive character

Definition 8. The *additive character* $\psi : \mathcal{O}_K/P \to \mathcal{O}_F$ is defined by

$$\psi(x) = \zeta_p^{\mathrm{tr}_{(\mathcal{O}_K/P)/(\mathbb{Z}/p\mathbb{Z})}(x)}.$$

We also view it as a character with values in $\mathcal{O}_L$.

Lemma 9. *The character ψ is nontrivial, i.e., $\psi \neq 1$.*

Proof. Since the extension $\mathcal{O}_K/P$ over $\mathbb{Z}/p\mathbb{Z}$ is separable, the trace $\mathrm{tr} : \mathcal{O}_K/P \to \mathbb{Z}/p\mathbb{Z}$ is nonzero, so there exists x with $\mathrm{tr}(x) \neq 0$, hence $\psi(x) = \zeta_p^{\mathrm{tr}(x)} \neq 1$. □

Lemma 10. *The character ψ is primitive.*

Proof. Since $\mathcal{O}_K/P$ is a field, any nontrivial additive character is primitive. The character ψ is nontrivial by 9. □

Lemma 11. *For all $x \in \mathcal{O}_K/P$, $\psi(x^p) = \psi(x)$.*

Proof. The Frobenius map $x \mapsto x^p$ is a $(\mathbb{Z}/p\mathbb{Z})$-algebra automorphism of $\mathcal{O}_K/P$, so it preserves the trace. □

Lemma 12. *Let $\mathfrak{Q}$ be an ideal of $\mathcal{O}_L$ with $\zeta_p - 1 \in \mathfrak{Q}$. Then*

$$\psi(x) \equiv 1 + \mathrm{tr}(x) \cdot (\zeta_p - 1) \pmod{\mathfrak{Q}^2}$$

for all $x \in \mathcal{O}_K/P$.

Proof. Write $\mathrm{tr}(x) = a$ with $a \in \mathbb{N}$. By the binomial theorem, $\psi(x) = (1+(\zeta_p-1))^a \equiv 1+a(\zeta_p-1) \pmod{\mathfrak{Q}^2}$. □

Lemma 13. *Let $\mathfrak{Q}$ be an ideal of $\mathcal{O}_L$ with $\zeta_p - 1 \in \mathfrak{Q}$. Then $\psi(x) \equiv 1 \pmod{\mathfrak{Q}}$ for all $x \in \mathcal{O}_K/P$.*

Proof. This follows from 12, since $\mathrm{tr}(x) \cdot (\zeta_p - 1) \in \mathfrak{Q}$. □

1.4 Primes above p

Lemma 14. *For every prime ideal $\mathfrak{Q}$ of $\mathcal{O}_L$ above p, we have $\zeta_p - 1 \in \mathfrak{Q}$.*

Proof. The ideal $(\zeta_p - 1)$ is the only prime of $\mathcal{O}_F$ above p, so it is $\mathfrak{Q} \cap \mathcal{O}_F$. □

Lemma 15. *Every prime ideal of $\mathcal{O}_L$ above p is unramified over $\mathcal{O}_F$.*

Proof. Let $\mathfrak{Q}$ be such a prime. By 105, $e(\mathfrak{Q} \mid p) = p - 1$, and this is also the ramification index of p in F. By multiplicativity of ramification indices in the tower $L/F/\mathbb{Q}$, the ramification index of $\mathfrak{Q}$ over $\mathcal{O}_F$ is 1. □

Chapter 2

The Gauss sum

Throughout this chapter and the next two, we assume that p is an odd prime.

2.1 Gauss and Jacobi sums

Definition 16. For $a \in \mathbb{Z}$, the *Gauss sum* is

$$g_a = g(\omega^{-a}, \psi) = \sum_{x \in \mathcal{O}_K/P} \omega(x)^{-a} \cdot \psi(x) \in \mathcal{O}_L.$$

Definition 17. For $a, b \in \mathbb{Z}$, the *Jacobi sum* is

$$J(a,b) = J(\omega^{-a}, \omega^{-b}) = \sum_{x+y=1} \omega(x)^{-a}\omega(y)^{-b} \in \mathcal{O}_K.$$

Lemma 18. *If $(q-1) \mid k$, then for all $a \in \mathbb{Z}$, $g_{a+k} = g_a$.*

Proof. Since $\omega^{q-1} = 1$ by 5, we have $\omega^{-k} = 1$, so $\omega^{-(a+k)} = \omega^{-a}$. □

Lemma 19. *If $(q-1) \mid a$, then $g_a = -1$.*

Proof. By 18, $g_a = g_0 = g(1, \psi)$, which is -1 by 107 since ψ is nontrivial by 9. □

Lemma 20. *For all $a \in \mathbb{Z}$, $g_{pa} = g_a$.*

Proof. Substitute $x \mapsto x^p$, a bijection of $\mathcal{O}_K/P$, in the sum defining g_a. We have $\omega(x^p)^{-a} = \omega(x)^{-pa}$ and $\psi(x^p) = \psi(x)$ by 11. □

Lemma 21. *If $(q-1) \nmid (a+b)$, then*

$$g_a \cdot g_b = g_{a+b} \cdot J(a,b).$$

Proof. The character $\omega^{-(a+b)}$ is nontrivial by 6, so this is `jacobiSum_mul_nontrivial` applied to ω^{-a} and ω^{-b}. □

Lemma 22. *If $(q-1) \nmid a$, then*

$$g_a \cdot g_{-a} = \omega^{-a}(-1) \cdot p^f.$$

Proof. The character ω^{-a} is nontrivial by 6 and ψ is primitive by 10. By `gaussSum_mul_gaussSum_eq_card`, $g(\omega^{-a}, \psi) \cdot g(\omega^a, \psi^{-1}) = |\mathcal{O}_K/P| = p^f$, and the change of variable $x \mapsto -x$ gives $g(\omega^a, \psi^{-1}) = \omega^a(-1) \cdot g_{-a}$. □

2.2 Congruences

Lemma 23. *If $(q-1) \nmid a$, then $g_a \in (\zeta_p - 1)\mathcal{O}_L$.*

Proof. By 13, $\psi(x) \equiv 1$ modulo $(\zeta_p - 1)$, so $g_a \equiv \sum_x \omega(x)^{-a}$, which is 0 by 6. □

Lemma 24. *If $(q-1) \nmid a$, then $g_a \in \mathfrak{P}$.*

Proof. Combine 23 and 14. □

Lemma 25. *If $(q-1) \nmid a$, then g_a is not a unit of $\mathcal{O}_L$.*

Proof. The element $\zeta_p - 1$ is not a unit of $\mathcal{O}_L$, so this follows from 23. □

Lemma 26. *If $(q-1) \nmid a$, then there exists $k \geq 1$ such that $|N_{L/\mathbb{Q}}(g_a)| = p^k$.*

Proof. Taking norms in 22, the integer $|N_{L/\mathbb{Q}}(g_a)|$ divides a power of p, so it is a power p^k. Since g_a is not a unit by 25, we have $k \geq 1$. □

Lemma 27. *For all $a \in \mathbb{Z}$, we have $g_a \neq 0$. If $(q-1) \nmid (a+b)$, then $J(a,b) \neq 0$.*

Proof. If $(q-1) \mid a$, then $g_a = -1$ by 19. Otherwise its norm is nonzero by 26. The second claim follows from the first and 21. □

Lemma 28. *We have*

$$g_1 \equiv -(\zeta_p - 1) \pmod{\mathfrak{P}^2}.$$

Proof. The extension $K/\mathbb{Q}$ is unramified at p, so $e(\mathfrak{P} \mid P) = p - 1 \geq 2$ by 105, hence $P \subseteq \mathfrak{P}^2$. Since $\zeta_p - 1 \in \mathfrak{P}$ by 14, 12 gives

$$g_1 \equiv \sum_x \omega(x)^{-1} + (\zeta_p - 1) \sum_x \omega(x)^{-1}\mathrm{tr}(x) \pmod{\mathfrak{P}^2}.$$

