ODD TATE TWISTS

Prerequisites. This chapter continues Chapter 26, *Denominators and the Stickelberger element*, whose notation A, $A^{(i)}$, $A^{\pm}$, ω, σ_a (Section 26.2, with $p = \ell$), Theorem 26.2.2 and Problem 26.2.8 we use. Continuous cohomology of profinite groups [NSW, Ch. I; Ch. II, §7], inflation–restriction, and the vanishing of $H^q(G, M)$, $q \geq 1$, for finite G of order invertible on M [SeL, Ch. VII–VIII]. Decomposition and inertia groups [Ne, Ch. I, §9], and the Artin isomorphism between the ideal class group of a number field and the Galois group of its Hilbert class field [Ne, Ch. VI, §6]. The duality theorems for Galois cohomology of number fields are stated in the text with references. In Sections 27.1 and 27.2, ℓ is an odd prime; $\mathrm{num}(r)$ is the numerator of a rational number r in lowest terms.

27.1. Tate twists over $\mathbb{Q}$

In the previous chapter Bernoulli values gave the orders of odd eigenspaces of a class group. Which Galois cohomology groups account for the numerators and denominators of zeta values? Let $\mathbb{Q}_S$ be the largest extension of $\mathbb{Q}$ unramified outside ℓ and ∞, $G_{\mathbb{Q},\ell} := \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, and $\chi_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$ the cyclotomic character, which factors through $G_{\mathbb{Q},\ell}$. For $k \in \mathbb{Z}$, $\mathbb{Z}_\ell(k)$ is $\mathbb{Z}_\ell$ with σ acting by $\chi_\ell(\sigma)^k$, and similarly for $\mathbb{Q}_\ell(k)$, $\mathbb{Q}_\ell/\mathbb{Z}_\ell(k)$ and $\mathbb{Z}/\ell(k)$. Let $W_e := \mathbb{Q}_\ell/\mathbb{Z}_\ell(-e)$, and let $G_\ell := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, mapped to $G_{\mathbb{Q},\ell}$ by restriction along a fixed embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$.

Definition. The *Tate–Shafarevich group of the twist* e is

$$\mathrm{Sha}_\ell(\mathbb{Q}, e) := \ker\big(H^1(G_{\mathbb{Q},\ell}, W_e) \to H^1(G_\ell, W_e)\big),$$

and $h_{\ell,e}(\mathbb{Q}) \in \{0, 1, 2, \ldots, \infty\}$ is its length as a $\mathbb{Z}_\ell$-module. For a number field E one defines $\mathrm{Sha}_\ell(E, e)$ and $h_{\ell,e}(E)$ in the same way, with the local Galois groups at all primes of E above ℓ.

Problem 27.1.1. If $(\ell - 1) \nmid k$, then $H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k)) = 0$. If $(\ell - 1) \mid k$ and $k \neq 0$, it is cyclic of order $\ell^{1+v_\ell(k)}$. The same holds for G_ℓ in place of $G_{\mathbb{Q},\ell}$.

By von Staudt and Clausen [Wa, Thm. 5.10], the denominator of B_k, $k \geq 2$ even, is the product of the primes p with $(p - 1) \mid k$.

Problem 27.1.2. For even $k \geq 2$, the power of ℓ in the denominator of $\zeta(1-k) = -B_k/k$ is $|H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k))|$.

For even $k \geq 2$, the ℓ-part of the denominator of $\zeta(1 - k)$ is the order of $H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k))$. The ℓ-part of its numerator will be the order of $\mathrm{Sha}_\ell(\mathbb{Q}, k-1)$.

Problem 27.1.3. Let $p \neq \ell$, $e \neq 0$, and $G_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Every unramified class in $H^1(G_p, W_e)$ is zero. Hence $\mathrm{Sha}_\ell(\mathbb{Q}, e)$ is the group of classes in $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), W_e)$ that vanish at every prime.

Let $F := \mathbb{Q}(\zeta_\ell)$.

Date: November 26, 2026.

