# THE CHAIN AND THE SQUARE ROOT

Prerequisites. Finite fields and Euler's criterion; polynomials over a field, their roots and multiplicities; a homogeneous linear system with more unknowns than equations has a nonzero solution. Lattices in a Euclidean space and their covolumes [Ne, Ch. I, §4]; the adjoint of a linear map between inner product spaces. The von Mangoldt function $\Lambda$ and Mertens' estimate $\sum_{n\le x}\Lambda(n)/n = \log x + O(1)$. The problems in Sections 8.1–8.4 require no earlier chapter; Chapter 7, *Stepanov without multiplicity*, is their motivation: one determinant, without multiplicity, is the case $m = 1$ of the chain. Section 8.5 uses the function $G$ of (1) and Theorem 1.2.1 of Chapter 1. The closing paragraphs of Sections 8.4 and 8.5 point to Chapters 6, 33, 55 and 35; Problem 8.5.5 states what it needs as hypotheses.

## 8.1. The auxiliary polynomial

How can a polynomial show that a set of about $q/2$ elements of $\mathbb{F}_q$ has at most $q/2+O(\sqrt{q})$ elements? Stepanov's answer [Ste69] is to make it vanish to high order on the set. We follow his method for the curve $y^2 = f(x)$.

Let $q$ be a power of an odd prime $p$, and let $f \in \mathbb{F}_q[X]$ have odd degree $d = 2g+1$ with $3 \le d < q$. Let

$$c := \frac{q-1}{2}, \qquad D := \frac{q-d}{2}.$$

For $\eta \in \{1,-1\}$ let $S_\eta := \{x \in \mathbb{F}_q : f(x)^c = \eta\}$, let $S_0 := \{x \in \mathbb{F}_q : f(x) = 0\}$, and let $N^{\mathrm{aff}}$ be the number of solutions $(x,y) \in \mathbb{F}_q^2$ of $y^2 = f(x)$.

**Problem 8.1.1.** $\mathbb{F}_q$ is the disjoint union of $S_1$, $S_{-1}$ and $S_0$, and $N^{\mathrm{aff}} = 2|S_1|+|S_0|$. For $q = 7$ and $f = X^3 - X$, $S_1 = \{4,5\}$, $S_{-1} = \{2,3\}$ and $N^{\mathrm{aff}} = 7$.

Hence $N^{\mathrm{aff}} - q = |S_1| - |S_{-1}|$, and a bound $|S_\eta| \le q/2 + B$ for both signs gives $|N^{\mathrm{aff}}-q| \le 2B+d$. For squarefree $f$, Weil's theorem [Wei48] gives $|N^{\mathrm{aff}}-q| \le 2g\sqrt{q}$.

The principle is the count of zeros against the degree: if $F \in \mathbb{F}_q[X]$ is nonzero and vanishes to order at least $\ell$ at every point of $S_\eta$, then

$$\ell\,|S_\eta| \le \deg F. \tag{1}$$

The polynomials $f^c-\eta$ and $X^q-X$ vanish on $S_\eta$, and give $|S_\eta| \le dc$ and $|S_\eta| \le q$. To reach $q/2$ one needs $\deg F/\ell$ close to $q/2$. Stepanov combines the two polynomials. Let $J \ge 1$ be an integer, and let $r_j, s_j \in \mathbb{F}_q[X]$, for $0 \le j < J$, have degree less than $D$ and be not all zero. The *auxiliary polynomial* is

$$F := \sum_{j<J} \bigl(r_j + s_j f^c\bigr) X^{jq}. \tag{2}$$

**Problem 8.1.2.** $\deg f^c = gq + D$, and $2D < q$.

**Problem 8.1.3.** The nonzero terms $r_j X^{jq}$ and $s_j f^c X^{jq}$ of (2) have pairwise distinct degrees. Hence $F \ne 0$ and $\deg F \le (J+g)q - d - 1$.

---

*Date*: November 26, 2026.

For $x \in S_\eta$ we have $x^{jq} = x^j$ and $f(x)^c = \eta$, so $F(x) = C_0(x)$, where

$$C_0 := \sum_{j<J} (r_j + \eta s_j) X^j.$$

If $C_0 = 0$, then $F$ vanishes on all of $S_\eta$.

