DENOMINATORS AND THE STICKELBERGER ELEMENT

Prerequisites. Ideal class groups [Ne, Ch. I, §§3, 6] and the norm of ideals in an extension of number fields. Cyclotomic fields, Bernoulli numbers and generalized Bernoulli numbers [Wa, Ch. 4–6]. From Chapter 6, *The slope method*: Euclidean lattices as normed spaces over $\mathbb{Q}$ with their slopes (Section 6.3), and the slope inequality of Theorem 6.4.1 with Problem 6.4.2. Chapter 30, *Tate–Shafarevich groups of Tate twists*, continues this one.

29.1. Denominators of linear maps

A linear map between $\mathbb{Q}$-vector spaces with integral structures need not respect them. What does that cost in a slope inequality, and how can it be reduced? The simplest example is differentiation. Let Int be the set of polynomials $f \in \mathbb{Q}[x]$ with $f(\mathbb{Z}) \subseteq \mathbb{Z}$, and let Int_n be its elements of degree at most n.

Problem 29.1.1. The binomial polynomials $\binom{x}{k}$, $0 \le k \le n$, form a $\mathbb{Z}$-basis of Int_n.

Problem 29.1.2. Let $D = d/dx$. Then

$$D\binom{x}{n} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \binom{x}{n-k}.$$

Hence the least positive integer c with $c\,D(\mathrm{Int}_n) \subseteq \mathrm{Int}$ is $\mathrm{lcm}(1, 2, \dots, n)$.

The logarithm of this denominator is $\sum_{p^a \le n} \log p$, of the size of n. Alpöge's note records a "need for division" [Alp, item 14]. In the reconstruction [Adr, §17.1] the defect sits at the places where the local type of the theta lifts is twisted: there the lattice of integral lifted forms differs from the lattice that the period pairing sees, and a congruence module measures the difference.

An integral structure can be built one prime at a time. For a lattice $L \subset \mathbb{Q}^r$ and a prime p, write $L_p := L \otimes \mathbb{Z}_p \subset \mathbb{Q}_p^r$.

Problem 29.1.3. For every family $(\Lambda_p)_p$ of $\mathbb{Z}_p$-lattices $\Lambda_p \subset \mathbb{Q}_p^r$ with $\Lambda_p = \mathbb{Z}_p^r$ for all but finitely many p, there is exactly one lattice $L \subset \mathbb{Q}^r$ with $L_p = \Lambda_p$ for every p, namely $L = \bigcap_p (\Lambda_p \cap \mathbb{Q}^r)$. If $\Lambda_2 = \frac{1}{2}\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\Lambda_3 = \mathbb{Z}_3 \oplus \frac{1}{3}\mathbb{Z}_3$, and $\Lambda_p = \mathbb{Z}_p^2$ otherwise, then $L = \frac{1}{2}\mathbb{Z} \oplus \frac{1}{3}\mathbb{Z}$.

For a finitely generated torsion $\mathbb{Z}_p$-module T let $\mathrm{len}_{\mathbb{Z}_p} T$ be its length.

Problem 29.1.4. If T is a finite abelian group, then $\log|T| = \sum_p \mathrm{len}_{\mathbb{Z}_p}(T \otimes \mathbb{Z}_p) \log p$. If $M' \subseteq M$ are lattices of the same rank, then $\log[M : M'] = \sum_p \mathrm{len}_{\mathbb{Z}_p}(M_p/M'_p) \log p$.

Let L and M be Euclidean lattices and $T\colon L_{\mathbb{Q}} \to M_{\mathbb{Q}}$ an injective linear map. If $T(L) \not\subseteq M$, one may replace M by the lattice $M + T(L)$, with the same norm.

Date: November 25, 2026.

Problem 29.1.5. $\mu_{\max}(M + T(L)) \le \mu_{\max}(M) + \log[M + T(L) : M]$. Hence $\mu(L) \le \mu_{\max}(M) + h_\infty(T) + \log[M + T(L) : M]$.

The index term in Theorem 6.5.1 has the same origin. So a denominator costs $\log|(M + T(L))/M|$, a sum of local terms by Problem 29.1.4. If several maps $T_1, \dots, T_k$ serve equally well, for instance because they have the same period, one may choose at each prime the lattice $(M + T_j(L))_p$ of smallest index over M_p, and Problem 29.1.3 assembles the choices into one lattice M^*. A map carrying L into M^* must then be found separately; for the Stickelberger element below it is a combination of the twists.

