SIZE AGAINST DIVISIBILITY

Prerequisites. Linear algebra over $\mathbb{C}$: Hermitian and positive semidefinite matrices, and Hadamard's inequality, in the form $\det A \le a_{11}\cdots a_{nn}$ for a positive semidefinite Hermitian matrix $A = (a_{ik})$, or $|\det(v_1,\dots,v_n)| \le \|v_1\|\cdots\|v_n\|$ for vectors. Dedekind domains, the absolute norm, the product formula [Ne, Ch. I and Ch. III], and the unique extension of the ℓ-adic absolute value to an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ [Ne, Ch. II, §4]. Transcendence bases [La, Ch. VIII, §1], and two consequences: $\mathbb{C}$ and $\overline{\mathbb{Q}}_\ell$ are isomorphic fields, both being algebraically closed of characteristic 0 and of transcendence degree the continuum over $\mathbb{Q}$; and an isomorphism between two subfields of $\mathbb{C}$ that are finitely generated over $\mathbb{Q}$ extends to an automorphism of $\mathbb{C}$. Legendre's formula $v_p(n!) = \sum_{e\ge1}\lfloor n/p^e\rfloor$, Stirling's formula, and the von Mangoldt function Λ. No earlier chapter is used. The next chapter, *A twist for each prime*, continues this one.

5.1. Divisibility against size

How can a divisibility statement bound a sum over primes? A binomial coefficient illustrates Chebyshev's factorial method [Ch]. Let $\theta(x) := \sum_{p\le x}\log p$. In the next two problems let n be a nonnegative integer.

Problem 5.1.1. Every prime p with $n < p \le 2n$ divides $\binom{2n}{n}$, and $\binom{2n}{n} \le 4^n$. Hence $\theta(2n) - \theta(n) \le n\log 4$.

The principle is the following. If a nonzero integer Δ is divisible by p^{e_p} for each prime p in a set S, where the e_p are nonnegative integers, then

$$\sum_{p\in S} e_p \log p \le \log|\Delta|. \tag{1}$$

For $\Delta = n!$ and $e_p = v_p(n!)$, with S the primes up to n, both sides of (1) are known exactly.

Problem 5.1.2. $\log n! = \sum_{r\le n}\Lambda(r)\lfloor n/r\rfloor$.

By Stirling's formula the left side is $n\log n - n + O(\log n)$. Without the floor function the right side would be $n\sum_{r\le n}\Lambda(r)/r$. Removing the floors overestimates the right side by $\sum_{r\le n}\Lambda(r)\{n/r\}$, an error of order n by Chebyshev's bounds, the scale of the linear term in Stirling's formula; so this estimate cannot see $\psi(n) - n$, where $\psi(x) := \sum_{r\le x}\Lambda(r)$. For a finer comparison one can seek divisibility bounds with a continuous weight on prime powers, such as $(x/p^e - 1)_+$, where $t_+ := \max(t, 0)$, and a size estimate whose error is smaller than its linear term.

The number Δ will be a minor of a matrix.

Problem 5.1.3. Let $A \in M_r(\mathbb{Z})$ with $\det A \ne 0$, and suppose that the jth column A_j is divisible by the positive integer g_j. Then

$$g_1\cdots g_r \le |\det A| \le \|A_1\|\cdots\|A_r\|.$$

Date: November 26, 2026.

For the columns $(6,6)$ and $(10,20)$, with $g_1 = 6$ and $g_2 = 10$, the three numbers are 60, 60 and $60\sqrt{10}$.