The first sum vanishes by 6 since $q-1 \geq 2$. For the second, we have $\omega(x) \equiv x \pmod{P}$ by 4 and $\mathrm{tr}(x) = \sum_{i<f} x^{p^i}$, and $\sum_{x \in \mathcal{O}_K/P} x^{-1}x^{p^i}$ is -1 for $i = 0$ and 0 for $0 < i < f$. Hence the second sum is -1 modulo $\mathfrak{P}^2$. □

2.3 Galois action

Lemma 29. *Restriction to K induces an isomorphism $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/(q-1)\mathbb{Z})^\times$. For $\sigma \in \mathrm{Gal}(L/F)$, we denote by $\mathfrak{n}(\sigma) \in \{0, \ldots, q-2\}$ the representative of its image, so that $\sigma(\zeta_{q-1}) = \zeta_{q-1}^{\mathfrak{n}(\sigma)}$.*

Proof. Since $\gcd(q-1, p) = 1$, the fields K and F are linearly disjoint over $\mathbb{Q}$ and $L = KF$. □

Lemma 30. *For all $\sigma \in \mathrm{Gal}(L/F)$ and $a \in \mathbb{Z}$,*

$$\sigma(g_a) = g_{a \cdot \mathfrak{n}(\sigma)}.$$

Proof. The automorphism σ fixes ζ_p, hence the values of ψ, and $\sigma(\omega(x)^{-a}) = \omega(x)^{-a\mathfrak{n}(\sigma)}$ by 7. □

Lemma 31. *Let $\tau \in \mathrm{Gal}(L/K)$ and $e \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $\tau(\zeta_p) = \zeta_p^e$. Then for all $a \in \mathbb{Z}$,*

$$\tau(g_a) = \omega(e)^a \cdot g_a.$$

Proof. The automorphism τ fixes the values of ω and $\tau(\psi(x)) = \psi(ex)$. The substitution $y = ex$ in the sum gives $\tau(g_a) = \sum_y \omega(y/e)^{-a}\psi(y) = \omega(e)^a g_a$. □

Chapter 3

The valuation function s

3.1 General properties

Definition 32. For $a \in \mathbb{Z}$ and a maximal ideal $\mathfrak{Q}$ of $\mathcal{O}_L$, let $s_{\mathfrak{Q}}(a) \in \mathbb{N}$ be the multiplicity of $\mathfrak{Q}$ in the ideal (g_a). We write $s(a) = s_{\mathfrak{P}}(a) = v_{\mathfrak{P}}(g_a)$.

Lemma 33. *If $a \equiv b \pmod{q-1}$, then $s(a) = s(b)$.*

Proof. Indeed $g_a = g_b$ by 18. □

Lemma 34. *If $(q-1) \mid a$, then $s(a) = 0$.*

Proof. By 19, $g_a = -1$ is a unit, so $(g_a) = \mathcal{O}_L$. □

Lemma 35. *If $(q-1) \nmid (a+b)$, then $s(a) + s(b) = s(a+b) + v_{\mathfrak{P}}(J(a,b))$.*

Proof. Take valuations in 21. All the elements involved are nonzero by 27, so the valuations are finite. □

Lemma 36. *For all $a, b \in \mathbb{Z}$, $s(a+b) \leq s(a) + s(b)$.*

Proof. If $(q-1) \mid (a+b)$, then $s(a+b) = 0$ by 34. Otherwise use 35. □

Lemma 37. *If $(q-1) \nmid a$, then $s(a) + s(-a) = f \cdot e(\mathfrak{P} \mid p)$.*

Proof. Take valuations in 22: the factor $\omega^{-a}(-1)$ is a root of unity, hence a unit, and $v_{\mathfrak{P}}(p^f) = f \cdot e(\mathfrak{P} \mid p)$. □

Lemma 38. *Assume $(q-1) \mid k$. Then*

$$s(a) + s(k-a) = \begin{cases} 0 & \text{if } (q-1) \mid a, \\ f \cdot e(\mathfrak{P} \mid p) & \text{otherwise.} \end{cases}$$

Proof. We have $s(k-a) = s(-a)$ by 33. Conclude with 34 and 37. □

Lemma 39. *We have*

$$2 \sum_{a=0}^{q-2} s(a) = (q-2) \cdot f \cdot e(\mathfrak{P} \mid p).$$

Proof. Pair the term a with $q-1-a$. By 38 with $k=q-1$, each of the $q-2$ values $1 \le a \le q-2$ gives $s(a)+s(q-1-a) = f \cdot e(\mathfrak{P} \mid p)$, and $s(0) = s(q-1) = 0$ by 34. □

Lemma 40. *Let $\mathfrak{Q}$ be a maximal ideal of $\mathcal{O}_L$ not lying above p. Then $s_{\mathfrak{Q}}(a) = 0$ for all $a \in \mathbb{Z}$.*

Proof. If $(q-1) \mid a$, use 34. Otherwise, if $g_a \in \mathfrak{Q}$, then the norm of $\mathfrak{Q}$ divides $N_{L/\mathbb{Q}}(g_a)$, which is a power of p by 26, so $\mathfrak{Q}$ lies above p. □

Lemma 41. *For all $\sigma \in \mathrm{Gal}(L/F)$ and $a \in \mathbb{Z}$, $s_{\sigma(\mathfrak{P})}(a) = s_{\mathfrak{P}}(a \cdot \mathfrak{n}(\sigma^{-1}))$.*

Proof. The multiplicity of $\sigma(\mathfrak{P})$ in (g_a) is the multiplicity of $\mathfrak{P}$ in $(\sigma^{-1}(g_a))$, and $\sigma^{-1}(g_a) = g_{a\mathfrak{n}(\sigma^{-1})}$ by 30. □

3.2 Upper bound by the sum of digits

Lemma 42. *We have $s(1) = 1$.*

Proof. By 24, $g_1 \in \mathfrak{P}$, so $s(1) \ge 1$. By 28, $g_1 \equiv -(\zeta_p - 1) \pmod{\mathfrak{P}^2}$, and $\zeta_p - 1 \notin \mathfrak{P}^2$ by 106, so $s(1) \le 1$. □

Lemma 43. *For all $a \in \mathbb{N}$, $s(a) \le a$.*

Proof. By induction on a, using $s(0) = 0$ (34), $s(a+1) \le s(a) + s(1)$ (36) and $s(1) = 1$ (42). □

Lemma 44. *Let $a \in \mathbb{N}$ and let $a = a_0 + a_1 p + \cdots + a_{t-1}p^{t-1}$ be its p-adic expansion. Then*

$$s(a) \le a_0 + a_1 + \cdots + a_{t-1}.$$

Proof. By induction on the list of digits. Write $a = a_0 + pa'$. Then $s(a) \le s(a_0) + s(pa') \le a_0 + s(a')$ by 36, 43, and $g_{pa'} = g_{a'}$ (20). □

3.3 The digit formula

Proposition 45. *Let $0 \le a \le q-2$ and let $a = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$, $0 \le a_i \le p-1$, be the p-adic expansion of a. Then*

$$s(a) = a_0 + a_1 + \cdots + a_{f-1}.$$

Proof. By 105, $e(\mathfrak{P} \mid p) = p-1$, so 39 gives $\sum_{a=0}^{q-2} s(a) = (q-2)f(p-1)/2$. A direct count shows that the sum of the digit sums of $0, \ldots, q-2$ has the same value. Since each term satisfies $s(a) \le a_0 + \cdots + a_{f-1}$ by 44, all these inequalities are equalities. □

Lemma 46. *Let $b > 1$, $l \ge 0$ and $0 \le x < b^l - 1$. Then*

$$(b-1)\sum_{i=0}^{l-1}(xb^i \bmod (b^l-1)) = (b^l-1)\cdot S_b(x),$$

where $S_b(x)$ is the sum of the base b digits of x.