Problem 27.1.4. Suppose that $(\ell-1) \nmid e$. Then $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}/\ell(-e)) \to H^1(G_{\mathbb{Q},\ell}, W_e)[\ell]$ is an isomorphism, and so is its analogue for G_ℓ. Hence $\mathrm{Sha}_\ell(\mathbb{Q}, e)[\ell]$ is the group of classes in $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}/\ell(-e))$ that vanish on G_ℓ.

Problem 27.1.5. Suppose that $(\ell-1) \nmid e$. Restriction to $\mathrm{Gal}(\mathbb{Q}_S/F)$, followed by the Artin map, identifies the group of Problem 27.1.4 with the group of homomorphisms $\phi\colon A \to \mathbb{F}_\ell$ such that $\phi(\sigma_a z) = \omega(a)^{-e}\phi(z)$, that is, with $\mathrm{Hom}(A^{(-e)}, \mathbb{F}_\ell)$.

Problems 27.1.4 and 27.1.5 prove the following.

Theorem 27.1.1. *Let* $(\ell-1) \nmid e$. *Then* $\mathrm{Sha}_\ell(\mathbb{Q}, e)[\ell] \cong \mathrm{Hom}(A^{(-e)}, \mathbb{F}_\ell)$. *In particular* $\mathrm{Sha}_\ell(\mathbb{Q}, e) = 0$ *if and only if* $A^{(-e)} = 0$.

Problem 27.1.6. Let $e \geq 1$ be odd. Then $\mathrm{Sha}_\ell(\mathbb{Q}, e) \neq 0$ if and only if $\ell \mid \mathrm{num}(B_{e+1}/(e+1))$. For example, $\mathrm{Sha}_{691}(\mathbb{Q}, 11) \neq 0$ and $\mathrm{Sha}_{37}(\mathbb{Q}, 31) \neq 0$.

We state four inputs as black boxes. By Soulé [So], $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ is finite for $k \geq 2$. By Poitou–Tate duality [NSW, Ch. VIII, §6], $\mathrm{Sha}_\ell(\mathbb{Q}, e)$ is dual to the kernel of $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(e+1)) \to H^2(G_\ell, \mathbb{Z}_\ell(e+1))$, and by local duality [NSW, Ch. VII, §2] $H^2(G_\ell, \mathbb{Z}_\ell(k))$ is dual to $H^0(G_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell(1-k))$. By Tate's global Euler characteristic formula [NSW, Ch. VIII, §7], for every finite $G_{\mathbb{Q},\ell}$-module M of ℓ-power order, $|H^0(M)||H^2(M)|/|H^1(M)| = |M^{c=1}|/|M|$, where c is a complex conjugation. Since ℓ is odd, $G_{\mathbb{Q},\ell}$ has ℓ-cohomological dimension at most 2 [NSW, Ch. VIII, §3], so $H^3(G_{\mathbb{Q},\ell}, M) = 0$ for every ℓ-primary M.

Problem 27.1.7. Let $e \geq 1$ be odd. Then $H^2(G_\ell, \mathbb{Z}_\ell(e+1)) = 0$, and $\mathrm{Sha}_\ell(\mathbb{Q}, e)$ is dual to $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(e+1))$.

Problem 27.1.8. Let $k \geq 2$. The $\mathbb{Z}_\ell$-module $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ has rank 1 if k is odd and rank 0 if k is even, and its torsion subgroup is isomorphic to $H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k))$.

The main conjecture of Iwasawa theory, proved by Mazur and Wiles [MW], gives the order; see [Wa, Ch. 15].

Theorem 27.1.2 (Mazur–Wiles)**.** *Let* $e \geq 1$ *be odd. Then*

$$h_{\ell,e}(\mathbb{Q}) = v_\ell\big(\mathrm{num}(B_{e+1}/(e+1))\big).$$

Problem 27.1.9. Let $k \geq 2$ be even. Then

$$\frac{|H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))|}{|H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))|} = |\zeta(1-k)|_\ell^{-1}.$$

For $k = 12$ and $\ell = 691$ both sides are 691.