The same principle holds over a number field K, where the product formula accounts for the size of a number at every place. At a finite place v write $\mathcal{O}_v$, $\mathfrak{p}_v$ and q_v for the valuation ring, its maximal ideal and the size of its residue field, and let $|x|_v := q_v^{-\operatorname{ord}_v x}$. At an archimedean place use the usual modulus. Let $n_v := 2$ at complex places and $n_v := 1$ at the other places. Then $\sum_v n_v \log|x|_v = 0$ for $x \in K^\times$. Hence, if $\gamma \in K^\times$ satisfies $|\gamma|_v \le \exp(b_v - g_v)$ at every place, where b_v and g_v are real and vanish for almost all v, then

$$\sum_v n_v g_v \le \sum_v n_v b_v. \tag{2}$$

Typically γ is a minor of a matrix, b_v bounds it through the sizes of the entries, and g_v records an improvement from a congruence. The minor is chosen once over K, but the basis in which one proves the congruence may vary with v.

5.2. A minor of a jet evaluation map

Where does a minor with many prime factors come from? One source is Frobenius. Throughout this section p denotes a prime. Let $K = \mathbb{Q}(\mathrm{i})$, so that a prime $p \equiv 3 \pmod 4$ is inert and $\mathbb{Z}[\mathrm{i}]/p$ is the field with p^2 elements.

Problem 5.2.1. If $p \equiv 3 \pmod 4$ and $u \in \mathbb{Z}[\mathrm{i}]$, then $\bar{u} \equiv u^p \pmod p$.

Thus complex conjugation is the Frobenius at every inert prime. Let $u_1, \dots, u_I \in \mathbb{Z}[\mathrm{i}]$, let $\mathcal{T} \subset \mathbb{Z}^2_{\ge 0}$ be a finite set of s exponents, and let J be a positive integer. On the K-span of the monomials $X^a Y^b$, $(a,b) \in \mathcal{T}$, consider the jet evaluation map

$$\mathrm{ev}\colon f \longmapsto \big((\partial_X^j f)(u_i, \bar{u}_i)\big)_{1 \le i \le I,\ 0 \le j < J}.$$

Its matrix has entries in $\mathbb{Z}[\mathrm{i}]$. Let $g := X^p - Y$.

Problem 5.2.2. Let $p \equiv 3 \pmod 4$. For $f \in \mathbb{Z}[\mathrm{i}][X,Y]$, $u \in \mathbb{Z}[\mathrm{i}]$ and integers $j, k \ge 0$, the number $\big(\partial_X^j (g^k f)\big)(u, \bar{u})$ is divisible by p^k.

Problem 5.2.3. Let $p \equiv 3 \pmod 4$, and suppose that $(a-p, b+1) \in \mathcal{T}$ whenever $(a,b) \in \mathcal{T}$ and $a \ge p$. Then every $s \times s$ minor of the matrix of ev is divisible by p^{N_p}, where $N_p := \sum_{(a,b)\in\mathcal{T}} \lfloor a/p \rfloor$. The set $\mathcal{T} = \{(a,b) : a + 2b \le N\}$ satisfies the hypothesis for every p.

Let $\beta := \max(1, |u_1|, \dots, |u_I|)$, $D := \sum_{\mathcal{T}} (a+b)$ and $A_* := \max(\{1\} \cup \{a : (a,b) \in \mathcal{T}\})$. Every $s \times s$ minor of the matrix of ev has absolute value at most $s!\, A_*^{s(J-1)} \beta^D$.

Theorem 5.2.1. *Suppose that* ev *is injective, and let P be a set of primes $p \equiv 3 \pmod 4$ for which $\mathcal{T}$ satisfies the hypothesis of Problem 5.2.3. Then*

$$\sum_{p \in P} \log p \sum_{(a,b)\in\mathcal{T}} \left\lfloor \frac{a}{p} \right\rfloor \le D \log \beta + \log s! + s(J-1) \log A_*.$$

Over a finite field, Stepanov's method for curves likewise compares the forced vanishing of an auxiliary function with a bound on its degree [Bom].

5.3. Heights of families

In Section 5.1 the size and the divisibility of one number were compared at the places of one field. In the proof the number examined at a prime may depend on the isomorphism used there, and no number field is fixed in advance. The places are therefore replaced by isomorphisms.