Proof. Modulo b^l-1, multiplication by b cyclically rotates the l base b digits of x. Hence each digit of x occurs exactly once in each position in the sum, which is therefore $S_b(x)(1+b+\cdots+b^{l-1})$. □

Lemma 47. *Let m, d be positive integers with $q-1 = md$, and let $a \in \mathbb{N}$ with $da \leq q-2$. Then*

$$m \cdot s(da) = (p-1) \sum_{i=0}^{f-1} (ap^i \bmod m).$$

Proof. Multiply both sides by d. Since $d(ap^i \bmod m) = dap^i \bmod (q-1)$, this follows from 45 and 46 applied to $b = p$, $l = f$ and $x = da$. □

Chapter 4

Ideal factorization of Gauss sums

4.1 Setup for Stickelberger's theorem

Let m be a positive integer with $p \nmid m$, and assume that f is the multiplicative order of p modulo m. Then $m \mid q-1$, and we set $d = (q-1)/m$. Let $k = \mathbb{Q}(\zeta_m)$, a subfield of L, and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_k$ lying above p. We assume that $\mathfrak{P}$ lies above $\mathfrak{p}$.

Let $G = \mathrm{Gal}(k/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. For $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, let $\sigma_a \in G$ denote the element with $\sigma_a(\zeta_m) = \zeta_m^a$. The *Stickelberger element* is

$$\Theta = \Theta(k) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} a \cdot \sigma_a^{-1} \in \mathbb{Z}[G],$$

where a is identified with its representative in $\{0, \dots, m-1\}$. For an ideal $\mathfrak{a}$ of $\mathcal{O}_k$, we write $\mathfrak{a}^\Theta = \prod_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_a^{-1}(\mathfrak{a})^a$.

Remark 2. With the notation of Washington, $\Theta = m\theta$ where $\theta = \sum_{(a,m)=1} \{a/m\}\sigma_a^{-1} \in \mathbb{Q}[G]$.

4.2 Descent of g_d^m to k

Lemma 48. *For any $\tau \in \mathrm{Gal}(L/K)$, we have $\tau(g_d^m) = g_d^m$.*

Proof. By 31, $\tau(g_d) = \omega(e)^d g_d$ for some e, and $\omega(e)^{dm} = \omega(e)^{q-1} = 1$ by 5. □

Lemma 49. *Let $E = \mathbb{Q}(\zeta_{mp}) \subseteq L$. For any $\tau \in \mathrm{Gal}(L/E)$, we have $\tau(g_d) = g_d$.*

Proof. The automorphism τ fixes F and ζ_m, so $\mathfrak{n}(\tau) \equiv 1 \pmod m$, hence $d\mathfrak{n}(\tau) \equiv d \pmod{q-1}$. Conclude with 30 and 18. □

Lemma 50. *There exists $\Gamma \in \mathcal{O}_k$ with $g_d^m = \Gamma$.*

Proof. By 48 and 49, the element g_d^m lies in $K \cap E = \mathbb{Q}(\zeta_{\gcd(q-1,mp)}) = k$, and it is integral. □

4.3 Factorization in L

Lemma 51. *For all $a \in \mathbb{Z}$, we have the equality of ideals of $\mathcal{O}_L$*

$$(g_a) = \prod_{\mathfrak{Q}|p} \mathfrak{Q}^{s_{\mathfrak{Q}}(a)},$$

where the product runs over the primes of $\mathcal{O}_L$ above p.

Proof. The ideal (g_a) is nonzero by 27, and no prime outside p divides it by 40. □

4.4 Primes of k above p

Lemma 52. *The stabilizer of $\mathfrak{p}$ in G is the subgroup $\langle\sigma_p\rangle$, which has order f.*

Proof. The stabilizer of $\mathfrak{p}$ is its decomposition group, which acts on the residue field through powers of the Frobenius, and σ_p induces the Frobenius. The two groups have order f. □

Definition 53. For each prime $\mathfrak{q}$ of $\mathcal{O}_k$ above p, choose $a_\mathfrak{q} \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $\sigma_{a_\mathfrak{q}}^{-1}(\mathfrak{p}) = \mathfrak{q}$. The map

$$\{\mathfrak{q} \mid p\} \times \{0, \dots, f-1\} \to (\mathbb{Z}/m\mathbb{Z})^\times, \qquad (\mathfrak{q}, j) \mapsto a_\mathfrak{q} p^j$$

is a bijection, and the image a of $(\mathfrak{q}, j)$ satisfies $\sigma_a^{-1}(\mathfrak{p}) = \mathfrak{q}$.

Proof. The group G acts transitively on the primes above p, so $a_\mathfrak{q}$ exists. The bijectivity and the last claim follow from 52. □

Lemma 54. *Let $\mathfrak{q}$ be a prime of $\mathcal{O}_k$ above p and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $\sigma_a^{-1}(\mathfrak{p}) = \mathfrak{q}$. Then the sum of the (representatives of the) images of $(\mathfrak{q}, j)$, $0 \le j < f$, under the bijection of 53 is $\sum_{j=0}^{f-1}(ap^j \bmod m)$. In particular, $v_\mathfrak{q}(\mathfrak{p}^\Theta) = \sum_{j=0}^{f-1}(ap^j \bmod m)$.*

Proof. The images of the $(\mathfrak{q}, j)$ are the ap^j up to a cyclic shift of j modulo f. The second claim follows since the exponents of $\mathfrak{q}$ in $\mathfrak{p}^\Theta$ are the b with $\sigma_b^{-1}(\mathfrak{p}) = \mathfrak{q}$. □

4.5 Valuations and the factorization

Lemma 55. *Let $\mathfrak{q}$ be a prime of $\mathcal{O}_k$ above p and $\mathfrak{Q}$ a prime of $\mathcal{O}_L$ above $\mathfrak{q}$. Then $e(\mathfrak{Q} \mid \mathfrak{q}) = p-1$.*

Proof. We have $e(\mathfrak{Q} \mid p) = p - 1$ by 105, and $k/\mathbb{Q}$ is unramified at p since $p \nmid m$. □

Lemma 56. *Let $\mathfrak{q}$ be a prime of $\mathcal{O}_k$ above p and $\mathfrak{Q}$ a prime of $\mathcal{O}_L$ above $\mathfrak{q}$. Then*

$$m \cdot s_\mathfrak{Q}(d) = (p-1)\sum_{j=0}^{f-1} b_j,$$

where $b_j \in \{0, \dots, m-1\}$ represents the image of $(\mathfrak{q}, j)$ under the bijection of 53.

Proof. The group $\mathrm{Gal}(L/F)$ acts transitively on the primes of $\mathcal{O}_L$ above p, since F has a single prime above p. Choose $\tau \in \mathrm{Gal}(L/F)$ with $\tau(\mathfrak{P}) = \mathfrak{Q}$ and let $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ be the image of $\mathfrak{n}(\tau^{-1})$ (29). The restriction of τ to k is σ_a^{-1}, so $\sigma_a^{-1}(\mathfrak{p}) = \mathfrak{q}$. By 41 and 33, $s_\mathfrak{Q}(d) = s_\mathfrak{P}(da)$, and we conclude with 47 and 54. □

Lemma 57. *Let $\Gamma \in \mathcal{O}_k$ with $g_d^m = \Gamma$ (50). Then*

$$(\Gamma) = \mathfrak{p}^\Theta$$

as ideals of $\mathcal{O}_k$.