This is the simplest case of the Bloch–Kato conjecture [BK].

27.2. Odd characters

Over $\mathbb{Q}$ the odd twists are controlled by Bernoulli numbers. How does this look over an abelian field, and what does it say about sums over all ℓ?

Let $E \subseteq \mathbb{Q}(\zeta_\ell)$ and $\Delta_E := \mathrm{Gal}(E/\mathbb{Q})$. Then Δ_E acts on $\mathrm{Sha}_\ell(E, e)$, by $(\delta z)(g) := \tilde{\delta}\, z(\tilde{\delta}^{-1} g \tilde{\delta})$ for a lift $\tilde{\delta}$ of δ, which is the direct sum of its η-parts over the characters η of Δ_E, with values in $\mu_{\ell-1} \subset \mathbb{Z}_\ell^\times$. Let $\mathrm{Sha}_\ell(\mathbb{Q}, e; \eta)$ be defined as $\mathrm{Sha}_\ell(\mathbb{Q}, e)$, with W_e replaced by $W_e \otimes \eta^{-1}$. A character η is *critical for* e if $\eta(-1) = (-1)^{e+1}$, and *plus for* e otherwise. The *minus part* of $\mathrm{Sha}_\ell(E, e)$ is the sum of the η-parts over the critical characters; it is the part on which complex conjugation acts by $(-1)^{e+1}$.

Problem 27.2.1. The η-part of $\mathrm{Sha}_\ell(E,e)$ is isomorphic to $\mathrm{Sha}_\ell(\mathbb{Q},e;\eta)$. In particular $\mathrm{Sha}_\ell(\mathbb{Q},e)$ is the part fixed by Δ_E.

Problem 27.2.2. Let $\eta=\omega^j$ with $(\ell-1)\nmid(e+j)$. Then $\mathrm{Sha}_\ell(\mathbb{Q},e;\eta)[\ell]\cong \mathrm{Hom}(A^{(-e-j)},\mathbb{F}_\ell)$, and η is critical for e if and only if $-e-j$ is odd.

Problem 27.2.3. For every $e\neq 0$, the minus part of $\mathrm{Sha}_\ell(\mathbb{Q}(\zeta_\ell),e)$ has the same ℓ-rank as A^-.

Over $\mathbb{Q}(\zeta_\ell)$ the critical characters account for the ℓ-rank of A^-. Over $\mathbb{Q}$, for each fixed positive odd e, one Bernoulli numerator controls all odd primes.

Problem 27.2.4. For a nonzero integer Y, $\sum_\ell v_\ell(Y)\log\ell\le\log|Y|$. Hence, for odd $e\ge 1$,

$$\sum_{\ell\ \mathrm{odd}} h_{\ell,e}(\mathbb{Q})\log\ell\le\log\Big|\mathrm{num}\Big(\frac{B_{e+1}}{e+1}\Big)\Big|.$$

Problem 27.2.5. For $k\ge 1$, $\log|\mathrm{num}(B_{2k}/2k)|\le 2k\log(2k)+3$.

For the data of Chapter 33, the proof uses a CM subfield of a cyclotomic field and the twists $0\le e<5r$, where r is the target rank of that chapter. The counterpart of Problem 27.2.4 there is Theorem 27.3.2 below. It gives one positive integer X_{odd} of controlled size such that, for every prime ℓ and every coefficient ring $\mathcal{O}$ allowed in the theorem, $v_{\mathcal{O}}(X_{\mathrm{odd}})$ bounds the $\mathcal{O}$-length of the module of cocycles of Definition 27.3.1 at every level n. The argument does not prove the main conjecture.

