

# Discriminants and finiteness theorems in number theory

Yuichiro Taguchi

In number theory, discriminants often appear at key points in proving theorems which assert the finiteness in number (or even non-existence) of certain kinds of arithmetic objects. A typical argument is to show two estimates for the discriminant of opposite directions which eventually contradict; one from above which is often done algebraically, and the other which is done by some other methods, say, analytically. As this seems rather prevalent, I try in this paper to explain some of these phenomena, including classical theorems such as Minkowski's as well as my recent results obtained jointly with H. Moon.

Mostly in this paper,  $K$  will denote an algebraic number field of finite degree  $n$  over the rational number field  $\mathbb{Q}$ .

**1. Discriminants and finiteness theorems.** In this section, we follow [22] to review the definition of the discriminant together with some classical theorems concerning it.

Let  $K$  be an algebraic number field of degree  $n$ . Then its ring of integers  $\mathcal{O}_K$  is a free  $\mathbb{Z}$ -module of rank  $n$ . Let  $(\omega_1, \dots, \omega_n)$  be a free  $\mathbb{Z}$ -basis of  $\mathcal{O}_K$ . Then the *discriminant*  $d_K$  of  $K$  is defined to be

$$d_K = \det \left( \omega_j^{(i)} \right)^2,$$

where  $\omega_j^{(i)}$  ( $1 \leq i \leq n$ ) are the conjugates over  $\mathbb{Q}$  of  $\omega_j$ . Then a celebrated theorem of Dedekind says that a prime  $p$  divides  $d_K$  if and only if the extension  $K/\mathbb{Q}$  (or, the covering  $\text{Spec } \mathcal{O}_K \rightarrow \text{Spec } \mathbb{Z}$ ) *ramifies* at  $p$ . The *raison d'être* of the discriminant would primarily be in this property.

Note that the discriminant is defined also in a relative case, i.e., for a finite extension of global fields. Also, there is a closely related notion *different*.

Following are some classical theorems of which we are interested in the type:

**Theorem 1** (Minkowski). *There exist no algebraic number field  $K$  such that  $|d_K| = 1$  except  $K = \mathbb{Q}$ .*

This is a direct consequence of Theorem 4 below. With some more efforts, one obtains:

**Theorem 2** (Hermite-Minkowski). *For any constant  $C > 0$ , there exist only finitely many algebraic number fields  $K$  such that  $|d_K| \leq C$ .*

A version of this is:

**Theorem 3.** *For any finite set  $S$  of prime numbers and any integer  $n \geq 1$ , there exist only finitely many algebraic number fields  $K$  of degree  $\leq n$  which are unramified outside  $S$ .*

Theorem 2 has a function field analogue (i.e. with a suitable formulation, it holds also for algebraic function fields in one variable over a finite field). Theorem 3, however, does not hold for function fields because the Artin-Schreier equations produce infinitely many extensions of degree  $p = \text{char } K$  which ramify only in  $S$ .

Traditionally, these theorems are proved by using “Geometry of Numbers”. In fact, by this method, one can prove:

**Theorem 4** (Minkowski bound). *One has*

$$|d_K| \geq \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2.$$

Here and elsewhere,  $r_1$  and  $r_2$  are, as usual, the number of real and complex places of  $K$ .

This bound has long been the best known estimate of this kind. In the mid 70’s, Stark invented a new analytic method ([21]), which was pursued further by Odlyzko [11], Serre [17], Poitou [12],  $\dots$ , and lead to:

**Theorem 5** (Odlyzko bound; cf. [17]). *Under the Generalized Riemann Hypothesis, one has*

$$|d_K| \geq (8\pi e^{\gamma+\pi/2})^{r_1} (8\pi e^{\gamma})^{2r_2} + o(1)$$

as  $[K : \mathbb{Q}] \rightarrow \infty$ .

Here,  $\gamma = 0.577\dots$  is the Euler constant.