Proof. Since $\mathcal{O}_L$ is faithfully flat over $\mathcal{O}_k$, it suffices to compare the extensions of both sides to $\mathcal{O}_L$. By 51, the ideal $(\Gamma)\mathcal{O}_L = (g_d)^m$ is $\prod_{\mathfrak{Q}\mid p} \mathfrak{Q}^{m s_\mathfrak{Q}(d)}$. Regrouping the factors of $\mathfrak{p}^\Theta$ with 53 and using $e(\mathfrak{Q} \mid \mathfrak{q}) = p - 1$ (55), the extension of $\mathfrak{p}^\Theta$ is $\prod_{\mathfrak{q}\mid p}\prod_{\mathfrak{Q}\mid\mathfrak{q}} \mathfrak{Q}^{(p-1)\sum_j b_j}$, with the notation of 56. The exponents agree by 56. □

4.6 Stickelberger's theorem

Lemma 58. *In the setting of this chapter, the ideal $\mathfrak{p}^\Theta$ of $\mathcal{O}_k$ is principal.*

Proof. Choose a maximal ideal $\mathfrak{P}$ of $\mathcal{O}_L$ above $\mathfrak{p}$ and let $P = \mathfrak{P} \cap \mathcal{O}_K$. The ideal P has Teichmüller lifts of order $q-1$ by 2. Take Γ as in 50; then $\mathfrak{p}^\Theta = (\Gamma)$ by 57. □

Theorem 59. *Let k be a number field isomorphic to $\mathbb{Q}(\zeta_m)$, let p be an odd prime with $p \nmid m$ and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_k$ above p. Then the ideal $\mathfrak{p}^\Theta$ is principal.*

Proof. Let f be the order of p modulo m and $q = p^f$. The field $L = \mathbb{Q}(\zeta_{p(q-1)})$ contains a subfield $k_0 = \mathbb{Q}(\zeta_m)$, and an isomorphism $k_0 \cong k$ commutes with the action of the σ_a. Apply 58 to the preimage of $\mathfrak{p}$ in $\mathcal{O}_{k_0}$ and transport the result to k. □

Lemma 60. *Let R be a Dedekind domain and J a nonzero ideal of R. Every ideal class of R contains an integral ideal coprime to J.*

Proof. Let I_0 be an integral ideal in the inverse class. By the Chinese remainder theorem, there is $x \in I_0$ such that $(x)I_0^{-1}$ is coprime to J, and this ideal lies in the given class. □

Corollary 61. *Let k be a number field isomorphic to $\mathbb{Q}(\zeta_m)$. The Stickelberger element Θ annihilates the ideal class group $\mathrm{Cl}(k)$: for every ideal class c,*

$$c^\Theta = \prod_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \sigma_a^{-1}(c)^a = 1.$$

Proof. By 60, choose an integral ideal $\mathfrak{b} \in c$ coprime to $2m$. Every prime factor of $\mathfrak{b}$ lies above an odd prime not dividing m, so 59 applied to each prime factor shows that $\mathfrak{b}^\Theta$ is principal. Hence $c^\Theta = [\mathfrak{b}^\Theta] = 1$. □

Remark 3. Mathematically, coprimality of the representative to m alone suffices for Stickelberger's theorem. We additionally require the norm to be odd (i.e. coprimality to $2m$) only because the formalized form of 59 is proved for primes of odd residue characteristic.

Chapter 5

The Kronecker-Weber theorem

Throughout this chapter, all number fields are subfields of a fixed field A of characteristic 0, and for every $n \geq 1$ we fix a primitive n-th root of unity $\zeta_n \in A$. Thus $\mathbb{Q}(\zeta_n)$ is a well-defined subfield of A, and $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_{n'}) = \mathbb{Q}(\zeta_{\mathrm{lcm}(n,n')})$. The compositum of two subfields K, K' of A is written KK'.

Definition 62. Let p be a prime. A number field K is *unramified outside p* if every prime number $q \neq p$ is unramified in K.

Lemma 63. *If K and F are number fields unramified outside p, then so is KF.*

Proof. A prime q that is unramified in K and in F is unramified in KF (Mathlib PR #36843). □

5.1 Reduction to the cyclic case

Theorem 64. *Let K be a number field such that $K/\mathbb{Q}$ is abelian. Then there exists n such that K embeds into the cyclotomic field $\mathbb{Q}(\zeta_n)$.*

Proof. Take for A an algebraic closure of K, and choose a primitive n-th root of unity in A for every $n \geq 1$. The image of K in A is an abelian extension of $\mathbb{Q}$, so by 66 it lies in $\mathbb{Q}(\zeta_n)$ for some $n \geq 1$. The field $\mathbb{Q}(\zeta_n)$ is isomorphic to the abstract cyclotomic field of level n. □

Lemma 65. *Every finite abelian extension K/F is the compositum of finitely many subextensions C_i/F, each of which is cyclic of prime power degree.*

Proof. The group $\mathrm{Gal}(K/F)$ is a finite abelian group, hence a direct product of cyclic groups of prime power order. Each factor corresponds to a cyclic subextension of prime power degree, and K is their compositum. □

Lemma 66. *Let $K \subseteq A$ be a number field with $K/\mathbb{Q}$ abelian. Then $K \subseteq \mathbb{Q}(\zeta_n)$ for some $n \geq 1$.*

Proof. By 65, the field K is the compositum of finitely many cyclic subextensions C_i of prime power degree. By 67, each C_i lies in some $\mathbb{Q}(\zeta_{n_i})$. By induction on the number of factors, K lies in $\mathbb{Q}(\zeta_n)$ with n the least common multiple of the n_i. □

Lemma 67. *Let p be a prime and $K \subseteq A$ a cyclic extension of $\mathbb{Q}$ of degree p^m. Then $K \subseteq \mathbb{Q}(\zeta_n)$ for some $n \geq 1$.*

Proof. By 79, there are a cyclic extension $F/\mathbb{Q}$ of degree p^k, unramified outside p, and an integer $n \geq 1$ with $K\mathbb{Q}(\zeta_n) = F\mathbb{Q}(\zeta_n)$. The field F lies in some $\mathbb{Q}(\zeta_c)$: take $c = 1$ if $k = 0$, use 104 if $p = 2$, and 97 if p is odd and $k > 0$. Then

$$K \subseteq K\mathbb{Q}(\zeta_n) = F\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_c)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\mathrm{lcm}(c,n)}).$$

□

5.2 Removing the ramification away from p

5.2.1 Tame ramification

In this subsection, G is a finite group acting on a Dedekind domain S by ring automorphisms, $R = S^G$ is the ring of invariants, and Q is a nonzero maximal ideal of S with finite residue field S/Q. Let $\mathfrak{p} = Q \cap R$ and $N\mathfrak{p} = \#(R/\mathfrak{p})$. The decomposition group $D(Q)$ is the stabilizer of Q in G, and the inertia group $I(Q) \subseteq D(Q)$ is the subgroup of elements acting trivially on S/Q. We say that Q is *tame* if $\#I(Q)$ is not zero in S/Q. Every element of $D(Q)$ preserves Q and Q^2, hence acts on the cotangent space Q/Q^2, which is a one-dimensional S/Q-vector space.

Definition 68. An element $\tau \in I(Q)$ acts trivially on S/Q, so it acts on Q/Q^2 by an S/Q-linear automorphism. The *tame character* is the determinant of this action,

$$\theta : I(Q) \to (S/Q)^\times, \qquad \theta(\tau) = \det(\tau \mid Q/Q^2).$$

It is a group homomorphism because the determinant is multiplicative.

Lemma 69. *For $\tau \in I(Q)$ and $v \in Q/Q^2$, one has $\tau v = \theta(\tau)v$.*

Proof. A linear endomorphism of a one-dimensional vector space is multiplication by its determinant. □

Lemma 70 (Rigidity)**.** *Assume that G acts faithfully on S. Let $\tau \in I(Q)$ be such that the order m of τ is not zero in S/Q and $\theta(\tau) = 1$. Then $\tau = 1$.*

Proof. Since $\theta(\tau) = 1$ and Q/Q^2 is one-dimensional, τ acts trivially on Q/Q^2, that is, $\tau x - x \in Q^2$ for all $x \in Q$. From the identity

$$\tau(xy) - xy = (\tau x - x)\,\tau y + x\,(\tau y - y)$$

and induction on n, one gets $\tau x - x \in Q^{n+1}$ for every $x \in Q^n$.

We now show by induction on n that $\delta = \tau x - x$ lies in Q^n for every $x \in S$. Assume that $\delta \in Q^n$. By the previous step, $\tau^k\delta \equiv \delta \pmod{Q^{n+1}}$ for all k. The sum $\sum_{k=0}^{m-1} \tau^k\delta$ telescopes to $\tau^m x - x = 0$, so $m\delta \in Q^{n+1}$. As m is a unit modulo Q, it is a unit modulo Q^{n+1}, hence $\delta \in Q^{n+1}$.