For a prime ℓ let $|\cdot|_\ell$ be the absolute value on $\overline{\mathbb{Q}}_\ell$ that extends the ℓ-adic one, so that $|\ell|_\ell = \ell^{-1}$. Write $\iota \mid \ell$ for a field isomorphism $\iota\colon \mathbb{C} \to \overline{\mathbb{Q}}_\ell$, put $|x|_\iota := |\iota(x)|_\ell$ for $x \in \mathbb{C}$, and let $\bar\iota \mid \ell$ be the isomorphism $x \mapsto \iota(\bar x)$. Let $\mathrm{Aut}(\mathbb{C})$ be the group of all field automorphisms of $\mathbb{C}$; most of them are not continuous. A *family* y assigns a complex number y_ι to every isomorphism $\iota \mid \ell$, for every prime ℓ.

Problem 5.3.1. Let $\iota \mid \ell$. If $x \in \mathbb{Q}$, then $|x|_\iota = |x|_\ell$. If $\ell \equiv 3 \pmod 4$ and $0 \neq x \in \mathbb{Z}[\mathrm{i}]$, then $|x|_\iota = \ell^{-v}$, where ℓ^v is the exact power of ℓ dividing x in $\mathbb{Z}[\mathrm{i}]$. If $\ell = 5$, then exactly one of $|2+\mathrm{i}|_\iota$ and $|2+\mathrm{i}|_{\bar\iota}$ equals $1/5$, and the other equals 1.

So the constant family 2+i has different absolute values at different isomorphisms above one prime. The following notion bounds a family by one number. Let $c \in \mathbb{R}$. A family y has *height at most* c if there are $H \in \mathbb{C}$, $\alpha \in \mathbb{R}$ and real numbers $h(\ell)$, one for each prime ℓ, such that

(i) $H \neq 0$, and $h(\ell) \geq 0$ for every prime ℓ;
(ii) $|\sigma H| \leq e^\alpha$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$;
(iii) $|Hy_\iota|_\iota \leq \ell^{h(\ell)}$ for every prime ℓ and every $\iota \mid \ell$;
(iv) $\alpha + \sum_{\ell \in U} h(\ell) \log \ell \leq c$ for every finite set U of primes.

The multiplier H and the bound α at infinity are common to all ι, while y_ι may depend on ι, even among the isomorphisms above one prime. There is no condition on the sign of α. We write $\mathrm{ht}(y) \leq c$ when y has height at most c.

Problem 5.3.2. If the families y and y' have heights at most c and c', then the family $\iota \mapsto y_\iota y'_\iota$ has height at most $c + c'$. If y has height at most c, then for every integer $n \geq 0$ the family $\iota \mapsto y_\iota^n$ has height at most nc.

Problem 5.3.3. (a) Let $e(\ell)$ be real numbers, of any sign, one for each prime ℓ, with $\sum_{\ell \in U} e(\ell) \leq c$ for every finite set U of primes. If $|y_\iota|_\iota \leq e^{e(\ell)}$ for every $\iota \mid \ell$, then y has height at most c. (b) If $H \neq 0$ and $|\sigma H| \leq e^c$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then the constant family H^{-1} has height at most c.

Can a height be negative? For the constant family 1, every admissible bound is nonnegative.

Problem 5.3.4. If $H \in \mathbb{C}$ is transcendental over $\mathbb{Q}$, then for every prime ℓ the numbers $|H|_\iota$, $\iota \mid \ell$, are unbounded. Hence a number H with $|H|_\iota \leq C$ for all $\iota \mid 2$ is algebraic.

Problem 5.3.5. If the constant family 1 has height at most c, then $c \geq 0$.

We now compare a height bound for a nonzero constant family with a uniform upper bound on the absolute values of its conjugates.

Theorem 5.3.1. *Let $z \in \mathbb{C}$, $z \neq 0$, and $c, c' \in \mathbb{R}$. If the constant family z has height at most c, and $|\sigma z| \leq e^{c'}$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then $-c \leq c'$.*

Problem 5.3.6. Let $x \in \mathbb{Q}^\times$. The constant family x has height at most c if and only if $c \geq -\log|x|$. For instance, the constant family 2 has height at most $-\log 2$.

