On the Hermite-Minkowski theorem

Gaëtan Chenevier

June 7th, 2018

Goal = discuss certain finiteness results and conjectures in algebraic number theory and arithmetic geometry. The simplest instance of them is a result known as the Hermite-Minkowski theorem. I will start from it and then move to Galois representations.

1 The Hermite-Minkowski theorem

First, I want to recall what is the discriminant of a polynomial.

Fix k a field and P in $k[X]$ monic. Write $P = \prod_i (X - \lambda_i)$ in $\overline{k}[X]$ and set $\operatorname{disc} P = \prod_{i<j}(\lambda_i - \lambda_j)^2$. This is a universal polynomial with coeff. in $\mathbb{Z}$ in the coefficients of P (with famous formulas in low degree, however quickly ugly); this is an element of k which vanishes iff P has a multiple root in $\overline{k}$. Alternatively, we have $\operatorname{disc} P = \pm \operatorname{Res}(P, P')$.

Assume $P \in \mathbb{Z}[X]$. Then for any prime p we have $(\operatorname{disc} P) \bmod p = \operatorname{disc}(P \bmod p)$. In particular, the prime factors p are exactly the ones such that $P \bmod p$ has multiple root in $\overline{\mathbb{F}}_p$. If P is irreducible then $\operatorname{disc} P \neq 0$, finitely many such p. Arguing in the p-adic numbers would also show that p-adic valuation of $\operatorname{disc} E$ is big if some λ_i are congruent modulo big powers of p.

Several interesting properties. One famous due to Minkowski : if $P \in \mathbb{Z}[X]$ is irreducible and $\operatorname{disc} P = \pm 1$ implies $\deg P = 1$. Interesting for a number theorist, as this is a quite complicated diophantine equation in general. For an algebraic geometer, it says that $\operatorname{Spec} \mathbb{Z}$ is simply connected !

Hermite-Minkowski Theorem : if we have a collection of irreducible polynomials $P \in \mathbb{Z}[X]$ with $\operatorname{disc} P$ bounded, then their roots generate a finite extension of $\mathbb{Q}$ in $\mathbb{C}$.

A key ingredient is a lattice theoretic interpretation. Fix $P \in \mathbb{Z}[X]$ monic irreducible of degree n, choose $\alpha \in \mathbb{C}$ a root of P and consider $A = \mathbb{Z}[\alpha]$. This is a subring of $\mathbb{C}$ isomorphic to $\mathbb{Z}[X]/(P)$, hence to $\mathbb{Z}^n$ as an abelian group. It naturally acts on itself by multiplication, hence we get a trace linear form $\mathrm{Tr} : A \to \mathbb{Z}$. The resultant interpretation shows that disc$P$ is the determinant of the symmetric bilinear form $(x, y) \mapsto \mathrm{Tr}(xy)$. It is not necessarily pos. def. but general theory, of which Hermite is a well-known contributor, applies. This led him to prove the theorem when degree of P is bounded in his 1857 Crelle's paper (using actually rather the determinant $A \to \mathbb{Z}$, or "Norm").

Minkowski's contribution is to have shown that $\mathrm{disc}\, P$ bounded implies deg P bounded. This is a beautiful application of his geometry of numbers, still viewing A as a lattice in the real vector space $A \otimes \mathbb{R}$. Using clever convex subsets he showed the lower bound :

$$|\mathrm{disc}\, P|^{\frac{1}{2n}} \geq \frac{\sqrt{\pi}}{2} \frac{n}{(n!)^{1/n}}$$

The RHS increases to $\frac{e\sqrt{\pi}}{2} \approx 2.41$ when n grows, and is approximately $1.25 > 1$ for $n = 2$. This shows that $|\mathrm{disc}\, P|$ grows exponentially with n, as well as $|\mathrm{disc}\, P| > 1$ for $n > 1$. □

All of this applies to arbitrary "number rings" A, i.e. subrings of $\mathbb{C}$ generated by finitely many algebraic integers (such an A is free of finite rank as an abelian groups). In particular, if K is a number field it applies to its ring of integers $\mathcal{O}_K$ (not necessarily of the form $\mathbb{Z}[\alpha]$). Number theorists define $\mathrm{disc}\, K$ as the discriminant of the trace bilinear form on $\mathcal{O}_K$. Get same inequalities with (deg $P, \mathrm{disc}\, P$) replaced by $([K : \mathbb{Q}], \mathrm{disc}\, K)$, and :

Classical HM theorem : that here are only finitely many number fields with given discriminant.