By Krull's intersection theorem, $\bigcap_n Q^n = 0$, so $\tau x = x$ for every $x \in S$. The action being faithful, $\tau = 1$. □

Lemma 71. *Assume that G acts faithfully on S and that Q is tame. Then θ is injective, and the inertia group $I(Q)$ is cyclic.*

Proof. The order of every $\tau \in I(Q)$ divides $\#I(Q)$, so it is not zero in S/Q. Hence θ is injective by 70. Thus $I(Q)$ embeds into the multiplicative group of the finite field S/Q, and a finite subgroup of the multiplicative group of a field is cyclic. □

Lemma 72. *Let $\sigma \in D(Q)$ be an arithmetic Frobenius, that is, $\sigma(x) \equiv x^{N\mathfrak{p}} \pmod{Q}$ for all $x \in S$. Then $\theta(\sigma\tau\sigma^{-1}) = \theta(\tau)^{N\mathfrak{p}}$ for all $\tau \in I(Q)$.*

Proof. The inertia group is normal in $D(Q)$, so $\sigma\tau\sigma^{-1} \in I(Q)$. The action of σ on Q/Q^2 is semilinear: $\sigma(cv) = \sigma(c)\sigma(v)$ for $c \in S/Q$. Using 69, for every $v \in Q/Q^2$,

$$\sigma\tau\sigma^{-1}v = \sigma\big(\theta(\tau)\,\sigma^{-1}v\big) = \sigma(\theta(\tau))\,v = \theta(\tau)^{N\mathfrak{p}}\,v.$$

□

Lemma 73. *Assume moreover that G is abelian and acts faithfully on S, and that Q is tame. Then $\#I(Q)$ divides $N\mathfrak{p} - 1$.*

Proof. Let τ generate the cyclic group $I(Q)$ (71) and let σ be an arithmetic Frobenius at Q, which exists since $R = S^G$. As G is abelian, $\sigma\tau\sigma^{-1} = \tau$, so 72 gives $\theta(\tau)^{N\mathfrak{p}-1} = 1$. Since θ is injective, $\tau^{N\mathfrak{p}-1} = 1$ and the order $\#I(Q)$ of τ divides $N\mathfrak{p} - 1$. □

When $S = \mathcal{O}_L$ for a Galois extension of number fields L/K and $G = \mathrm{Gal}(L/K)$, the order of $I(Q)$ is the ramification index $e(Q \mid \mathfrak{p})$. In particular, if Q lies above the prime number q and $q \nmid \#G$, then Q is tame (`Ideal.card_inertia_notMem_of_not_dvd`).

5.2.2 Abhyankar's lemma and the inertia field

Lemma 74. *Let H_1, H_2 be subgroups of a finite cyclic group C with $H_1 \cap H_2 = 1$. Then $\#C$ divides $\mathrm{lcm}([C : H_1], [C : H_2])$.*

Proof. The map $C \to C/H_1 \times C/H_2$ is injective, and the exponent of the target divides the least common multiple of the two orders. A cyclic group has order equal to its exponent. □

Lemma 75 (Tame Abhyankar)**.** *Let $K/\mathbb{Q}$ be a finite Galois extension, E, F two Galois subextensions with $EF = K$, and $\mathfrak{P}$ a prime of K above a prime number p with $p \nmid [K : \mathbb{Q}]$. Then*

$$e(\mathfrak{P} \mid p) \;\big|\; \mathrm{lcm}\,\big(e(\mathfrak{P} \cap E \mid p),\ e(\mathfrak{P} \cap F \mid p)\big).$$

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and $I = I(\mathfrak{P}) \subseteq G$. As $p \nmid \#G$, the prime $\mathfrak{P}$ is tame, so I is cyclic by 71, of order $e(\mathfrak{P} \mid p)$. Write $H_E = \mathrm{Gal}(K/E)$ and $H_F = \mathrm{Gal}(K/F)$. The group $I \cap H_E$ is the inertia group of $\mathfrak{P}$ in K/E, so the multiplicativity of ramification indices in $\mathbb{Q} \subseteq E \subseteq K$ gives $[I : I \cap H_E] = e(\mathfrak{P} \cap E \mid p)$, and likewise for F. Since $EF = K$, we have $H_E \cap H_F = 1$, and 74 applies to $I \cap H_E$ and $I \cap H_F$. □

Lemma 76 (Tame inertia complement)**.** *Let $L/\mathbb{Q}$ be a finite abelian extension, and let $K, E \subseteq L$ be subfields with $KE = L$, $[K : \mathbb{Q}] = p^m$ and $E \cong \mathbb{Q}(\zeta_q)$, where $q \neq p$ are primes and $q \nmid [L : \mathbb{Q}]$. Let $\mathfrak{Q}$ be a prime of L above q. Then the inertia group $I = I(\mathfrak{Q}) \subseteq \mathrm{Gal}(L/\mathbb{Q})$ is a complement of $\mathrm{Gal}(L/E)$: one has $I \cap \mathrm{Gal}(L/E) = 1$ and $\#I \cdot \#\mathrm{Gal}(L/E) = [L : \mathbb{Q}]$.*

Proof. We first show that $e(\mathfrak{Q} \mid q) = q - 1$. By 75, $e(\mathfrak{Q} \mid q)$ divides the least common multiple of $e(\mathfrak{Q} \cap K \mid q)$ and $e(\mathfrak{Q} \cap E \mid q) = q - 1$. The extension $K/\mathbb{Q}$ is abelian and $q \nmid p^m$, so 73 gives that $e(\mathfrak{Q} \cap K \mid q)$ divides $q - 1$. Hence $e(\mathfrak{Q} \mid q)$ divides $q - 1$. Conversely $q - 1 = e(\mathfrak{Q} \cap E \mid q)$ divides $e(\mathfrak{Q} \mid q)$.

It follows that $e(\mathfrak{Q} \mid \mathfrak{Q} \cap E) = 1$. This ramification index is the order of $I \cap \mathrm{Gal}(L/E)$, the inertia group of $\mathfrak{Q}$ in L/E, so $I \cap \mathrm{Gal}(L/E) = 1$. Finally $\#I \cdot \#\mathrm{Gal}(L/E) = (q-1)[L : E] = [E : \mathbb{Q}][L : E] = [L : \mathbb{Q}]$. □

Lemma 77 (Inertia field from a complement)**.** *Let L/K be a finite Galois extension with group G, let E be an intermediate field, and let I be a normal subgroup of G that is a complement of $\mathrm{Gal}(L/E)$. Then the fixed field $F = L^I$ satisfies $FE = L$, and $G/I \cong \mathrm{Gal}(L/E)$.*

Proof. By the Galois correspondence, FE is the fixed field of $I \cap \mathrm{Gal}(L/E) = 1$, that is, L. The isomorphism $G/I \cong \mathrm{Gal}(L/E)$ is induced by the inclusion of $\mathrm{Gal}(L/E)$ in G. □

Lemma 78. *Let $K \subseteq A$ be a cyclic extension of $\mathbb{Q}$ of degree p^m, and let $q \neq p$ be a prime that ramifies in K. Then there is a cyclic extension $F \subseteq A$ of $\mathbb{Q}$ of p-power degree such that*

- *the prime q is unramified in F;*
- *every prime that is unramified in K is unramified in F;*
- *one has $K\mathbb{Q}(\zeta_q) = F\mathbb{Q}(\zeta_q)$.*

Proof. Put $E = \mathbb{Q}(\zeta_q)$ and $L = KE$. The extension $L/\mathbb{Q}$ is abelian, and $[L : \mathbb{Q}]$ divides $[K : \mathbb{Q}][E : \mathbb{Q}] = p^m(q-1)$, so $q \nmid [L : \mathbb{Q}]$. Fix a prime $\mathfrak{Q}$ of L above q, with inertia group $I \subseteq \mathrm{Gal}(L/\mathbb{Q})$. By 76, the group I is a complement of $\mathrm{Gal}(L/E)$. Let $F = L^I$ be the inertia field of $\mathfrak{Q}$. By 77, we get $FE = L = KE$ and

$$\mathrm{Gal}(F/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/I \cong \mathrm{Gal}(L/E).$$

Restriction to K is injective on $\mathrm{Gal}(L/E)$, since $KE = L$. Hence $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to a subgroup of the cyclic group $\mathrm{Gal}(K/\mathbb{Q})$, so it is cyclic of order dividing p^m.