27.3. Odd cocycles

In this section ℓ is any prime. Fix an embedding $\overline{\mathbb{Q}}\subset\mathbb{C}$, and let $c\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be complex conjugation. Let $E\subset\overline{\mathbb{Q}}$ be a CM field, $G_E:=\mathrm{Gal}(\overline{\mathbb{Q}}/E)$, and $\chi:=\chi_\ell|_{G_E}$. Then $cG_Ec=G_E$ and $\chi(cgc)=\chi(g)$. For a place $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ let $D_{\mathfrak{P}}\supseteq I_{\mathfrak{P}}$ be its decomposition and inertia groups in G_E. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_\ell$, with valuation $v_{\mathcal{O}}$ normalized by $v_{\mathcal{O}}(\pi)=1$ on a uniformizer π and $v_{\mathcal{O}}(0)=\infty$; for $n\ge 0$ let $\mathcal{O}_n:=\mathcal{O}/\ell^n\mathcal{O}$, and write $\mathcal{O}_n(-e)$ for this quotient with $g\in G_E$ acting by $\chi(g)^{-e}$. We write len for length over $\mathcal{O}$, with values in $\{0,1,\dots,\infty\}$.

Definition 27.3.1. For integers $e,n\ge 0$, $\mathrm{Sha}_\ell^{\mathrm{odd}}(E,\mathcal{O};e,n)$ is the $\mathcal{O}$-module of maps $z\colon G_E\to\mathcal{O}_n$ such that:

(a) z is locally constant and $z(gh)=z(g)+\chi(g)^{-e}z(h)$ for all $g,h\in G_E$;
(b) $z=0$ on $I_{\mathfrak{P}}$ for every $\mathfrak{P}$ above a prime other than ℓ;
(c) for every $\mathfrak{P}$ above ℓ: $z=0$ on $I_{\mathfrak{P}}$ if $e=0$, and $z=0$ on $D_{\mathfrak{P}}\cap\ker\chi$ if $e>0$;
(d) if $e>0$, then $z(cgc)=-z(g)$ for all $g\in G_E$.

These are cocycles, not classes: nothing is divided out. In (c) the kernel is that of the ℓ-adic character, not of its reduction modulo ℓ^n. For $e>0$ this module is modelled on the odd part of $\mathrm{Sha}^1(E,\mathcal{O}_n(-e))$; the proof does not compare the two. Problems 27.3.1 and 27.3.2 explain the shape of the definition.

Problem 27.3.1. Let ℓ be odd and $e>0$. For $b\in\mathcal{O}_n$, the coboundary $z_b(g):=(\chi(g)^{-e}-1)b$ satisfies (a)–(c), and it satisfies (d) only if $z_b=0$.

Problem 27.3.2. For z satisfying (a)–(c) put $(c\cdot z)(g):=(-1)^e z(cgc)$. Then $c\cdot z$ satisfies (a)–(c) and $c\cdot(c\cdot z)=z$. For $e>0$, condition (d) is equivalent to $c\cdot z=(-1)^{e+1}z$. For odd ℓ this is the sign of the minus part in Section 27.2.

The twist $e = 0$. Then (a) says that z is a continuous homomorphism, (d) is void, and (b), (c) together say that z vanishes on every inertia group.

Problem 27.3.3. The Artin map identifies $\mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; 0, n)$ with $\mathrm{Hom}(\mathrm{Cl}(E), \mathcal{O}_n)$.

Problem 27.3.4. Let $C \cong \bigoplus_i \mathbb{Z}/m_i\mathbb{Z}$ be a finite abelian group. Then

$$\operatorname{len} \mathrm{Hom}(C, \mathcal{O}_n) = \sum_i \min\big(v_{\mathcal{O}}(m_i),\, n\, v_{\mathcal{O}}(\ell)\big) \le v_{\mathcal{O}}(|C|),$$

with equality for all large n.

Problem 27.3.5. For $E = \mathbb{Q}(\sqrt{-23})$, $\ell = 3$ and $\mathcal{O} = \mathbb{Z}_3$, the length of $\mathrm{Sha}_3^{\mathrm{odd}}(E, \mathbb{Z}_3; 0, n)$ is $\min(1, n)$; for $\ell \neq 3$ and every $\mathcal{O}$ it is 0.

Let $h_E := |\mathrm{Cl}(E)|$. Problems 27.3.3 and 27.3.4 prove the following.