If $g = \prod_{p\in S} p^{e_p}$, with S a finite set of primes, divides the nonzero integer Δ, then the constant family Δ has height at most $-\log g$, and Theorem 5.3.1 then gives (1).

Problem 5.3.7. Let S be a finite set of primes and $N := \prod_{\ell\in S} \ell$. The family with $y_\iota = \ell^{-1}$ for $\iota \mid \ell$ with $\ell \in S$, and $y_\iota = 1$ for $\iota \mid \ell$ with $\ell \notin S$, has height at most c if and only if $c \geq \log N$. For $S = \{2, 3\}$ the least height is $\log 6$.

5.4. Index and covolume

The minor Δ of Section 5.2 is a Gaussian integer and a determinant. In the proof the corresponding comparison is between Gram determinants of families of vectors: bounds on squared lengths control the size, and at each ι the rows of a matrix of controlled determinant give integral combinations of the vectors, which controls the divisibility. Here we use one map; the next chapter allows a choice of twist for each $\iota \mid \ell$.

For $\iota \mid \ell$ let $\mathcal{O}_\iota := \{x \in \mathbb{C} : |x|_\iota \leq 1\}$, a subring of $\mathbb{C}$. A *lattice datum* consists of

(i) a complex vector space V, a complex inner product space W, with $\langle\cdot,\cdot\rangle$ conjugate-linear in the first variable, and a linear map $\Theta\colon V \to W$;
(ii) for every prime ℓ and every $\iota \mid \ell$, an $\mathcal{O}_\iota$-submodule $\Lambda_\iota \subseteq W$, such that $|\langle\varphi, \varphi'\rangle|_\iota \leq 1$ for all $\varphi \in \Lambda_{\bar\iota}$ and $\varphi' \in \Lambda_\iota$;
(iii) a finite set I, a linear map $b\colon W \to \mathbb{C}^I$, and a matrix $G \in M_I(\mathbb{Q})$, positive definite as a complex matrix, with $\langle\varphi, \varphi'\rangle = b(\varphi)^* G\, b(\varphi')$ for all $\varphi, \varphi' \in W$, where * is the conjugate transpose.

A vector $y \in V$ is *integral at* ι if $\Theta y \in \Lambda_\iota$; these vectors form an $\mathcal{O}_\iota$-submodule M_ι of V. The *standard datum* on $\mathbb{C}^n$ has $V = W = \mathbb{C}^n$, $\Theta = b = \mathrm{id}$, $G = 1$ and $\Lambda_\iota = \mathcal{O}_\iota^n$.

Let S be a finite set, $y = (y_s)_{s\in S}$ a family of vectors of V, and $\delta \in \mathbb{R}$. The family y has *index at most* δ if there are real numbers $e(\ell) \geq 0$, one for each prime ℓ, with $\sum_{\ell\in U} e(\ell)\log\ell \leq \delta$ for every finite set U of primes, such that for every $\iota \mid \ell$ some matrix $u \in M_S(\mathcal{O}_\iota)$ satisfies

$$|\det u|_\iota \geq \ell^{-e(\ell)} \quad \text{and} \quad \sum_{k\in S} u_{ik}\, y_k \in M_\iota \text{ for every } i \in S.$$

The matrix may depend on ι. Every admissible δ is nonnegative.

Problem 5.4.1. The standard datum satisfies condition (ii). In it, a family of vectors with entries in $\mathbb{Z}[\mathrm{i}]$ has index at most 0. On $\mathbb{C}^1$, the family consisting of the one vector $1/3$ has index at most δ if and only if $\delta \geq \log 3$.

Problem 5.4.2. If $y = (y_s)_{s\in S}$ has index at most δ and $y' = (y'_s)_{s\in S'}$ has index at most δ', then the family indexed by the disjoint union $S \sqcup S'$ that restricts to y and y' has index at most $\delta + \delta'$.