The prime q is unramified in the inertia field F (Mathlib PR #36733). Let q' be a prime unramified in K. Then $q' \neq q$, so q' is also unramified in $E = \mathbb{Q}(\zeta_q)$, hence in the compositum $L = KE$ (Mathlib PR #36843), and finally in the subfield F of L. □

Lemma 79. *Let $K \subseteq A$ be a cyclic extension of $\mathbb{Q}$ of degree p^m. Then there exist a cyclic extension $F \subseteq A$ of $\mathbb{Q}$ of p-power degree, unramified outside p, and an integer $n \geq 1$ such that $K\mathbb{Q}(\zeta_n) = F\mathbb{Q}(\zeta_n)$.*

Proof. Let S be the finite set of prime divisors of the discriminant of K. Every prime $q \neq p$ outside S is unramified in K. We prove the statement by induction on S, for all cyclic extensions K of p-power degree in which every prime $q \neq p$ outside S is unramified.

If S is empty, take $F = K$ and $n = 1$. Otherwise write $S = \{r\} \cup S'$. If $r = p$, or if r is unramified in K, the induction hypothesis applies to K and S'. Otherwise 78 gives a cyclic extension E of p-power degree, unramified at r and at every prime unramified in K, with $K\mathbb{Q}(\zeta_r) = E\mathbb{Q}(\zeta_r)$. The induction hypothesis applied to E and S' gives F and n with $E\mathbb{Q}(\zeta_n) = F\mathbb{Q}(\zeta_n)$. Then

$$K\mathbb{Q}(\zeta_{\mathrm{lcm}(n,r)}) = K\mathbb{Q}(\zeta_r)\mathbb{Q}(\zeta_n) = E\mathbb{Q}(\zeta_r)\mathbb{Q}(\zeta_n) = F\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_r) = F\mathbb{Q}(\zeta_{\mathrm{lcm}(n,r)}).$$

□

5.3 Comparing cyclic extensions

Lemma 80. *Let $K, K' \subseteq A$ be number fields such that $KK'/\mathbb{Q}$ is Galois with cyclic Galois group. If $[K : \mathbb{Q}]$ divides $[K' : \mathbb{Q}]$, then $K \subseteq K'$.*

Proof. Let $G = \mathrm{Gal}(KK'/\mathbb{Q})$. By the Galois correspondence, it suffices to show that $\mathrm{Gal}(KK'/K') \subseteq \mathrm{Gal}(KK'/K)$. In the cyclic group G, a subgroup is contained in another if and only if its order divides the order of the other. The orders are $[KK' : K'] = [KK' : \mathbb{Q}]/[K' : \mathbb{Q}]$ and $[KK' : K] = [KK' : \mathbb{Q}]/[K : \mathbb{Q}]$, and the first divides the second since $[K : \mathbb{Q}]$ divides $[K' : \mathbb{Q}]$. □

Lemma 81. *Let $C \subseteq A$ be an abelian extension of $\mathbb{Q}$, unramified outside p, and let H be a subgroup of $\mathrm{Gal}(C/\mathbb{Q})$ of index p^m with cyclic quotient. Then the fixed field C^H is a cyclic extension of $\mathbb{Q}$ of degree p^m, unramified outside p.*

Proof. By the Galois correspondence, $[C^H : \mathbb{Q}] = [\mathrm{Gal}(C/\mathbb{Q}) : H] = p^m$ and $\mathrm{Gal}(C^H/\mathbb{Q}) \cong \mathrm{Gal}(C/\mathbb{Q})/H$, which is cyclic. A subfield of C is unramified outside p because C is. □

Lemma 82. *Let $K, K' \subseteq A$ be abelian extensions of $\mathbb{Q}$ of the same degree p^m, both unramified outside p. Assume that any two cyclic subextensions of KK' of degree p over $\mathbb{Q}$ and unramified outside p are equal. Then $K = K'$.*

Proof. The group $\mathrm{Gal}(KK'/\mathbb{Q})$ is an abelian p-group, since $[KK' : \mathbb{Q}]$ divides p^{2m}. If it were not cyclic, it would have two distinct subgroups of index p. Their fixed fields would be two distinct cyclic subfields of KK' of degree p, unramified outside p by 63, a contradiction. So $KK'/\mathbb{Q}$ is cyclic, and 80 gives $K \subseteq K'$. The degrees being equal, $K = K'$. □

5.4 The odd case

5.4.1 The Kummer extension

In this subsection, p is an odd prime and F is a number field with $F \cong \mathbb{Q}(\zeta_p)$.

Lemma 83. *Let L/F be a finite extension such that $L/\mathbb{Q}$ is Galois and $[L : \mathbb{Q}] = p(p-1)$. Then L/F is Galois, cyclic of degree p.*

Proof. Since $[F : \mathbb{Q}] = p - 1$, the tower formula gives $[L : F] = p$. The extension L/F is Galois as $L/\mathbb{Q}$ is, and a group of prime order is cyclic. □

Lemma 84. *Let L/F be a cyclic extension of degree p. Then there is a nonzero $\mu \in \mathcal{O}_F$ such that L is the splitting field of $X^p - \mu$ over F.*

Proof. The field F contains the p-th roots of unity, so by Kummer theory $L = F(\alpha)$ with $\alpha^p = x \in F$. Choose a nonzero integer d with $dx \in \mathcal{O}_F$. Then $\mu = d^p x$ lies in $\mathcal{O}_F$, the element $d\alpha$ is a root of $X^p - \mu$, and $L = F(d\alpha)$ is the splitting field of $X^p - \mu$. Finally $\mu \neq 0$, since otherwise $L = F$. □

For the rest of this subsection, L/F is a cyclic extension of degree p with $L/\mathbb{Q}$ abelian, and $\mu \in \mathcal{O}_F$ is nonzero, with $X^p - \mu$ irreducible over F and L the splitting field of $X^p - \mu$. For $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we write σ_a for the element of $\mathrm{Gal}(F/\mathbb{Q})$ with $\sigma_a(\zeta) = \zeta^a$ for every p-th root of unity ζ, and we identify a with its representative in $\{1, \dots, p-1\}$.

Lemma 85. *There is a nonzero $\alpha \in \mathcal{O}_L$ with $\alpha^p = \mu$.*

Proof. Take a root $\alpha \in L$ of $X^p - \mu$. It is integral since $\alpha^p = \mu$ is, and nonzero since $L \neq F$. □

Lemma 86. *For every $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, there is a nonzero $\xi \in F$ with $\sigma_a(\mu) = \xi^p \mu^a$.*

Proof. Let $\alpha \in L$ be a root of $X^p - \mu$, let τ generate $\mathrm{Gal}(L/F)$ and write $\tau(\alpha) = \zeta\alpha$, with ζ a primitive p-th root of unity. Extend σ_a to $\tilde{\sigma} \in \mathrm{Gal}(L/\mathbb{Q})$. As $\tilde{\sigma}(\alpha)^p = \sigma_a(\mu) \in F$, Kummer theory gives $\tilde{\sigma}(\alpha) = c\alpha^j$ with $c \in F$ and $0 \leq j < p$. Since $L/\mathbb{Q}$ is abelian, $\tilde{\sigma}\tau = \tau\tilde{\sigma}$. Applying both sides to α gives $\zeta^a c\alpha^j = c\zeta^j\alpha^j$, so $j = a$. Therefore $\sigma_a(\mu) = \tilde{\sigma}(\alpha)^p = c^p\mu^a$. □

Lemma 87. *Let $\mathfrak{q}$ be a prime of $\mathcal{O}_F$ such that $p \nmid v_\mathfrak{q}(\mu)$. Then every $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ with $\sigma(\mathfrak{q}) = \mathfrak{q}$ is the identity.*

Proof. Write $\sigma = \sigma_a$ and $r = v_{\mathfrak{q}}(\mu)$. By 86, $\sigma(\mu) = \xi^p \mu^a$. Choose a nonzero integer d such that $\beta = d\xi$ lies in $\mathcal{O}_F$; then $\sigma(d^p\mu) = \beta^p \mu^a$. Since $\sigma(\mathfrak{q}) = \mathfrak{q}$, the valuations at $\mathfrak{q}$ of $\sigma(x)$ and x agree, so

$$p\, v_{\mathfrak{q}}(d) + r = p\, v_{\mathfrak{q}}(\beta) + ar.$$

Reducing modulo p gives $r \equiv ar \pmod{p}$. As $p \nmid r$, this forces $a \equiv 1 \pmod{p}$, that is, $\sigma = 1$. □

Lemma 88. *Assume that L is unramified outside p. Then $p \mid v_{\mathfrak{q}}(\mu)$ for every prime $\mathfrak{q}$ of $\mathcal{O}_F$.*

Proof. Let q be the prime number below $\mathfrak{q}$.