Not quite the end of the story, as Minkowski's lower bound has then been much improved by Odlyzko (using ideas of Stark and Serre). These improvements have been very useful for the concrete question of classifying number fields with given degree and bounded discriminant. Odlyzko's method very different : it relies on the analytic property of the Dedekind zeta function of K. It is a Dirichlet series defined for $\mathrm{Re}\, s > 1$ by the absolutely convergent Euler product:

$$\zeta_K(s) = \prod_P (1 - |\mathcal{O}_K/P|^{-s})^{-1}$$

when P varies over all maximal ideals of $\mathcal{O}_K$ (e.g. we have $\zeta_{\mathbb{Q}} = \zeta$). This function "contains" the rule giving the decomposition of the rational primes in $\mathcal{O}_K$. Set $\xi_K(s) = \zeta_K(s)\ \{\pi^{-s/2}\Gamma(s/2)\}^{r_1}\ \{(2\pi)^{-s}\Gamma(s)\}^{r_2}$. Hecke showed that ξ_K has a meromorphic continuation to $\mathbb{C}$, with $s = 0, 1$ as unique (simple) poles, as well as the functional equation

$$\xi_K(s) \ = \ |\mathrm{disc}\, K|^{1/2-s}\, \xi_K(1-s).$$

A key idea is to apply the explicit formula “à la Weil” to this function (and suitable test functions). This leads miraculously, but rather easily, to better bounds than that of Minkowski.

2 Galois representations

In order to introduce them, consider again $P \in \mathbb{Z}[X]$ monic irreducible of degree n. For a prime p not dividing $\mathrm{disc}\, P$, we may write

$$P \bmod p = P_1 P_2 ... P_g$$

with the P_i irreducible $\neq$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. A very important open problem in algebraic number theory is : can we characterize the p (not dividing $\mathrm{disc}\, P$) such that the associated list $\{\deg\, P_1, \deg P_2,\ ...,\ \deg P_g\}$ is given ? (e.g. is irreducible, or is totally split...).

Example: $P = X^2 - d$, then $\mathrm{disc}\, P \ = \ 4d$, the question is : when d is a square mod p ? Well-known answer given by quadratic reciprocity law : it only depends on p mod $4d$ (the discriminant!). Very much open in general, although Langlands has a candidate for a reciprocity law in terms of automorphic forms of GL_n of level $\mathrm{disc}\, P$.

Frobenius found a Galois theoretic reformulation of the question. Let K be the splitting field of P (a Galois number field). We have a natural morphisms $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{S}_n$ induced by permutations of the roots of P. For any p not dividing $\mathrm{disc}\, P$, and following Frobenius, there is a natural conjugacy class $\mathrm{Frob}_p \subset \mathrm{Gal}(K/\mathbb{Q})$ whose cycle decomposition is the list of $\deg P_i$. Everything reduces to the problem of studying the map $p \mapsto \mathrm{Frob}_p$.

Inspired by Dirichlet's work on arithmetic progression, Artin takes a Fourier analysis approach on the finite group $\mathrm{Gal}(K/\mathbb{Q})$. For any representation $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$, he defines

$$\mathrm{L}(s,\rho) \;=\; \prod_{p \nmid \mathrm{disc} P} \det(1-\rho(\mathrm{Frob}_p)p^{-s})^{-1} \times (\text{explicit factor for each other places}).$$

When ρ is the permutation representation on $\mathbb{C}[\mathrm{Roots}(P)]$, we actually have $\mathrm{L}(s,\rho) = \zeta_K$, but the philosophy needs all of them. Artin defines also the *conductor of* ρ, an integer denoted by $\mathrm{N}(\rho)$, and the conjectures the meromorphic continuation and the functionnal equation

$$\mathrm{L}(s,\rho) \;=\; \epsilon\, \mathrm{N}(\rho)^{1/2-s}\, \mathrm{L}(1-s,\rho^\vee),$$

and that $\mathrm{L}(s,\rho)$ is entire if ρ does not contain the trivial rep. Those conjectures have been proved by Hecke and others, except this last assertion ("Artin conjecture"). Nevertheless, the study of $\mathrm{L}(1,\rho)$ still leads to the proof of the so-called Cebotarev's theorem. Note that the conductor is to ρ what $\mathrm{disc}\, K$ is to K.