An index bound is usually proved one submodule at a time. For $\mathcal{O}_\iota$-submodules M, M' of V and $z \in \mathcal{O}_\iota$, say that *the colength of M' in M divides z* if for every $n \geq 0$ and all $\Phi_1, \ldots, \Phi_n \in M$ there is a matrix $m \in M_n(\mathcal{O}_\iota)$ such that $\det m$ divides z in $\mathcal{O}_\iota$ and $\sum_k m_{ik}\Phi_k \in M'$ for every i. No inclusion between M and M' is assumed. This colength condition gives an upper bound for the index.

Theorem 5.4.1. *Let $y_1, \ldots, y_n \in V$, $\delta \in \mathbb{R}$, and let $e(\ell) \geq 0$, one for each prime ℓ, satisfy $\sum_{\ell\in U} e(\ell)\log\ell \leq \delta$ for every finite set U of primes. Suppose that for every $\iota \mid \ell$ there are an integer $j \geq 0$ and an $\mathcal{O}_\iota$-submodule $M \subseteq V$ such that $j \leq e(\ell)$,*

every y_i lies in M, and the colength of M_ι in M divides ℓ^j. Then y has index at most δ.

Problem 5.4.3. Let $\Lambda \subset \mathbb{Q}^n$ be a subgroup that contains $\mathbb{Z}^n$ with finite index N, and let $y_1, \dots, y_n$ be a basis of Λ. In the standard datum on $\mathbb{C}^n$, the family y has index at most $\log N$, and $\det(y_i^* y_k)_{i,k} = N^{-2}$.

Now the size. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $y \in V$ let $v_\sigma(y) \in \mathbb{C}^I$ be the vector $b(\Theta y)$ with σ applied to each coordinate, and let $N(y,\sigma) := \mathrm{Re}\big(v_\sigma(y)^* G\, v_\sigma(y)\big)$. A family $y = (y_s)_{s\in S}$ has *covolume at most c* if

$$\big|\det\big(v_\sigma(y_i)^* G\, v_\sigma(y_k)\big)_{i,k\in S}\big| \le e^c \quad \text{for every } \sigma \in \mathrm{Aut}(\mathbb{C}).$$

For $\sigma = \mathrm{id}$ the determinant is the Gram determinant of the vectors Θy_s, the square of a volume. So the family of Problem 5.4.3 has covolume at most c exactly when $c \ge -2\log N$. In the next example G differs from the identity when $D \ge 3$. For $f \in \mathbb{C}[z]$ let

$$\|f\|^2 := \frac{1}{\pi}\int_{\mathbb{C}} |f(z)|^2 e^{-|z|^2}\, dA(z).$$

Problem 5.4.4. The monomials are orthogonal, and $\|z^a\|^2 = a!$.

Problem 5.4.5. Let D be a positive integer, let $V = W$ be the polynomials of degree less than D with the inner product of Problem 5.4.4, $\Theta = \mathrm{id}$, $b(f) = (f_0, \dots, f_{D-1})$ the coefficients, $G = \mathrm{diag}(0!, 1!, \dots, (D-1)!)$, and Λ_ι the polynomials with coefficients in $\mathcal{O}_\iota$. This is a lattice datum. In it, the family $(z^a/a!)_{0\le a<D}$ has index at most $\sum_{a<D} \log a!$, and covolume at most c if and only if $c \ge -\sum_{a<D}\log a!$. For $D = 4$ the sum is $\log 12$.

Problem 5.4.6. Let $G \in M_I(\mathbb{C})$ be positive semidefinite and $w_1, \dots, w_n \in \mathbb{C}^I$. Then $|\det(w_i^* G w_k)_{i,k}| \le \prod_i w_i^* G w_i$. For $G = 1$ and the columns $(6,6)$ and $(10,20)$ of Problem 5.1.3 the two sides are 3600 and 36000.