Problem 29.1.6. Let $M_j := M + T_j(L)$, and let M^* be the lattice with $M^*_p = (M_j)_p$ for a $j = j(p)$ that minimizes $\operatorname{len}_{\mathbb{Z}_p}\big((M_j)_p/M_p\big)$. Then $M^* \supseteq M$ and

$$\log[M^* : M] = \sum_p \min_j \operatorname{len}_{\mathbb{Z}_p}\big((M_j)_p/M_p\big) \log p.$$

If $M = \mathbb{Z}$ and $M_j = D_j^{-1}\mathbb{Z}$ with positive integers D_j, then $[M^* : M] = \gcd(D_1, \dots, D_k)$. For $D_j = 6, 10, 15$ each map alone costs at least $\log 6$, and together they cost nothing.

Alpöge's note glues its integral structures in this way, "across Hecke characters for a 'gcd' " [Alp, item 15]. What no twist removes is, at each prime, a finite module that it identifies with a group of Galois cohomology classes [Alp, item 17]; in the reconstruction the congruence modules are bounded by lengths of Tate–Shafarevich groups of Tate twists, through deformation rings and Wach modules [Adr, §§17.3 and 17.5], so the Stickelberger element below is a model of the minus part only. The simplest instance, a rational element whose twists are integral and whose remainder is measured by a class group, is the Stickelberger element of $\mathbb{Q}(\zeta_p)$.

29.2. The Stickelberger element

Let p be an odd prime, $F := \mathbb{Q}(\zeta_p)$, $G := \operatorname{Gal}(F/\mathbb{Q})$, and let $\sigma_a \in G$ be the automorphism with $\sigma_a(\zeta_p) = \zeta_p^a$. Let A be the p-primary part of $\operatorname{Cl}(F)$, a $\mathbb{Z}_p[G]$-module. Let $\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ be the Teichmüller character, with $\omega(a) \equiv a \pmod p$, and view it as a character of G. For $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ let $A^{(i)} := \{z \in A : \sigma_a z = \omega(a)^i z \text{ for all } a\}$, and

$$\varepsilon_i := \frac{1}{p-1} \sum_{a=1}^{p-1} \omega(a)^i \sigma_a^{-1} \in \mathbb{Z}_p[G].$$

Problem 29.2.1. The ε_i are orthogonal idempotents with sum 1, $\sigma_a \varepsilon_i = \omega(a)^i \varepsilon_i$, and $A = \bigoplus_i \varepsilon_i A = \bigoplus_i A^{(i)}$. Complex conjugation σ_{-1} acts on $A^{(i)}$ by $(-1)^i$.

Write A^+ and A^- for the sums of the $A^{(i)}$ with i even and with i odd.

Problem 29.2.2. If $K \subseteq F$, then extension of ideals identifies the p-primary part of $\operatorname{Cl}(K)$ with $A^{\operatorname{Gal}(F/K)}$. Hence $A^{(0)} = 0$, A^+ is the p-primary part of the class group of $F^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, and if $p \equiv 1 \pmod 4$, then $A^{((p-1)/2)}$ is the p-primary part of $\operatorname{Cl}(\mathbb{Q}(\sqrt{p}))$.

The *Stickelberger element* is

$$\theta := \frac{1}{p}\sum_{a=1}^{p-1} a\,\sigma_a^{-1} \in \mathbb{Q}[G],$$

with the denominator p. We use Stickelberger's theorem as a black box [Wa, Thm. 6.10].

Theorem 29.2.1 (Stickelberger)**.** *If $\beta \in \mathbb{Z}[G]$ and $\beta\theta \in \mathbb{Z}[G]$, then $\beta\theta$ annihilates* $\mathrm{Cl}(F)$.

The integral multiples of θ are its twists.

Problem 29.2.3. For c prime to p, $(c-\sigma_c)\theta = \sum_{b=1}^{p-1} \lfloor cb/p \rfloor\, \sigma_b^{-1}$. In particular $(c-\sigma_c)\theta \in \mathbb{Z}[G]$.

For a nontrivial Dirichlet character χ modulo p let $B_{1,\chi} := \frac{1}{p}\sum_{a=1}^{p-1} \chi(a)\,a$.

Problem 29.2.4. $\varepsilon_i\theta = B_{1,\omega^{-i}}\varepsilon_i$ for $i \not\equiv 0$. If $i \not\equiv 0$ is even, then $B_{1,\omega^{-i}} = 0$.

So θ says nothing about A^+. On $A^{(i)}$ the twist $(c-\sigma_c)\theta$ acts as $(c-\omega(c)^i)B_{1,\omega^{-i}}$, and the gluing of Problem 29.1.6 asks for the ideal generated by the factors $c-\omega(c)^i$.

Problem 29.2.5. The ideal of $\mathbb{Z}_p$ generated by the numbers $c-\omega(c)^i$, c prime to p, is $\mathbb{Z}_p$ if $i \not\equiv 1$ and $p\mathbb{Z}_p$ if $i \equiv 1$. Moreover $v_p(B_{1,\omega^{-1}}) = -1$.