**Problem 8.1.4.** If $C_0 = 0$, then $\deg F \geq q$. If $D \geq 2$ and $J \geq 2$, the tuple $r_0 = -X$, $r_1 = 1$, all others zero, gives $F = X^q - X$.

So the gain must come from the order of vanishing.

## 8.2. Vanishing to order $\ell$

In characteristic $p$ the derivative of order $p$ vanishes identically, so one uses Hasse derivatives. For $G \in \mathbb{F}_q[X]$ define $H^k G \in \mathbb{F}_q[X]$ by

$$G(X+Y) = \sum_{k \geq 0} (H^k G)(X)\, Y^k \qquad \text{in } \mathbb{F}_q[X,Y].$$

**Problem 8.2.1.** For $0 \leq k \leq n$, $H^k(X^n) = \binom{n}{k} X^{n-k}$, and $H^k(X^n) = 0$ for $k > n$. Also $H^k(G_1 G_2) = \sum_{i \leq k} H^i G_1 \cdot H^{k-i} G_2$. For $\alpha \in \mathbb{F}_q$, $(X-\alpha)^\ell$ divides $G$ if and only if $(H^k G)(\alpha) = 0$ for all $k < \ell$.

**Problem 8.2.2.** $(X+Y)^{jq} = (X^q + Y^q)^j$. Hence $H^k(GX^{jq}) = (H^k G) X^{jq}$ for $k < q$.

To differentiate $f^c$, write $f(X+Y)^c = f(X)^c \big(f(X+Y)/f(X)\big)^c$ and define $U_i \in \mathbb{F}_q(X)$ by

$$\Big(\frac{f(X+Y)}{f(X)}\Big)^c = \sum_{i \geq 0} \frac{U_i}{f^i}\, Y^i \qquad \text{in } \mathbb{F}_q(X)[[Y]].$$

**Problem 8.2.3.** Each $U_i$ is a polynomial of degree at most $i(d-1)$. Moreover $U_0 = 1$ and $U_1 = cf'$.

For $k \geq 0$ let

$$C_k := \sum_{j<J} \Big( f^k H^k r_j + \eta \sum_{i \leq k} f^{k-i} U_i\, H^{k-i} s_j \Big) X^j. \tag{3}$$

For $k = 0$ this is the polynomial $C_0$ of Section 8.1.

**Problem 8.2.4.** Let $\alpha \in S_\eta$, so that $f(\alpha) \neq 0$, and let $k < q$. Then $(H^k F)(\alpha) = f(\alpha)^{-k} C_k(\alpha)$.

**Problem 8.2.5.** $\deg C_k \leq D + J - 2 + k(d-1)$.

By Problems 8.2.1 and 8.2.4, if $\ell \leq q$ and

$$C_0 = C_1 = \cdots = C_{\ell-1} = 0, \tag{4}$$

then $F$ vanishes to order at least $\ell$ at every point of $S_\eta$, whatever $S_\eta$ is.

## 8.3. The count and the balance

**Problem 8.3.1.** If $2JD > \ell(D+J-1)+(d-1)\ell(\ell-1)/2$, then there is an auxiliary polynomial (2) satisfying (4).

**Problem 8.3.2.** Let $\ell$ be an even integer with $0 \le \ell < q-d$, and let $J = \ell/2 + t$. Then

$$2JD - \ell(D+J-1) - (d-1)\frac{\ell(\ell-1)}{2} = t\,(q-d-\ell) - \frac{d\ell^2 - (d+1)\ell}{2}.$$

Hence the hypothesis of Problem 8.3.1 holds if $t > d\ell^2/\big(2(q-d-\ell)\big)$.

The preceding problems give the following estimate.

**Theorem 8.3.1** (A bound by Stepanov's method)**.** *Let $\ell$ be even with $2 \le \ell < q-d$, and let $t := \lfloor d\ell^2/(2(q-d-\ell))\rfloor + 1$. Then, for $\eta = \pm 1$,*

$$|S_\eta| \le \frac{q}{2} + \frac{(g+t)\,q}{\ell}.$$

This is Stepanov's method [Ste69]; see [Sch76] for Hasse derivatives. For example, for $q = 1009$, $d = 3$ and $\ell = 24$ one has $t = 1$, and the bound is $588.58\ldots$; for $f = X^3 + X + 1$ the sets have $|S_1| = 516$ and $|S_{-1}| = 492$.

