TATE–SHAFAREVICH GROUPS OF TATE TWISTS

Prerequisites. This chapter continues Chapter 29, *Denominators and the Stickelberger element*, whose notation A, $A^{(i)}$, $A^{\pm}$, ω (Section 29.2, with $p=\ell$), Problem 29.2.2 and Theorem 29.2.2 we use. Continuous cohomology of profinite groups [NSW, Ch. I; Ch. II, §7], inflation–restriction, and the vanishing of $H^q(G,M)$, $q\ge 1$, for finite G of order invertible on M [SeL, Ch. VII–VIII]. The Artin isomorphism between the ideal class group of a number field and the Galois group of its Hilbert class field [Ne, Ch. VI]. The duality theorems for Galois cohomology of number fields are stated in the text with references. Section 30.3 uses the ramps of Problem 7.4.1 in *The slope inequality in the mean*. Throughout, ℓ is an odd prime and $\mathrm{num}(r)$ is the numerator of a rational number r in lowest terms.

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

In the previous chapter the denominator that no twist removes was measured by an eigenspace of a class group. Which Galois cohomology groups play this role for a Tate twist, and what are their orders? 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 $\chi_\ell\colon G_{\mathbb{Q},\ell}\to\mathbb{Z}_\ell^\times$ the cyclotomic character. 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

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

and $h_{\ell,e}(\mathbb{Q})\in\{0,1,2,\dots,\infty\}$ 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 30.1.1. 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, $k\ge 2$ even, is the product of the primes p with $(p-1)\mid k$.

Problem 30.1.2. For even $k\ge 2$, the power of ℓ in the denominator of $\zeta(1-k)=-B_k/k$ is $|H^0(G_{\mathbb{Q},\ell},\mathbb{Q}_\ell/\mathbb{Z}_\ell(k))|$.

So the denominators of the values $\zeta(1-k)$ are orders of H^0; their numerators will be orders of Sha.

Problem 30.1.3. 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.

To compute Sha, restrict to $F=\mathbb{Q}(\zeta_\ell)$.

Date: November 25, 2026.

Problem 30.1.4. 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 30.1.5. Suppose that $(\ell-1) \nmid e$. Restriction to $\mathrm{Gal}(\mathbb{Q}_S/F)$, followed by the Artin map, identifies the group of Problem 30.1.4 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 30.1.4 and 30.1.5 prove the following.

Theorem 30.1.1. *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 30.1.6. If $(\ell - 1) \mid e$ and $e \neq 0$, then $\mathrm{Sha}_\ell(\mathbb{Q}, e) = 0$.

Problem 30.1.7. 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 2 [NSW, Ch. VIII, §3], so $H^3(G_{\mathbb{Q},\ell}, M) = 0$ for every ℓ-primary M.

Problem 30.1.8. 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 30.1.9. 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 30.1.2 (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 30.1.10. 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]. For odd $k \geq 3$, that is for even $e = k-1$, the value $\zeta(1-k)$ vanishes, $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ has rank one (Problem 30.1.9), and $\mathrm{Sha}_\ell(\mathbb{Q}, k-1)$ is dual to a subgroup of $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$. One expects the order of $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ to be the index in $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ of the subgroup generated by cyclotomic elements, as for A^+; this chapter does not use it.

30.2. The minus part and the plus part

Over $\mathbb{Q}$ the twists split by the parity of e: odd e is controlled by a Bernoulli number, even e by the plus part of a class group. 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 $\mathrm{Sha}_\ell(E, e)$, 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* and the *plus part* of $\mathrm{Sha}_\ell(E, e)$ are the sums of the η-parts over the critical and over the plus characters.

Problem 30.2.1. 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 30.2.2. 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 30.2.3. For every $e \neq 0$, the minus part of $\mathrm{Sha}_\ell(\mathbb{Q}(\zeta_\ell), e)$ has the same ℓ-rank as A^-, and the plus part has ℓ-rank at least that of A^+.

So the critical eigenspaces see the minus part of a class group, where Stickelberger's theorem and Bernoulli numbers apply, and the plus eigenspaces see the plus part, where they do not. On the minus side one number controls every ℓ at once.