Variant of Hermite-Minkowski : given $N, n \geq 1$, there are only finitely many iso. classes of irred. rep. $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ with $N(\rho) = N$. This actually follows from Hermite's result, Jordan theorem + some class field theory (Anderson, Blasius, Coleman, Zettler). Assuming the Artin conjecture, Odlyzko shows that it is not even necessary to fix n ! This is the right generalization of Minkowki's contribution. Proof still uses now explicit formula for $\mathrm{L}(s,\rho)$.

This is a very nice way of thinking about HM, but there are many other interesting Galois representations which are not Artin. They occur as follows. Let $X \subset \mathbb{P}^n$ be a projective smooth variety defined over $\mathbb{Q}$. For any $i \geq 0$, and any prime ℓ, consider the Betti cohomology group

$$\mathrm{H}^i(\mathrm{X}(\mathbb{C}), \mathbb{Z}) \otimes \overline{\mathbb{Q}_\ell}.$$

Grothendieck defined a continuous linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on this finite dim. $\overline{\mathbb{Q}_\ell}$-vector space. The philosophy is that this representation knows a lot about X (Grothendieck, Tate, Deligne...). For instance it knows $\sharp X(\mathbb{Z}/p\mathbb{Z})$ for all p of good reduction of X : for any such

p, Grothendieck has shown that the Frobenius elements at p in the Galois group acts in a well-defined way, and the alternate sum of their trace is $\sharp X(\mathbb{Z}/p\mathbb{Z})$.

An ℓ-adic representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}_\ell})$ is said *geometric* it it occurs as a subquotient of such a rep., for some i and X. The integer i may be deduced from ρ by Deligne's purity theorem (modulus on Frobenius eigenvalues), it is called the weight of ρ. When $i = 0$ we get all Artin representations (with different coeff. fields, but it does not matter). For $i > 0$, get rep. with infinite image, never Artin. In all cases, we still have a definition of $\mathrm{L}(s, \rho)$ and $\mathrm{N}(\rho)$ "à la Artin".

Folklore Conjecture: There are only finitely many isomorphism classes of ℓ-adic geometric irreducible ρ of given dimension, conductor and weight.

The reason I know to believe in this conjecture is the following :

Theorem: (Harish-Chandra) The folklore conjecture is true if we restrict to the automorphic ρ.

The geometric representation ρ is said automorphic if we have $\mathrm{L}(s, \rho) = \mathrm{L}(s, \pi)$ with π automorphic representation of GL_n over $\mathbb{Q}$ with $n = \dim \rho$. The generalized modularity conjecture (or general Langlands reciprocity conjecture) asserts that all geometric ρ are modular, hence imply the folklore conjecture. What Harish-Chandra really proves, in quite bigger generality, is that "spaces of modular forms of fixed weight and level are finite dimensional".

I can now state my recent contribution to this subject, in Minkowski-Odlyzko's style.

Theorem: (Ch.) Fix $N \geq 1$. There are finitely many automorphic irreducible, geometric, ℓ-adic ρ with conductor N and weight ≤ 23.

To prove this theorem I study the explicit formula for the Rankin-Selberg L-function $\mathrm{L}(s, \rho \otimes \rho^\vee)$ in the spirit of Odlyzko's method. I won't explain more than this here ! At some point the following fact plays a role : the matrix $(\log \pi \; - \; \psi(\frac{1+|i-j|}{2}) \,)_{0 \leq i,j \leq w}$ is positive definite iff $w \leq 23$ (and of signature $(w, 1)$ otherwise). Under GRH, a different matrix shows up and I can replace 23 by 24. I don't know if it holds for higher w. THE END