**Problem 8.3.3.** If $q \ge 16d^2$ and $\ell$ is an even integer with $|\ell - \sqrt{q}| \le 1$, then $|S_\eta| \le q/2 + 2d\sqrt{q}$ for $\eta = \pm 1$, and $|N^{\mathrm{aff}} - q| \le 4d\sqrt{q} + d$.

Where does the square root come from? Write $(J+g)q - d - 1 = \frac{\ell}{2}q + \big((g+1)q - d - 1\big) + (t-1)q$. After division by $\ell$ the first term is the main term $q/2$. The second is paid once, however high the order. The third comes from the growing number of equations of the $k$th identity, through $t - 1 = \lfloor d\ell^2/(2(q-d-\ell))\rfloor$. For fixed $d$ and $d + \ell \le q/2$ the error term is $O_d(q/\ell + \ell)$, of the shape $q/m + m$, and the two terms of this upper bound balance at $\ell$ of order $\sqrt{q}$.

**Problem 8.3.4.** For every $\ell$ as in Theorem 8.3.1, $(g+t)q/\ell > \sqrt{2gdq}$.

Thus the error term in Theorem 8.3.1 never gives $o(\sqrt{q})$. We expect the same for Bombieri's form [Bom74], but do not prove it here.

## 8.4. The chain inequality

What does a chain of $m$ linear maps give that one map does not?

Let $V$ and $W$ be Euclidean spaces of the same dimension $n \ge 1$, with lattices $L \subset V$ and $M \subset W$ of rank $n$. The *volume* of a linear map $u\colon V \to W$ is $\det(u^*u)$, where $u^*$ is the adjoint; in orthonormal bases it is $(\det u)^2$.

**Problem 8.4.1.** Let $u\colon V \to W$ be injective, and let $\lambda > 0$ be real with $u(L) \subseteq \lambda M$. Then

$$n \log \lambda \le \log \mathrm{covol}(L) - \log \mathrm{covol}(M) + \tfrac{1}{2}\log\det(u^*u).$$

For $L = M = \mathbb{Z}$, $u$ the multiplication by 6 and $\lambda = 6$, both sides are $\log 6$.

Let $m \ge 1$ be an integer, and let $V_0, \ldots, V_m$ be Euclidean spaces of dimension $n$ with lattices $L_j \subset V_j$ of rank $n$. Let $u_j\colon V_{j-1} \to V_j$ be linear maps and $\lambda_j > 0$ real numbers with $u_j(L_{j-1}) \subseteq \lambda_j L_j$, and let $\Psi := u_m \circ \cdots \circ u_1$.

**Problem 8.4.2.** $\det(\Psi^*\Psi) = \prod_{j=1}^m \det(u_j^* u_j)$, also when some $u_j$ is not injective. The identity fails for spaces of different dimensions: for $u_1(x) = (x, 0)$ from $\mathbb{R}$ to $\mathbb{R}^2$ and $u_2(y, z) = y$ from $\mathbb{R}^2$ to $\mathbb{R}$ the left side is 1 and the right side is 0.

**Problem 8.4.3.** $\Psi(L_0) \subseteq \lambda_1 \cdots \lambda_m L_m$. In particular, if $u_j(L_{j-1}) \subseteq p^{e_j} L_j$ for each $j$, then $\Psi(L_0) \subseteq p^{e_1+\cdots+e_m} L_m$.

For the composite of the chain we have the following inequality; if $\Psi$ is injective, then so is every $u_j$, because all dimensions are equal.

**Theorem 8.4.1** (Chain inequality)**.** *If $\Psi$ is injective, then*

$$n \sum_{j=1}^m \log \lambda_j \le \log \operatorname{covol}(L_0) - \log \operatorname{covol}(L_m) + \frac{1}{2} \sum_{j=1}^m \log \det(u_j^* u_j).$$

The right side uses the two ends and the volume of each step, and the ends are paid once: if $\Psi$ is injective, $\log \lambda_j \ge \beta$ and $\frac{1}{2n} \log \det(u_j^* u_j) \le \sigma$ for every $j$, and $\frac{1}{n}(\log \operatorname{covol}(L_0) - \log \operatorname{covol}(L_m)) \le c_{\mathrm{end}}$, then $\beta \le \sigma + c_{\mathrm{end}}/m$.