There are more explicit versions, as well as unconditional ones (though weaker than the above). See [12]. The proof depends on Weil’s explicit formula [24], which is an equality of (i) a certain sum over zeroes of the Dedekind zeta function  $\zeta_K(s)$  of  $K$ , plus a certain sum over prime ideals of  $K$ ; and (ii) an integral involving the gamma factor of  $\zeta_K(s)$ , which contains the term  $|d_K|^{s/2}$ .

**2. Conductors and finiteness theorems.** Conductors are closely related to discriminants. Generally speaking, conductors are defined by Galois theoretic or class-field theoretic means, while discriminants are defined more directly from, say, the defining equations of the objects.

In this section, we discuss conductors in various contexts and related finiteness theorems.

(1) *Abelian extensions.* The conductor of an abelian extension of a global field is defined to be the product of those of local extensions for all places. To define the local conductor, let  $K$  be a (non-archimedean) local field. Then local class field theory asserts that there exists a unique homomorphism  $\rho_K : K^\times \rightarrow G_K^{\text{ab}} = \text{Gal}(K^{\text{ab}}/K)$  (where  $K^{\text{ab}}$  denotes the maximal abelian extension of  $K$ ) which induces an isomorphism  $\rho_{L/K} : K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} \text{Gal}(L/K)$  for each finite abelian extension  $L/K$ . If  $\mathfrak{p}$  denotes the maximal ideal of the integer ring  $\mathcal{O}_K$  of  $K$ , the *conductor* of  $L/K$  is defined to be the largest ideal  $\mathfrak{p}^f$  (i.e. with the smallest  $f$ ) such that the composite map  $K^\times \xrightarrow{\rho_K} G_K^{\text{ab}} \rightarrow \text{Gal}(L/K)$  factors through  $K^\times / (1 + \mathfrak{p}^f)$ .

For example, the conductor of the  $n$ -th cyclotomic extension  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  is  $n$  if  $2 \nmid n$  or  $4 \mid n$ .

The following theorem, which is a corollary of global class field theory, is a first example of our finiteness theorems related to the conductor.

**Theorem 6.** *Let  $K$  be an algebraic number field. Let  $\mathfrak{m}$  be a positive divisor of  $K$ . Then there exist only finitely many finite abelian extensions of  $K$  whose conductor divides  $\mathfrak{m}$ .*

Or, what amounts to the same thing, there exists a maximal abelian extension of  $K$  with conductor dividing  $\mathfrak{m}$ , which is finite over  $K$ .

In the function field case, the same holds if one restricts to geometric extensions, i.e., extensions with no constant field extensions.

(2) *Galois representations.* For any field  $K$ , we denote by  $G_K$  its absolute Galois group  $\text{Gal}(\overline{K}/K)$ . Given a continuous Galois representation  $\rho : G_K \rightarrow \text{GL}_k(V)$  of a global field  $K$  (where  $V$  is a finite-dimensional vector space over a field  $k$  with discrete topology), its Artin conductor is defined, which is again a product of local ones. To define the local conductor, let  $K$  be a local field,  $\rho : G_K \rightarrow \text{GL}_k(V)$  a continuous representation (hence with finite image), and  $L/K$  a finite Galois extension such that  $\rho$  factors through  $G = \text{Gal}(L/K)$ . Then one has the *Artin representation*  $a_G$  of  $G$  (cf. [15], Chap. VI). Let  $f(\rho)$  be the inner product  $\langle a_G, \rho \rangle_G$  of  $a_G$  and  $\rho$ , which is equal to  $\dim_k \text{Hom}_G(a_G, \rho)$  if  $V$  is projective as a  $k[G]$ -module. If the characteristic  $\ell$  of the field  $k$  does not divide the order of  $G$ , it coincides with the expression  $n(\rho) := \sum_{i \geq 0} \dim(V/V^{G_i}) / (G_0 : G_i)$ , where  $G_i$  is the  $i$ th ramification subgroup of  $G$ . The *Artin conductor* of  $\rho$  is by definition  $\mathfrak{f}(\rho) = \mathfrak{p}^{f(\rho)}$

(or  $N(\rho) = \mathfrak{p}^{n(\rho)}$  according to the purpose), where  $\mathfrak{p}$  is the maximal ideal of the integer ring  $\mathcal{O}_K$  of  $K$ .