Problem 30.2.4. For a nonzero integer N, $\sum_\ell v_\ell(N) \log \ell \leq \log|N|$. Hence, for odd $e \geq 1$,

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

Problem 30.2.5. For $k \geq 1$, $\log|\mathrm{num}(B_{2k}/2k)| \leq 2k \log(2k) + 3$.

On the plus side no such number is available. One case is elementary.

Problem 30.2.6. If $\ell \equiv 1 \pmod 4$, the class number of $\mathbb{Q}(\sqrt{\ell})$ is less than ℓ.

Problem 30.2.7. Let $e \geq 2$ be even with $(\ell - 1) \mid 2e$. Then $\mathrm{Sha}_\ell(\mathbb{Q}, e) = 0$. For example $\mathrm{Sha}_5(\mathbb{Q}, 2) = 0$.

Problem 30.2.8. If ℓ does not divide the class number of $\mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$, then $\mathrm{Sha}_\ell(\mathbb{Q}, e) = 0$ for every even $e \neq 0$.

Over $\mathbb{Q}$ the pairs (ℓ, e) therefore fall into three cases: e odd, given by Theorem 30.1.2; e even with $(\ell - 1) \mid 2e$, zero by Problem 30.2.7; and e even with $(\ell - 1) \nmid 2e$, zero under Vandiver's conjecture and unknown in general. The fields of the argument are abelian CM fields of large degree, and there the plus part is the difficulty; Alpöge's note speaks of the classes "that we couldn't kill by twisting" and of a "significant weakening of Vandiver" [Alp, item 17]. No proof of such a bound has been published. In [Adr] the bound the argument needs is [Adr, Hyp. 17.11]; see the ledger in Section 58.7 of Chapter 58.

30.3. The size of the bound

How large may these groups be before they spoil the slope inequality? For a number field E and an integer $t \geq 2$ let

$$V(E,t) := \sum_{\ell} \log \ell \sum_{1 \leq e < t} h_{\ell,e}(E),$$

the logarithm of the order of $\bigoplus_{\ell,e} \mathrm{Sha}_\ell(E,e)$ when this group is finite. By Problem 7.4.1, the divisibility at the inert and ramified primes, summed with weights $\log p$, is w times a ramp sum at the scale $x = a/w$. In Alpöge's argument, as reconstructed in [Adr], the denominators left after gluing are paid for by $V(E,t)$, for a CM field E whose degree and number of twists t are bounded by powers of x, and the weight is $w = b := \exp(x^\varepsilon)$ with a small fixed $\varepsilon > 0$. The bound that the argument needs is $V(E,t) \leq \sqrt{b}$. In [Adr] it follows, on suitable windows of scales, from the Selmer bound on windows by [Adr, Prop. 18.4]; in [Adr] the Selmer bound is [Adr, Hyp. 17.11], assumed there. The Lean formalization proves it; Chapter 57 outlines the proof. See (W3) and the ledger in Section 58.7 of Chapter 58.

Problem 30.3.1. Suppose that $bS \leq bM + bR + V$ with real numbers S, M, R and $0 \leq V \leq \sqrt{b}$. Then $S \leq M + R + \exp(-x^\varepsilon/2)$, and $\exp(-x^\varepsilon/2) = o(x^{-C})$ for every C.

In the applications S is a ramp sum over primes, M its main term of size $x \log x$, and R must be $O(x^{1/2+\varepsilon})$.

Problem 30.3.2. If $V(E,t) \leq x^C$ for a constant C, then $V(E,t) \leq \sqrt{b}$ for all large x. The same holds if $V(E,t) \leq \exp(x^{\varepsilon'})$ with $\varepsilon' < \varepsilon$. For $c > 0$ and $d \geq x$, on the other hand, $\exp(\exp(cd)) > \sqrt{b}$ for all large x.

Through Soulé's Chern class maps [So], $\mathrm{Sha}_\ell(E,e)$ is dual to a subquotient of $K_{2e}(\mathcal{O}_E) \otimes \mathbb{Z}_\ell$, so one expects $V(E,t)$ to be polynomial in x. Over $\mathbb{Q}$ this follows from Vandiver's conjecture.