**Problem 8.4.4.** Suppose that every $u_j$ is injective. The sum of the inequalities of Problem 8.4.1 for $u_1, \ldots, u_m$ and $\lambda_1, \ldots, \lambda_m$ is the inequality of Theorem 8.4.1.

Measured by volumes, then, the intermediate lattices cost nothing. The product of the operator norms, by contrast, can strictly exceed the operator norm of the composite.

**Problem 8.4.5.** Let $w \ge 2$ be an integer, $L_0 = L_2 = \mathbb{Z}^2$ and $L_1 = \mathbb{Z}e_1 + \mathbb{Z}we_2$, all in $\mathbb{R}^2$ with the standard norm, and let $u_1(x, y) = (x, wy)$ and $u_2(x, y) = (x, y/w)$. Then $\lambda_1 = \lambda_2 = 1$ are the largest admissible scalars, $\det(u_1^* u_1) = w^2$, $\det(u_2^* u_2) = w^{-2}$, and the inequalities of Problem 8.4.1 for $u_1$, $u_2$ and of Theorem 8.4.1 are equalities. But $\|u_1\| \, \|u_2\| = w$, while $\Psi$ is the identity.

A divisibility is often known only on a sublattice. Its index is a loss, paid once.

**Problem 8.4.6.** Suppose that $\Psi$ is injective and that $\Psi(L_0') \subseteq \lambda L_m$ for a sublattice $L_0' \subseteq L_0$ of finite index and a real $\lambda > 0$. Then

$$n \log \lambda \le \log \operatorname{covol}(L_0) - \log \operatorname{covol}(L_m) + \frac{1}{2} \sum_{j=1}^m \log \det(u_j^* u_j) + \log [L_0 : L_0'].$$

Theorem 6.2.1 gives a related index and covolume inequality for a twisted lattice. For the chain of the proof, the determinant divided by its value at the trivial twist is the product of the corresponding quotients for the single lifts, times a correction factor (Theorem 55.4.1). This factor is a power of the norm of the modulus times a product of ratios of absolute values of partial Hecke $L$-values, all raised to the dimension of the target forms.

How precisely must the two ends and the volumes of the steps be known?

## 8.5. The budget $x/m + m$

How long should the chain be? Let $G(x) = \sum_{n \le x} \Lambda(n)(x/n - 1) - x \log x + (1 + \gamma)x$ be the function of (1) in Chapter 1. By Mertens' estimate, $G(x) = O(x)$. By Theorem 1.2.1, if $G(x) \le x^\theta$ for some $0 < \theta < 1$ and all large $x$, then $\zeta(s) \ne 0$ for $\operatorname{Re} s > \theta$. So a one-sided bound with exponent $\frac{1}{2}$ gives the Riemann hypothesis.

Let $a, b > 0$ and $x := a/b$. As in Section 1.3, $(a/p^e - b)_+ = b(x/p^e - 1)_+$, so that

$$\sum_p \log p \sum_{e\ge 1} \Big(\frac{a}{p^e} - b\Big)_+ = b \sum_{\nu \le x} \Lambda(\nu) \Big(\frac{x}{\nu} - 1\Big),$$

where $u_+ := \max(u, 0)$; for integral $a$ the inner sum is a smoothed analogue of Legendre's sum $\sum_{e\ge 1} \lfloor a/p^e \rfloor$ for $v_p(a!)$. We consider a chain as in Section 8.4, with $\Psi$ injective, and real numbers $c_{\mathrm{end}}$ and $c_1, \dots, c_m$ such that for $1 \le j \le m$

$$\begin{gathered} \log \lambda_j \ge b \sum_{\nu \le x} \Lambda(\nu) \Big(\frac{x}{\nu} - 1\Big), \qquad \frac{1}{2n} \log \det(u_j^* u_j) \le a(\log x - 1 - \gamma) + c_j, \\ \frac{1}{n} \big(\log \mathrm{covol}(L_0) - \log \mathrm{covol}(L_m)\big) \le c_{\mathrm{end}}. \end{gathered} \tag{5}$$

Here $c_{\mathrm{end}}$ is the cost at the ends, and $c_j$ the cost of the $j$th step. This models the bookkeeping only.