The conductor is related to the discriminant by the Führerdiskriminantenproduktformel:

**Theorem 7** (Artin). *Let  $L/K$  be a finite Galois extension of global or local fields, and let  $G$  be its Galois group. Then one has*

$$d_{L/K} = \prod_{\chi \in \text{Irr}(G)} f(\chi)^{\dim \chi}.$$

Here the product is over the irreducible representations  $\chi$  of  $G$ .

This has been generalized by T. Saito [14] to the case of a relative curve over a discrete valuation ring.

(3) *Abelian varieties.* The conductor of an Abelian variety over a global field is also defined locally. Let  $A$  be an Abelian variety over a local field  $K$ . Let  $N(A)$  denote the Artin conductor of the group  ${}_{\ell}A(\overline{K})$  of  $\ell$ -torsion points of  $A$ , viewed as a Galois representation of  $K$ . This does not depend on the choice of a prime  $\ell$  different from the residue characteristic of  $K$ . It measures in some sense the badness of the reduction of  $A$ :

**Theorem 8** (Serre-Tate [19]). *The maximal ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$  divides  $N(A)$  if and only if  $A$  has bad reduction at  $\mathfrak{p}$ .*

Concerning the finiteness, Shafarevich conjectured the following ([20]):

**Theorem 9** (Faltings [4]). *Let  $K$  be an algebraic number field, and  $S$  a finite set of finite places of  $K$ . Let  $g$  be an integer  $\geq 1$ . Then there exist only finitely many isomorphism classes of principally polarized Abelian varieties over  $K$  of dimension  $g$  which have good reduction outside  $S$ .*

**Theorem 10** (Fontaine, Abrashkin [5], [1]). *There exists no Abelian variety over  $\mathbb{Q}$  which has everywhere good reduction.*

In Faltings' theorem, the origin of the finiteness is in the finiteness of heights on the moduli space. The proof of the theorem of Fontaine and Abrashkin, very roughly speaking, consists in the two contradicting estimates of the discriminant of the field of  $p$ -torsion points of the Abelian variety over  $\mathbb{Q}$ , one from above (shown algebraically), and the other from below (= the Odlyzko bound, which is analytic in nature). The estimate from above goes as follows:

**Theorem 11** (Fontaine [5]). *Let  $K$  be a complete discrete valuation field of characteristic zero with perfect residue field of characteristic  $p$ .*

Let  $J$  be a finite flat group scheme over  $\mathcal{O}_K$  which is killed by  $p^n$ , and let  $L/K$  be the smallest Galois extension such that  $G_L$  acts trivially on the geometric points  $J(\overline{K})$  of  $J$ . Then one has

$$v_p(d_{L/K}) < [L : K] \left( n + \frac{1}{p-1} \right).$$

**Theorem 12** (Abrashkin [2]). *Let  $K$  be as in the previous theorem. Assume further that  $p$  is a uniformizer of  $K$ . Let  $X$  be a proper smooth variety over  $K$  with good reduction. Let  $H$  be a subquotient of  $H_{\text{ét}}^i(X \otimes_K \overline{K}, \mathbb{Q}_p)$  which is killed by  $p^n$ , and let  $L/K$  be the smallest Galois extension such that  $G_L$  acts trivially on  $H$ . If  $i < p$ , then one has*

$$v_p(d_{L/K}) < [L : K] \left( n + \frac{i}{p-1} \right).$$

On the conductor of an Abelian variety, we may add the following:

**Theorem 13** (Mestre [8]). *Let  $A$  be an Abelian variety over  $\mathbb{Q}$ . If we assume some standard conjectures on the  $L$ -function of  $A/\mathbb{Q}$ , then we have:*

$$N(A) > 10^{\dim A}.$$

(In particular, it follows that there does not exist an Abelian variety over  $\mathbb{Q}$  with everywhere good reduction.)

Note that this is in accordance with the fact that  $N = 11$  is the least  $N$  such that the modular curve  $X_0(N)$  has genus  $\geq 1$ , hence the estimate is the best possible.