A uniform bound on squared norms gives a covolume bound.

Theorem 5.4.2. *Let $y_1, \dots, y_n \in V$ and $h \in \mathbb{R}$. If $N(y_i, \sigma) \le e^h$ for every i and every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then y has covolume at most nh.*

The hypothesis concerns every σ. For the vector $1 - \sqrt{2}$ in the standard datum on $\mathbb{C}^1$, $N(1-\sqrt{2}, \mathrm{id}) = 3 - 2\sqrt{2}$, but $N(1-\sqrt{2}, \sigma) = 3 + 2\sqrt{2}$ when $\sigma\sqrt{2} = -\sqrt{2}$.

Size and divisibility now meet in one determinant. Let $y_1, \dots, y_n \in V$, and let $\Gamma := \det(\langle \Theta y_i, \Theta y_k\rangle)_{i,k}$ be their Gram determinant. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ let σ' be the automorphism $x \mapsto \overline{\sigma(\bar{x})}$.

Problem 5.4.7. For $y, y' \in V$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$, $\sigma\langle \Theta y, \Theta y'\rangle = v_{\sigma'}(y)^* G\, v_\sigma(y')$.

Problem 5.4.8. Let $G \in M_I(\mathbb{C})$ be positive semidefinite, and let A, B be $I \times n$ matrices. Then $|\det(A^* G B)|^2 \le |\det(A^* G A)|\,|\det(B^* G B)|$. Consequently, if y has covolume at most c, then $|\sigma\Gamma| \le e^c$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$.

Problem 5.4.9. Let $\iota \mid \ell$, and let $u, u' \in M_n(\mathbb{C})$ satisfy $\sum_k u_{ik} y_k \in M_\iota$ and $\sum_k u'_{ik} y_k \in M_{\bar\iota}$ for every i. Then $|\overline{\det u'}|_\iota\, |\Gamma|_\iota\, |\det u|_\iota \le 1$. Consequently, if y has index at most δ, then the constant family Γ has height at most 2δ.

If Θ is injective and y is a basis of V, then $\Gamma \ne 0$.

Theorem 5.4.3. *Let Θ be injective, and let $y_1, \dots, y_n$ be a basis of V. If y has covolume at most c and index at most δ, then*

$$0 \le c + 2\delta.$$

By Problems 5.4.1 and 5.4.3, equality holds for the vector $1/3$ in $\mathbb{C}^1$, with $c = -2\log 3$ and $\delta = \log 3$, and for a basis of a lattice $\Lambda \supseteq \mathbb{Z}^n$. In the datum of Problem 5.4.5 the bounds found there give $c + 2\delta = \sum_{a<D} \log a!$.

Problem 5.4.10. In the setting of Theorem 5.2.1, let Δ be a nonzero $s \times s$ minor of the matrix of ev, let $g := \prod_{p \in P} p^{N_p}$, and let $B := s!\, A_*^{s(J-1)} \beta^D$. In the standard datum on $\mathbb{C}^1$, the vector Δ/g has index at most 0 and covolume at most $2\log(B/g)$, and Theorem 5.4.3 gives Theorem 5.2.1. For $P = \{3\}$, $I = 1$, $u_1 = \mathrm{i}$, $J = 2$ and $\mathcal{T} = \{(3,0),(0,1)\}$: $\Delta = \pm 3\mathrm{i}$, $g = 3$ and $B = 18$.