Theorem 27.3.1. *Let $E \subset \overline{\mathbb{Q}}$ be a CM field, ℓ a prime, $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_\ell$, and $n \ge 0$. Then* $\operatorname{len} \mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; 0, n) \le v_{\mathcal{O}}(h_E)$.

The field $\mathbb{Q}(\zeta_\ell)$ modulo ℓ. Now let ℓ be odd, $E = F := \mathbb{Q}(\zeta_\ell)$, $\mathcal{O} = \mathbb{Z}_\ell$, $n = 1$ and $e > 0$, and let λ be the prime of F above ℓ.

Problem 27.3.6. Every $z \in \mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ is a homomorphism $G_F \to \mathbb{F}_\ell$. The module $\mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ does not depend on $e > 0$.

Problem 27.3.7. The map $z_{\mathrm{cyc}}(g) := (\chi(g) - 1)/\ell \bmod \ell$ is a homomorphism $G_F \to \mathbb{F}_\ell$ satisfying (b) and (c), it is nonzero on $D_{\mathfrak{P}}$ for every $\mathfrak{P}$ above ℓ, and $z_{\mathrm{cyc}}(cgc) = z_{\mathrm{cyc}}(g)$. So $z_{\mathrm{cyc}} \notin \mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$.

Problem 27.3.8. Every $z \in \mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ vanishes on all of $D_{\mathfrak{P}}$, for every $\mathfrak{P}$ above ℓ.

Problem 27.3.9. The Artin map identifies $\mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ with $\mathrm{Hom}(A^-, \mathbb{F}_\ell)$, for every $e > 0$. Hence its length is the ℓ-rank of A^-.

By Problem 27.2.3, this is also the ℓ-rank of the minus part of $\mathrm{Sha}_\ell(F, e)$. So in this case the odd cocycles see what the minus part sees modulo ℓ: condition (d) removes the plus part, and (c) and (d) together remove the cyclotomic homomorphism z_{cyc}.

One integer for all ℓ. For a CM field in $\mathbb{Q}(\zeta_N)$, the following theorem gives one integer for every prime ℓ, every coefficient ring specified below, every $0 \le e < t$, and every $n \ge 0$.

Theorem 27.3.2. *Let $N \ge 1$ and $t \ge 0$ be integers (in the application, $t = 5r$), let d_N be the exponent of the group $(\mathbb{Z}/N\mathbb{Z})^\times$, and let $E \subset \overline{\mathbb{Q}}$ be a CM field contained in $\mathbb{Q}(\zeta_N)$. There is an integer X_{odd} with*

$$1 \le X_{\mathrm{odd}} \le 2^{4(N+t+3)^{27}} h_E$$

such that for every prime ℓ (including $\ell = 2$), every ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_\ell$ that contains a primitive d_N-th root of unity, every integer e with $0 \le e < t$, and every $n \ge 0$,

$$\operatorname{len} \mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; e, n) \le v_{\mathcal{O}}(X_{\mathrm{odd}}).$$

In particular these lengths are finite. Here N is a cyclotomic modulus, not the level of Chapter 33. For $e = 0$ the bound follows from Theorem 27.3.1, and for $t = 1$ one may take $X_{\mathrm{odd}} = h_E$. For $0 < e < t$ the proof argues through twisted Stickelberger sums, Jacobi-type quotients of Gauss sums and Kolyvagin's derivative cocycles; Chapter 28 illustrates the Gauss-sum method. It proves no equality of characteristic ideals, only this upper bound at finite level.

In the Lean formalization. In the Lean proof [GL], Theorem 27.3.2 is `New.exists_length_shaOdd_le` and Theorem 27.3.1 is `New.length_shaOdd_zero_le_addVal_classNumber`, both in `grh/src/Lib/Cyclotomic/OddSha.lean`, and Definition 27.3.1 is the case $\Lambda = \mathcal{O}$ of `New.Selmer.shaOdd` in `grh/src/Lib/GaloisRep/Main/SelmerModules.lean`.