Problem 30.3.3. Assume Vandiver's conjecture for every odd ℓ. Then for $t \geq 2$

$$\sum_{\ell \text{ odd}} \log \ell \sum_{1 \leq e < t} h_{\ell,e}(\mathbb{Q}) \leq t^2 \log t + 3t.$$

The difficulty is therefore not the size of $V(E,t)$ but its uniformity in ℓ, e and a field E that changes with x. On the minus part one Bernoulli number bounds all ℓ at once (Problem 30.2.4); on the plus part no such number is available, already over $\mathbb{Q}$. Over $\mathbb{Q}$ the minus part is given exactly by Theorem 30.1.2. Over the fields E of the argument the formalization needs only an upper bound, and obtains it without the main conjecture, by a one-sided Euler-system argument with Gauss sums (Chapter 55); the plus part it bounds by congruences, case by case (Chapter 56).

Questions. The following are not known to us. Is $A^+ = 0$ for every odd prime p (Vandiver's conjecture)? Is there a constant C such that $\sum_{\ell \text{ odd}} \log \ell \sum_{1 \leq e < t,\ e \text{ even}} h_{\ell,e}(\mathbb{Q}) \leq t^C$ for all $t \geq 2$? A positive answer to the second question would give, for the plus part over $\mathbb{Q}$, far more than the argument requires: it needs only $V(E,t) \leq \sqrt{b}$, with t a power of x and $b = \exp(x^\varepsilon)$, and only on windows of scales. In [Adr] this requirement is [Adr, §17.3, Hyp. 17.11], assumed there; the formalization proves it (Chapter 57); see the ledger in Section 58.7 of Chapter 58. It implies a bound toward Vandiver's conjecture stronger than the published ones [Adr, Prop. 17.22].

The route to it sketched in [Adr, §17.4] passes through an automorphy statement for residually reducible Galois representations of unitary type in three variables, (G3) there; its status is recorded in Section 33.4 of Chapter 33. The route of the formalization is that of Chapters 55, 56 and 57.

Hints

§30.1.

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

30.1.2: Combine Problem 30.1.1 with the theorem of von Staudt and Clausen. If $(\ell-1) \nmid k$, then B_k/k is ℓ-integral [Wa, Cor. 5.14].

30.1.3: 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 $G_{\mathbb{Q},\ell}$.

30.1.4: Use the sequence $0 \to \mathbb{Z}/\ell(-e) \to W_e \xrightarrow{\ell} W_e \to 0$ and Problem 30.1.1.

30.1.5: 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.

30.1.6: Now $\mathbb{Z}/\ell(-e)$ is trivial and $\mathbb{Q}$ has class number 1. Compare the images of $H^0(W_e)/\ell$ globally and at ℓ using Problem 30.1.1.

30.1.7: Let $i \equiv -e \pmod{\ell-1}$. Use Theorem 30.1.1, Theorem 29.2.2, 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].

30.1.8: Problem 30.1.1 with $k = -e$, and local duality.

30.1.9: 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 $0 \to \mathbb{Z}_\ell(k) \to \mathbb{Q}_\ell(k) \to \mathbb{Q}_\ell/\mathbb{Z}_\ell(k) \to 0$.

30.1.10: Problems 30.1.8, 30.1.9 and 30.1.2, and Theorem 30.1.2 with $e = k-1$.

§30.2.

30.2.1: 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.

30.2.2: Repeat Problems 30.1.4 and 30.1.5; $W_e \otimes \omega^{-j}$ is congruent to ω^{-e-j} modulo ℓ.

30.2.3: Sum Problem 30.2.2 over j, using $A^{(0)} = 0$. The one character ω^{-e} not covered there is plus for e.

30.2.4: For the second part, Theorem 30.1.2.

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

30.2.6: Minkowski's bound, and count integral ideals of small norm.

30.2.7: If $(\ell-1) \mid e$, Problem 30.1.6. Otherwise $-e \equiv (\ell-1)/2$; use Theorem 30.1.1, Problem 29.2.2 and Problem 30.2.6.

30.2.8: Theorem 30.1.1 and Problem 29.2.2; if $(\ell-1) \mid e$, Problem 30.1.6.

§30.3.

30.3.2: Compare logarithms: $\log \sqrt{b} = x^{\varepsilon}/2$.

30.3.3: The even e contribute nothing. For odd e, Problems 30.2.4 and 30.2.5 with $2k = e + 1 \leq t$.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[Alp] L. Alpöge, untitled note announcing a proof of the Riemann hypothesis, 20 November 2026, `https://alpo.ge/remark.pdf`.

[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.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, 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.