Assume first that $q = p$. The prime p is totally ramified in F, so the stabilizer of $\mathfrak{q}$ in $\mathrm{Gal}(F/\mathbb{Q})$ has order $e(\mathfrak{q} \mid p) f(\mathfrak{q} \mid p) = p - 1 > 1$, as p is odd. It contains some $\sigma \neq 1$, and 87 gives $p \mid v_{\mathfrak{q}}(\mu)$.

Assume now that $q \neq p$, and let $\mathfrak{Q}$ be a prime of L above $\mathfrak{q}$. The prime q is unramified in L and in F, so $e(\mathfrak{Q} \mid \mathfrak{q}) = 1$. Let $\alpha \in \mathcal{O}_L$ with $\alpha^p = \mu$ (85). Then

$$v_{\mathfrak{q}}(\mu) = e(\mathfrak{Q} \mid \mathfrak{q})\, v_{\mathfrak{q}}(\mu) = v_{\mathfrak{Q}}(\mu) = v_{\mathfrak{Q}}(\alpha^p) = p\, v_{\mathfrak{Q}}(\alpha).$$

□

Lemma 89. *Assume that L is unramified outside p. Then $(\mu) = \mathfrak{a}^p$ for some nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_F$.*

Proof. By 88, write $v_{\mathfrak{q}}(\mu) = p\, n_{\mathfrak{q}}$ for every prime $\mathfrak{q}$, and take $\mathfrak{a} = \prod_{\mathfrak{q}} \mathfrak{q}^{n_{\mathfrak{q}}}$. □

5.4.2 The class group argument

We keep the setting of the previous subsection.

Lemma 90. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_F$ with $\mathfrak{a}^p = (\mu)$. Then $\mathfrak{a}$ is principal.*

Proof. Let c be the class of $\mathfrak{a}$ in $\mathrm{Cl}(F)$. Since $\mathfrak{a}^p = (\mu)$ is principal, $c^p = 1$.

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. By 86, $\sigma_a(\mu) = \xi^p \mu^a$ with $\xi \in F^\times$. Hence, as fractional ideals,

$$\sigma_a(\mathfrak{a})^p = \sigma_a((\mu)) = (\xi)^p\, (\mu)^a = \left((\xi)\, \mathfrak{a}^a\right)^p,$$

and since the group of fractional ideals is torsion-free, $\sigma_a(\mathfrak{a}) = (\xi)\mathfrak{a}^a$. Thus $\sigma_a(c) = c^a$.

By 61, applied to $F \cong \mathbb{Q}(\zeta_p)$,

$$1 = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \sigma_a^{-1}(c)^a = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} c^{a^{-1}a} = c^{p-1},$$

where $\sigma_a^{-1} = \sigma_{a^{-1}}$ and $c^{a^{-1}a} = c$ because $c^p = 1$. Together with $c^p = 1$, this gives $c = 1$. □

Lemma 91. *Let $\mathfrak{a}$ be a nonzero principal ideal of $\mathcal{O}_F$ with $\mathfrak{a}^p = (\mu)$. Then $\mu = \alpha^p \eta$ for some nonzero $\alpha \in \mathcal{O}_F$ and some unit $\eta \in \mathcal{O}_F^\times$.*

Proof. Write $\mathfrak{a} = (\alpha)$. Then $(\alpha^p) = (\mu)$, so $\mu = \alpha^p \eta$ with η a unit, and $\alpha \neq 0$ since $\mu \neq 0$. □

Lemma 92. *Let $\alpha \in \mathcal{O}_F$ and $\eta \in \mathcal{O}_F^\times$ with $\mu = \alpha^p \eta$. Then $\eta\, \sigma_{-1}(\eta)$ is a p-th power in F.*

Proof. By 86 with $a = p - 1$, there is $\xi \in F^\times$ with $\sigma_{-1}(\mu) = \xi^p \mu^{p-1} = (\xi\mu)^p \mu^{-1}$. Substituting $\mu = \alpha^p \eta$,

$$\sigma_{-1}(\alpha)^p\, \sigma_{-1}(\eta) = (\xi\mu)^p\, \alpha^{-p}\, \eta^{-1},$$

whence $\eta\, \sigma_{-1}(\eta) = \left(\xi\mu / (\alpha\, \sigma_{-1}(\alpha))\right)^p$. □

Lemma 93. *Let $\alpha \in \mathcal{O}_F$ and $\eta \in \mathcal{O}_F^\times$ with $\mu = \alpha^p \eta$. Then $\eta^4 = \zeta\, \delta^p$ for some p-th root of unity ζ and some nonzero $\delta \in F$.*

Proof. The field F is a CM field, and the automorphism σ_{-1} is its complex conjugation. Every unit of a CM field has a square of the form $\zeta_0 \varepsilon_0$, with ζ_0 a root of unity and ε_0 a real unit (`NumberField.IsCMField.exists_torsion_realunits_pow_two_eq_mul`). Squaring, $\eta^4 = \zeta\varepsilon$ with $\zeta = \zeta_0^2$ and $\varepsilon = \varepsilon_0^2$. The roots of unity of F form a group of order $2p$, so $\zeta^p = \zeta_0^{2p} = 1$.

The automorphism σ_{-1} fixes ε and inverts ζ, so $\sigma_{-1}(\eta)^4 = \zeta^{-1}\varepsilon$. Multiplying, $\varepsilon^2 = (\eta\, \sigma_{-1}(\eta))^4$. By 92, $\eta\, \sigma_{-1}(\eta) = w^p$, so $\varepsilon^2 = (w^4)^p$. As $\gcd(2, p) = 1$, it follows that $\varepsilon = \delta^p$ for some nonzero $\delta \in F$. □

Lemma 94. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_F$ with $\mathfrak{a}^p = (\mu)$. Then L is the cyclotomic field of level p^2, that is, $L = \mathbb{Q}(\xi)$ for a primitive p^2-th root of unity $\xi \in L$.*

Proof. By 90 and 91, $\mu = \alpha^p \eta$ with $\alpha \neq 0$ and η a unit, and by 93, $\eta^4 = \zeta\delta^p$. As $\gcd(4, p) = 1$, the polynomial $X^p - \mu^4$ is irreducible over F and L is its splitting field. Since $\mu^4 = \zeta(\alpha^4\delta)^p$, the field L is also the splitting field of $X^p - \zeta$. In particular $\zeta \neq 1$, since otherwise $L = F$, so ζ is a primitive p-th root of unity. A root $\xi \in L$ of $X^p - \zeta$ is then a primitive p^2-th root of unity. Finally $\mathbb{Q}(\xi) \subseteq L$ and both fields have degree $p(p-1)$ over $\mathbb{Q}$, so $L = \mathbb{Q}(\xi)$. □

5.4.3 Cyclic extensions of odd prime power degree

Proposition 95. *Let p be an odd prime and $K \subseteq A$ a cyclic extension of $\mathbb{Q}$ of degree p, unramified outside p. Then $K \subseteq \mathbb{Q}(\zeta_{p^2})$.*

Proof. Put $F = \mathbb{Q}(\zeta_{p^2}^p)$, so that $F \cong \mathbb{Q}(\zeta_p)$, and $M = KF$. The field F is unramified outside p, hence so is M by 63, and $M/\mathbb{Q}$ is abelian. Since $[K : \mathbb{Q}] = p$ and $[F : \mathbb{Q}] = p - 1$ are coprime, $K \cap F = \mathbb{Q}$ and $[M : \mathbb{Q}] = p(p-1)$. By 83, the extension M/F is cyclic of degree p, and by 84, M is the splitting field of $X^p - \mu$ for some nonzero $\mu \in \mathcal{O}_F$. The polynomial $X^p - \mu$ is irreducible: otherwise μ would be a p-th power in F, and $X^p - \mu$ would split over F, giving $M = F$.