Problem 27.3.10. Let $E = \mathbb{Q}(\zeta_{37})$, $N = 37$ and $t \geq 2$. Then $\mathbb{Z}_{37}$ satisfies the hypotheses of Theorem 27.3.2, and every integer X_{odd} as in that theorem is divisible by 37.

Problem 27.3.11. Let N, t, d_N, E, X_{odd} be as in Theorem 27.3.2, and for each prime ℓ let $\mathcal{O}_{(\ell)}$ be the ring of integers of $\mathbb{Q}_\ell(\zeta_{d_N})$. Then $\mathcal{O}_{(\ell)}$ satisfies the hypotheses of the theorem, and for $0 \leq e < t$, $n \geq 0$ and every finite set T of primes,

$$\sum_{\ell \in T} \frac{\operatorname{len} \mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}_{(\ell)}; e, n)}{v_{\mathcal{O}_{(\ell)}}(\ell)} \log \ell \leq \log X_{\mathrm{odd}} \leq 4(N + t + 3)^{27} \log 2 + \log h_E.$$

This is the analogue of Problem 27.2.4. Chapter 65 applies Theorem 27.3.2 to the field E of Chapter 33, with $t = 5r$. In the proof, the resulting term in the denominator error at ℓ is $t\, v_\ell(X_{\mathrm{odd}})$. For every finite set T of primes its contribution to the weighted sum is $t \sum_{\ell \in T} v_\ell(X_{\mathrm{odd}}) \log \ell \leq t \log X_{\mathrm{odd}}$.

Hints

§27.1.

27.1.1: χ_ℓ maps $G_{\mathbb{Q},\ell}$ and G_ℓ onto $\mathbb{Z}_\ell^\times$. Compute the least $v_\ell(u^k - 1)$ over $u \in \mathbb{Z}_\ell^\times$.

27.1.2: Combine Problem 27.1.1 with the theorem of von Staudt and Clausen. If $(\ell - 1) \nmid k$, then B_k/k is ℓ-integral [Wa, Cor. 5.14].

27.1.3: An unramified class lies in $H^1(\hat{\mathbb{Z}}, W_e) = W_e/(\varphi - 1)W_e$, where Frobenius φ acts by p^{-e}. For the second statement, inflate from $G_{\mathbb{Q},\ell}$; conversely, by inflation–restriction a class that is unramified outside ℓ comes from $G_{\mathbb{Q},\ell}$, since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_S)$ is generated as a closed normal subgroup by the inertia groups at primes $p \neq \ell$.

27.1.4: Use the sequence $0 \to \mathbb{Z}/\ell(-e) \to W_e \xrightarrow{\ell} W_e \to 0$ and Problem 27.1.1.

27.1.5: Use inflation–restriction to $G_F := \mathrm{Gal}(\mathbb{Q}_S/F)$, which acts trivially on $\mathbb{Z}/\ell(-e)$. The prime above ℓ in F is principal, and $[F_\lambda : \mathbb{Q}_\ell] = \ell - 1$ is prime to ℓ.

27.1.6: Let $i \equiv -e \pmod{\ell - 1}$. Use Theorem 27.1.1, Theorem 26.2.2, and Kummer's congruence $B_m/m \equiv B_n/n \pmod{\ell}$ for even $m, n \geq 2$ with $m \equiv n \not\equiv 0 \pmod{\ell - 1}$ [Wa, Ch. 5]; treat $i \equiv 1$ separately, using $A^{(1)} = 0$ [Wa, Prop. 6.16].

27.1.7: Problem 27.1.1 with $k = -e$, and local duality.

27.1.8: Apply the Euler characteristic formula to $\mathbb{Z}_\ell(k)/\ell^n$ and let $n \to \infty$; since the groups $H^i(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k)/\ell^n)$ are finite, their inverse limit is $H^i(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ [NSW, Ch. II, §7]. For the upper bound on the rank, show that $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k)/\ell^n) = H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))/\ell^n$, which is bounded by Soulé's theorem. For the torsion, use $0 \to \mathbb{Z}_\ell(k) \to \mathbb{Q}_\ell(k) \to \mathbb{Q}_\ell/\mathbb{Z}_\ell(k) \to 0$. The groups $H^i(G_{\mathbb{Q},\ell}, M)$ are finite for finite $G_{\mathbb{Q},\ell}$-modules M of ℓ-power order [NSW, Ch. VIII, §3]; finite generation of $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ follows from finiteness of its reduction modulo ℓ by Nakayama's lemma, and $H^3 = 0$ passes to the limit.