In the Lean formalization. In the Lean proof [GL], the height bound $\mathrm{ht}(y) \le c$ is `HeightLe`, Problem 5.3.5 is `HeightLe.nonneg_of_one` and Theorem 5.3.1 is `HeightLe.neg_le_of_norm_map_le` (file `New/Reduction/Lattices/Heights.lean`). In `HeightLe` and `TwistedLattice.IndexLe`, respectively, the functions h and e are defined on all natural numbers and are nonnegative everywhere. Only their values at primes occur in the local bounds and finite sums. A lattice datum is a `TwistedLattice` with a single twist, allowed at every $m \in \mathbb{N}$; index and covolume are `TwistedLattice.IndexLe` and `TwistedLattice.CovolumeLe`, Theorems 5.4.1 and 5.4.2 are `TwistedLattice.indexLe_of_colengthDvd` and `TwistedLattice.covolumeLe_of_normSqAt_le`, and Theorem 5.4.3 is the case of `TwistedLattice.covolume_add_index_nonneg` with this single twist, no completing vectors, the auxiliary scalar 1 and the three auxiliary bounds 0, for any inner product on V (file `New/Reduction/Lattices/TwistedLattice.lean`).

Theorem 5.4.3 compares the size and divisibility bounds for a single nonzero Gram determinant. In the proof, integrality at $\iota \mid \ell$ is tested through every map allowed at ℓ, one allowed map is chosen for each ι, and the covolume is read through the map of the trivial twist; Chapter 6 adds a height bound for the family whose value at ι is the squared volume of the trivial map divided by that of the chosen map.

Hints

§5.1.

5.1.1: Write $\binom{2n}{n} = (2n)!/(n!)^2$. For the size, expand $(1+1)^{2n}$.
5.1.2: Count the multiples of p^e up to n.
5.1.3: Divide each column by g_j.

§5.2.

5.2.1: The binomial theorem modulo p.
5.2.2: Problem 5.2.1 and the Leibniz rule.
5.2.3: Write $a = kp + t$ with $0 \le t < p$, and consider the polynomials $X^t Y^b g^k$.

§5.3.

5.3.1: The restriction of $|\cdot|_\iota$ to $\mathbb{Q}(\mathrm{i})$ is an absolute value extending $|\cdot|_\ell$. For $\ell = 5$: $(2+\mathrm{i})(2-\mathrm{i}) = 5$, and $\bar{\iota}(2+\mathrm{i}) = \iota(2-\mathrm{i})$.
5.3.2: Multiply the multipliers.
5.3.3: (a) Take $H = 1$. (b) Take the multiplier H.

5.3.4: Fix one $\iota_0 \mid \ell$. Extend an isomorphism $\mathbb{Q}(H) \to \mathbb{Q}(\iota_0^{-1}(t))$, for a suitable transcendental $t \in \overline{\mathbb{Q}}_\ell$, to an automorphism of $\mathbb{C}$.

5.3.5: Problem 5.3.4, then the product formula for the norm of H from $\mathbb{Q}(H)$ to $\mathbb{Q}$.

5.3.6: Take $H = x^{-1}$; for the converse, Theorem 5.3.1.

5.3.7: Compare with the constant family $1/N$.

§5.4.

5.4.1: At $\iota \mid 3$ a 1×1 matrix (u) must satisfy $|u|_\iota \leq 1/3$.

5.4.2: Block diagonal matrices.

5.4.3: Express the standard basis in terms of y.

5.4.4: Polar coordinates.

5.4.5: A diagonal matrix.

5.4.6: The matrix $(w_i^* G w_k)$ is positive semidefinite.

5.4.7: The entries of G are rational.

5.4.8: The Gram matrix of the $2n$ columns of A and B is positive semidefinite; apply a Schur complement after adding ε times the identity, and let $\varepsilon \to 0$. Then Problem 5.4.7.

5.4.9: Compare the matrix of inner products of the two transformed families with that of the vectors Θy_k. Then Problem 5.3.3(a).

5.4.10: An automorphism of $\mathbb{C}$ restricts to the identity or to complex conjugation on $\mathbb{Q}(\mathrm{i})$.

References

[Bom] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, Exp. 430, Lecture Notes in Math. 383, Springer, 1974, 234–241.

[Ch] P. L. Chebyshev, *Mémoire sur les nombres premiers*, J. Math. Pures Appl. **17** (1852), 366–390.

[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/`.

[La] S. Lang, *Algebra*, rev. 3rd ed., Grad. Texts in Math. 211, Springer, 2002.

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