**Problem 8.5.1.** Under (5), $G(x) \le (c_{\mathrm{end}} + c_1 + \cdots + c_m)/(mb)$.

**Problem 8.5.2.** If $c_{\mathrm{end}} = a$ and $c_j = (2j-1)b$, then $G(x) \le x/m + m$. With $m = \lceil \sqrt{x} \rceil$ this gives $G(x) \le 2\sqrt{x} + 1$. For $x = 10^6$ the bound is 2000 at $m = 1000$ and 10100 at $m = 100$.

What happens if the cost at the ends is paid separately for every step?

**Problem 8.5.3.** Retain the first two bounds of (5). Suppose that every $u_j$ is injective and that Problem 8.4.1 is applied to each $u_j$ separately, with $\frac{1}{n}(\log \mathrm{covol}(L_{j-1}) - \log \mathrm{covol}(L_j)) \le a$ for every $j$ and $c_j = (2j-1)b$. Then the $j$th step gives $G(x) \le x + 2j - 1$, so the best of these bounds is $G(x) \le x + 1$, the bound for $m = 1$.

**Problem 8.5.4.** $\sum_{j=1}^m (3j^2 - 3j + 1) = m^3$. So if $c_{\mathrm{end}} = a$ and $c_j = (3j^2 - 3j + 1)b$, then $G(x) \le x/m + m^2$. For every $m > 0$, $x/m + m^2 \ge 3 \cdot 2^{-2/3} x^{2/3}$. For $x = 10^6$ the least value over integers $m$ is $18899.2\ldots$, at $m = 79$.

If such chains exist for every sufficiently large $x$ at a length minimizing the bound in Problem 8.5.4, that bound gives $G(x) \le x^\theta$ eventually for each $\theta > 2/3$, and hence a zero-free half-plane $\mathrm{Re}\, s > 2/3$ for $\zeta$. The exponent is decided by how the total cost grows with the length of the chain.

The chain of the proof. This chapter serves the main inequality. Chapter 35 proves $m \cdot \mathrm{rem} \le f a \log^5 b$ (Theorem 35.2.1) and deduces a bound for $R_{d,q_0}(x)$. From here on $f$ is the number of infinite places of the field $E$, $k = r + 1 - m$ is the rank of the source, and $U = f a \log^3 b$ is the unit of error, all as in Chapter 33 (they are not the polynomial $f$ and the index $k$ of Sections 8.1–8.3); the data have $\sqrt{x} \le m \le 2\sqrt{x}$. In the proof two estimates involve $m$ through $m^2$ relative to their budgets. First, the level $N$ is a prime with $m \log b \le \log N \le 30 m \log b$; the allowed loss at $N$ is $2mfb$ (here $N \ge b > x_1$, so $N$ is not a small non-split prime); and for every finite set of natural numbers the sum over its elements $p$ of the allowed loss at $p$ times $\log p$, with the summand at $p = 0$ defined to be zero, is at most $U$. Second, local defect bounds $\delta_p$ satisfy $\sum_{p \in T} \delta_p \log p \le C_{\mathrm{loc}} f (m/k) b \log b$ for every finite set $T$ of primes, with $C_{\mathrm{loc}} = 4 \cdot 10^6 e^{180}$, while for each lift index the sum of the logarithmic denominator bounds over every finite set of primes must be at most $B = U/(mk)$.

**Problem 8.5.5.** Let $m, x, f, k > 0$, $b > 1$, $L := \log b$, $a := xb$ and $U := faL^3$. (a) If $mL \le \log N \le 30mL$, then $2m^2fbL \le 2mfb\log N \le 60m^2fbL$; hence $2mfb\log N \le U$ forces $m \le L\sqrt{x/2}$, and holds if $m \le L\sqrt{x/60}$. (b) For $C_{\mathrm{loc}} > 0$, $C_{\mathrm{loc}} f(m/k)bL \le U/(mk)$ if and only if $m \le L\sqrt{x/C_{\mathrm{loc}}}$.