Thus on each $A^{(i)}$ with $i \not\equiv 0, 1$ the twists together act as $B_{1,\omega^{-i}} \in \mathbb{Z}_p$: the gluing recovers the eigenvalue of θ itself. On $A^{(1)}$ every factor $c-\omega(c)$ is divisible by p and cancels the denominator of $B_{1,\omega^{-1}}$, so the twists generate $\mathbb{Z}_p$ and not $p^{-1}\mathbb{Z}_p$: the gluing does not recover the eigenvalue of θ. This p is the order of μ_p, on which G acts by ω. (The group $A^{(1)}$ vanishes for another reason [Wa, Prop. 6.16].) By Kummer's congruences [Wa, Ch. 5], if i is odd and $3 \le i \le p-2$, then

$$B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} \pmod{p}. \tag{1}$$

Problem 29.2.6. For $p = 7$ the character ω^{-3} is the Legendre symbol, $B_{1,\omega^{-3}} = -1$, and $B_4/4 = -1/120 \equiv -1 \pmod 7$.

Problem 29.2.7. Let i be odd with $3 \le i \le p-2$. If $p \nmid B_{p-i}$, then $A^{(i)} = 0$.

This is Herbrand's theorem [Wa, Thm. 6.17]. Its converse is due to Ribet [Ri], and the exact order to Mazur and Wiles [MW]; see [Wa, Ch. 15]. We use them as a black box.

Theorem 29.2.2 (Herbrand, Ribet, Mazur–Wiles)**.** *Let i be odd with $3 \le i \le p-2$. Then $A^{(i)} \ne 0$ if and only if $p \mid B_{p-i}$, and $|A^{(i)}| = |B_{1,\omega^{-i}}|_p^{-1}$.*

Problem 29.2.8. For $p < 100$, the pairs (p,k) with k even, $2 \le k \le p-3$ and $p \mid B_k$ are $(37,32)$, $(59,44)$ and $(67,58)$. Hence for $p < 100$ the group A^- is nonzero only for $p = 37, 59, 67$, and then exactly one odd eigenspace is nonzero, $A^{(5)}$, $A^{(15)}$ and $A^{(9)}$ respectively.

The plus part A^+ is not seen by θ (Problem 29.2.4). Its order is the p-part of an index of cyclotomic units in the units of F^+ [Wa, Thm. 8.2]. Vandiver's conjecture, that $A^+ = 0$ for every p, has not been proved; it has been verified for $p < 2^{31}$ [HHO]. The next chapter meets the same division between minus and plus parts in Galois cohomology.

Hints

§29.1.

29.1.1: Use the difference operator $\Delta f(x) := f(x+1) - f(x)$ and $\Delta\binom{x}{k} = \binom{x}{k-1}$.

29.1.2: Formally $D = \log(1+\Delta)$. For the sharpness, use the uniqueness in Problem 29.1.1.

29.1.3: Choose an integer N with $N\mathbb{Z}_p^r \subseteq \Lambda_p \subseteq N^{-1}\mathbb{Z}_p^r$ for all p, and work in $N^{-1}\mathbb{Z}^r/N\mathbb{Z}^r$.

29.1.4: The p-primary part of T is $T \otimes \mathbb{Z}_p$.

29.1.5: For a subspace U, compare the lattices $U \cap M$ and $U \cap (M + T(L))$. Then apply Theorem 6.4.1 and Problem 6.4.2 to $T\colon L \to M + T(L)$.

29.1.6: Apply Problem 29.1.4 to M^*/M.

§29.2.

29.2.1: Orthogonality of the characters ω^i of the cyclic group G, whose order is prime to p.

29.2.2: Compose extension of ideal classes with the norm, in both orders; $[F : K]$ is prime to p. For the last claim, find the subfield fixed by the squares in G.

29.2.4: Use $\sigma_a^{-1}\varepsilon_i = \omega(a)^{-i}\varepsilon_i$. For even χ, pair a with $p - a$.

29.2.5: Reduce $c - \omega(c)^i$ modulo p. For $B_{1,\omega^{-1}}$, reduce $pB_{1,\omega^{-1}}$ modulo p.

29.2.7: Apply Theorem 29.2.1 to $\beta = c - \sigma_c$, project with ε_i, choose c by Problem 29.2.5, and use (1).

29.2.8: The first part is a finite computation. For the second use Theorem 29.2.2 with $k = p - i$, and $A^{(1)} = 0$ [Wa, Prop. 6.16].

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`.

[HHO] W. Hart, D. Harvey and W. Ong, *Irregular primes to two billion*, Math. Comp. **86** (2017), 3031–3049.

[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.

[Ri] K. A. Ribet, *A modular construction of unramified p-extensions of* $\mathbf{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162.

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