By 89, $(\mu) = \mathfrak{a}^p$ with $\mathfrak{a} \neq 0$. By 94, the field M is the cyclotomic field of level p^2, so $M = \mathbb{Q}(\zeta_{p^2})$. Hence $K \subseteq M = \mathbb{Q}(\zeta_{p^2})$. □

Corollary 96. *Let p be an odd prime. Any two cyclic extensions $K_1, K_2 \subseteq A$ of $\mathbb{Q}$ of degree p, unramified outside p, are equal.*

Proof. By 95, both fields lie in $\mathbb{Q}(\zeta_{p^2})$, which has degree $p(p-1)$. So $[K_1K_2 : K_1] \leq p - 1$. As $K_2/\mathbb{Q}$ is Galois, $[K_1K_2 : K_1]$ divides $[K_2 : \mathbb{Q}] = p$, hence $[K_1K_2 : K_1] = 1$ and $K_2 \subseteq K_1$. The degrees being equal, $K_1 = K_2$. □

Proposition 97. *Let p be an odd prime, $m \geq 1$, and $K \subseteq A$ an abelian extension of $\mathbb{Q}$ of degree p^m, unramified outside p. Then $K \subseteq \mathbb{Q}(\zeta_{p^{m+1}})$.*

Proof. Put $C = \mathbb{Q}(\zeta_{p^{m+1}})$. It is unramified outside p, and since p is odd, $\mathrm{Gal}(C/\mathbb{Q}) \cong (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$ is cyclic of order $p^m(p-1)$. Let σ be a generator and $H = \langle \sigma^{p^m} \rangle$, a subgroup of index p^m with cyclic quotient. By 81, the field $K' = C^H$ is a cyclic extension of $\mathbb{Q}$ of degree p^m, unramified outside p. By 96, the hypothesis of 82 holds, so $K = K' \subseteq C$. □

5.5 The case $p = 2$

The argument follows Lemmermeyer (Prop. 1.5) and does not need the Kummer theory of the odd case.

Lemma 98. *A quadratic field unramified outside* 2 *has discriminant* -8, -4 *or* 8.

Proof. Let d be the discriminant. A prime number divides d if and only if it ramifies, so 2 is the only possible prime divisor of d. The discriminant of a quadratic field is a fundamental discriminant (Mathlib PR #43490), so $d \equiv 0$ or $1 \pmod 4$.

If $d \equiv 1 \pmod 4$, then d is odd. By Minkowski's bound $|d| > 2$, so d has a prime divisor, which is odd: a contradiction. Hence $d = 4m$. Since $4m$ is a fundamental discriminant, the integer m is squarefree and $m \not\equiv 1 \pmod 4$. As the only prime dividing m is 2, this leaves $m \in \{-1, 2, -2\}$, that is, $d \in \{-4, 8, -8\}$. □

Proposition 99. *Any two totally real quadratic fields* $K_1, K_2 \subseteq A$ *unramified outside* 2 *are equal.*

Proof. By 98, each discriminant is -8, -4 or 8. The discriminant of a totally real quadratic field is positive (Mathlib PR #43493), so both discriminants equal 8. Two quadratic fields with the same discriminant are isomorphic (Mathlib PR #43490), and a quadratic field is normal over $\mathbb{Q}$, so $K_1 = K_2$ as subfields of A. □

Lemma 100. *Let* $L \subseteq A$ *be a CM field with complex conjugation* $c \in \mathrm{Gal}(L/\mathbb{Q})$. *Then its maximal real subfield* L^+ *is the fixed field of* $\langle c \rangle$.

Proof. An element of L lies in L^+ if and only if it is fixed by c. Since c has order 2, being fixed by c is the same as being fixed by $\langle c \rangle$. □

Lemma 101. *Under the isomorphism* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, *complex conjugation corresponds to* -1.

Proof. Complex conjugation sends every root of unity to its inverse, so it sends ζ_n to $\zeta_n^{-1} = \zeta_n^{n-1}$. □

Lemma 102. *For every* $n \geq 0$, *the quotient* $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times/\langle -1 \rangle$ *is cyclic.*

Proof. The subgroups generated by 5 and by -1 are complementary in $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times$, so the quotient is isomorphic to the cyclic group generated by 5. □

Proposition 103. *Let* $K \subseteq A$ *be a totally real cyclic extension of* $\mathbb{Q}$ *of degree* 2^m, *unramified outside* 2. *Then* $K \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$.

Proof. Put $C = \mathbb{Q}(\zeta_{2^{m+2}})$, a CM field unramified outside 2, and let c be its complex conjugation. The subgroup $\langle c \rangle$ has order 2, hence index 2^m in $\mathrm{Gal}(C/\mathbb{Q})$. By 101, the quotient $\mathrm{Gal}(C/\mathbb{Q})/\langle c \rangle$ is isomorphic to $(\mathbb{Z}/2^{m+2}\mathbb{Z})^\times/\langle -1 \rangle$, which is cyclic by 102. By 81 and 100, the maximal real subfield $K' = C^+$ is a cyclic extension of $\mathbb{Q}$ of degree 2^m, unramified outside 2, and it is totally real.

The compositum KK' is totally real, so every subfield of KK' is totally real. By 99, any two quadratic subfields of KK' unramified outside 2 are equal. Hence 82 gives $K = K' \subseteq C$. □

Proposition 104. *Let* $K \subseteq A$ *be a cyclic extension of* $\mathbb{Q}$ *of degree* 2^m, *unramified outside* 2. *Then* $K \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$.

Proof. If K is totally real, this is 103. Otherwise let $L = K\mathbb{Q}(i)$, with $i = \zeta_4$. It is a totally complex abelian extension of $\mathbb{Q}$, unramified outside 2 by 63, of degree 2^l with $l \leq m+1$; it is a CM field. Let $M = L^+$ be its maximal real subfield, of degree 2^k with $k \leq l$. As L is totally complex, $M \neq L$, so $k \leq m$. The field M is abelian and unramified outside 2.

The field M is cyclic over $\mathbb{Q}$. Indeed, $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q})/\langle c \rangle$, where c is the complex conjugation of L. The restriction map $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ is injective, so $\mathrm{Gal}(M/\mathbb{Q})$ embeds into the quotient of $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ by the image of $\langle c \rangle$. The restriction of c to $\mathbb{Q}(i)$ generates $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, so this quotient is generated by the image of the cyclic group $\mathrm{Gal}(K/\mathbb{Q}) \times 1$. Hence it is cyclic, and so is $\mathrm{Gal}(M/\mathbb{Q})$.

By 103, $M \subseteq \mathbb{Q}(\zeta_{2^{k+2}})$. Since $[L : M] = 2$ and $i \notin M$, we get $L = M\mathbb{Q}(i)$. Therefore

$$K \subseteq L = M\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_{2^{k+2}})\mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_{2^{m+2}}).$$

□

Chapter 6

Auxiliary results

Lemma 105. *The ramification index of $\mathfrak{P}$ above p is $p-1$, i.e.,*

$$e(\mathfrak{P} \mid p) = p - 1.$$

Proof. This follows from the general formula for the ramification index in cyclotomic extensions. □

Lemma 106. *We have $\zeta_p - 1 \notin \mathfrak{P}^2$.*

Proof. By 105, $e(\mathfrak{P} \mid p) = p-1$. Since ζ_p is a primitive p-th root of unity, $(\zeta_p - 1)$ generates the unique prime above p in $\mathbb{Q}(\zeta_p)$, which has ramification index $p-1$. Hence $v_{\mathfrak{P}}(\zeta_p - 1) = 1$, so $\zeta_p - 1 \notin \mathfrak{P}^2$. □

Lemma 107. *For any additive character ψ of $\mathcal{O}_K/P$,*

$$g(1, \psi) = \begin{cases} q-1 & \text{if } \psi = 1 \\ -1 & \text{otherwise,} \end{cases}$$

where $\psi = 1$ denotes the trivial character (identically equal to 1).

Proof. □