The data have $\log\log b \ge 10^{12}C$, with $C \ge 1$ the constant of Chapter 33, so both comparisons of Problem 8.5.5 hold in the range $\sqrt{x} \le m \le 2\sqrt{x}$. Up to powers of $\log b$, the length has the same square-root scale as in Problem 8.5.2.

In the Lean formalization. In the Lean proof [GL] the main inequality is `New.star_inequality` (`grh/src/New/Reduction/MainInequality.lean`); the allowed loss is `New.Data.allowedLoss`, and the estimates used in the discussion of Problem 8.5.5 are `New.Data.log_N_mem_Icc`, `New.Data.sum_allowedLoss_mul_log_le`, `New.Selmer.sum_localDefectBound_mul_log_le` and `New.Data.IsDenominatorBound.sum_le` with `New.Data.denominatorBudget`, together with the fields `N_prime`, `m_mem` and `constantBound_le` of `New.Data`.

## Hints

**§8.1.**

**8.1.1:** Euler's criterion: $f(x)$ is a nonzero square in $\mathbb{F}_q$ exactly when $f(x)^c = 1$.

**8.1.2:** Substitute $d = 2g + 1$ in $dc$.

**8.1.3:** Look at the quotient and the remainder of each degree on division by $q$.

**8.1.4:** If $r_j = s_j = 0$ for all $j \ge 1$, then $s_0 \ne 0$. Otherwise use Problem 8.1.3.

**§8.2.**

**8.2.1:** For the last statement, expand $G(\alpha + Y)$ and substitute $Y = X - \alpha$.

**8.2.2:** The map $u \mapsto u^q$ is a ring homomorphism in characteristic $p$.

**8.2.3:** Write $f(X + Y) = f(X) + \Delta$ with $\Delta = \sum_{k\ge1}(H^k f)Y^k$, and expand $(1 + \Delta/f)^c$ by the binomial theorem. Note $\deg H^k f \le d - k$.

**8.2.4:** Expand $F(\alpha + Y)$ modulo $Y^{k+1}$. Use Problem 8.2.2, $\alpha^q = \alpha$, and $f(\alpha)^c = \eta$.

**8.2.5:** Bound each of the two kinds of terms in (3) separately, using Problem 8.2.3.

**§8.3.**

**8.3.1:** Compare the number of unknowns with the upper bound for the number of equations from Problem 8.2.5.

**8.3.2:** Use $2D = q - d$.

**8.3.3:** Check that $\sqrt{q} \ge 12$, $q - d - \ell \ge 8q/9$ and $11\sqrt{q}/12 \le \ell \le 13\sqrt{q}/12$. Then bound $t - 1$ and $g$ by multiples of $d$.

**8.3.4:** $t > d\ell^2/(2q)$. Then use the inequality between arithmetic and geometric means.

**§8.4.**

**8.4.1:** Compare $\mathrm{covol}(u(L)) = |\det u|\,\mathrm{covol}(L)$ with $\mathrm{covol}(\lambda M)$.

**8.4.2:** Take orthonormal bases. For the counterexample write out the $2 \times 2$ matrix of $u_2^* u_2$.

**8.4.3:** Track the image of one lattice vector along the chain.

**8.4.4:** Follow the coefficient of each intermediate $\log \operatorname{covol}(L_j)$.
**8.4.5:** $u_1(L_0) = L_1$ and $u_2(L_1) = L_2$.
**8.4.6:** Apply Problem 8.4.1 to $\Psi$ and the lattice $L_0'$.

**§8.5.**

**8.5.1:** Divide Theorem 8.4.1 by $n$ before applying (5).
**8.5.2:** Write $2j - 1$ as a difference of consecutive squares.
**8.5.3:** Each step gives a bound for the same quantity.
**8.5.4:** Minimize over real $m > 0$ first.

## References

[Bom74] 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.

[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/`.

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

[Sch76] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Math. **536**, Springer, 1976.

[Ste69] S. A. Stepanov, *On the number of points of a hyperelliptic curve over a finite prime field*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1171–1181.

[Wei48] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, 1948.