27.1.9: Problems 27.1.7, 27.1.8 and 27.1.2, and Theorem 27.1.2 with $e = k-1$.

§27.2.

27.2.1: Shapiro's lemma for $\mathrm{Ind}_{G_{E,\ell}}^{G_{\mathbb{Q},\ell}} W_e \cong \bigoplus_\eta W_e \otimes \eta$. The field E has one prime above ℓ.

27.2.2: Repeat Problems 27.1.4 and 27.1.5 with the twisted coefficients. On $(W_e \otimes \eta^{-1})[\ell]$, the action is through the reduction of ω^{-e-j}.

27.2.3: Sum Problem 27.2.2 over the critical j. The one character ω^{-e} not covered there is plus for e.

27.2.4: For the second part, Theorem 27.1.2.

27.2.5: $B_{2k} = (-1)^{k+1} 2(2k)!\zeta(2k)/(2\pi)^{2k}$, and bound the denominator by von Staudt–Clausen and $\prod_{p \le n} p \le 4^n$.

§27.3.

27.3.1: χ is trivial on inertia at primes other than ℓ, and $\chi(cgc) = \chi(g)$; 2 is a unit in $\mathcal{O}_n$.

27.3.2: $\chi_\ell(c) = -1$. Conjugation by c carries $D_\mathfrak{P}$, $I_\mathfrak{P}$ to $D_{c\mathfrak{P}}$, $I_{c\mathfrak{P}}$.

27.3.3: A homomorphism killing all inertia groups factors through the Galois group of the Hilbert class field; E has no real places.

27.3.4: $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathcal{O}_n) \cong \mathcal{O}/(m, \ell^n)$, and $\mathcal{O}/\pi^k\mathcal{O}$ has length k.

27.3.5: The class number of $\mathbb{Q}(\sqrt{-23})$ is 3.

27.3.6: $\chi(g) \equiv 1 \pmod{\ell}$ on G_F.

27.3.7: $\chi(D_\mathfrak{P}) = 1 + \ell\mathbb{Z}_\ell$, since $\mathbb{Q}_\ell(\zeta_{\ell^2})$ has degree ℓ over $\mathbb{Q}_\ell(\zeta_\ell)$.

27.3.8: On $D_\mathfrak{P}$, z factors through $\chi(D_\mathfrak{P}) = 1 + \ell\mathbb{Z}_\ell$, so it is a multiple of z_{cyc} there. Compare at $\mathfrak{P}$ and $c\mathfrak{P}$, which are conjugate under G_F.

27.3.9: Problems 27.3.8 and 27.3.2; $\lambda = (1 - \zeta_\ell)$ is principal, the Artin map satisfies $\mathrm{Art}(\sigma\mathfrak{a}) = \tilde{\sigma}\,\mathrm{Art}(\mathfrak{a})\,\tilde{\sigma}^{-1}$, and $c = \sigma_{-1}$ acts on $A^{(i)}$ by $(-1)^i$.

27.3.10: Problems 27.3.9 and 26.2.8.

27.3.11: $v_\mathcal{O}(X_{\mathrm{odd}}) = v_\mathcal{O}(\ell)\, v_\ell(X_{\mathrm{odd}})$, and Problem 27.2.4.

References

[BK] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in: The Grothendieck Festschrift, Vol. I, Progr. Math. 86, Birkhäuser, 1990, 333–400.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* **Q**, Invent. Math. **76** (1984), 179–330.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. 323, Springer, 2008.

[SeL] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, 1979.

[So] C. Soulé, *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Invent. Math. **55** (1979), 251–295.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.