The proof of the above theorem depends on Weil's explicit formula for the  $L$ -function, hence is in the same spirit as the Odlyzko bound.

Shafarevich's conjecture may be considered for other kinds of varieties. At present, only a few cases are known ([1], [6]).

Such conjectures are generalized in terms of  $p$ -adic Galois representations, and formulated by Fontaine and Mazur ([7]). Here, let us cite only one of their conjectures, which asserts the finiteness of certain Galois representations:

**Conjecture 14** (Fontaine-Mazur). *Let  $K$  be an algebraic number field. Then there would exist only finitely many isomorphism classes of continuous semi-simple  $p$ -adic representations  $\rho : G_K \rightarrow \text{GL}_d(\overline{\mathbb{Q}}_p)$  of dimension  $d$  which are geometric, of bounded inertial level, and of a given Hodge-Tate type.*

The condition "geometric", which is defined algebraically via the theory of Fontaine, is conjectured to be equivalent to that the representation comes from algebraic geometry, i.e., realized as an étale cohomology

group of an algebraic variety over  $K$  (this is in fact the main part of the Fontaine-Mazur conjectures). The inertial level, of which we omit explanation here, is something like the conductor. The Hodge-Tate type is, so to speak, the “geometric shape” of the representation.

(4) *Modular forms.* Let  $S_k(\Gamma_0(N), \mathbb{C})$  be the space of cusp forms of weight  $k$  with respect to the congruence subgroup  $\Gamma_0(N)$ . Then it is of *finite* dimension (being the space of the global sections of a coherent sheaf on the proper curve  $X_0(N)$ ). The integer  $N$ , called the *level*, is related to the ramification of a Galois representation by the following theorem due to Shimura ( $k = 2$ ) and Deligne ( $k \geq 2$ ): To any Hecke eigenform  $f \in S_k(\Gamma_0(N), \mathbb{C})$ , there is associated a continuous irreducible representation

$$\rho_f : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(K_{\mathfrak{p}})$$

(where  $K_{\mathfrak{p}}$  is a  $p$ -adic field) which is unramified outside  $Np$  and such that  $\mathrm{Trace} \rho_f(\mathrm{Frob}_{\ell}) = a_{\ell}$ , the  $\ell$ th Fourier coefficient of  $f$ , for all prime numbers  $\ell$  not dividing  $Np$ .

(5) *Fermat’s Last Theorem.* Let us mention that the strategy of the proof of Fermat’s Last Theorem, as suggested by G. Frey and explained in §4.2 of [18], is also, in some sense, concerned with the estimate of the ramification of Galois representations. Wiles showed ([25]) that every semi-stable elliptic curve  $E$  over  $\mathbb{Q}$  is modular. If  $E$  is a so-called Frey curve, which is constructed from an assumed integral solution  $(a, b, c)$  to the equation  $X^p + Y^p = Z^p$ , then the Galois representation on its  $p$ -torsion points is “too good” in terms of ramification (in other words, its ramification is bounded from above too keenly). Then Wiles’ theorem, together with the part of the  $\varepsilon$ -conjecture proved by Ribet ([13]),  $E$  must be modular of weight 2 and level 2, which does not exist (if  $f \in S_2(\Gamma_0(N), \mathbb{C})$  is non-trivial, then  $N \geq 11$ ); contradiction.

(6) *Mod  $p$  Galois representations.* Let us begin with the following conjecture of Serre. Let  $\overline{\mathbb{F}}_p$  be an algebraic closure of the prime field of  $p$  elements. Consider a two-dimensional continuous  $\overline{\mathbb{F}}_p$ -linear representation  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$  of the Galois group  $G_{\mathbb{Q}}$  of  $\mathbb{Q}$ .

**Conjecture 15** (Serre [16], [18]). *If  $\rho$  is odd and irreducible, then  $\rho$  would be modular, i.e., would come from a modular eigenform  $f$ . Moreover, the level  $N$  and weight  $k$  of  $f$  can be precisely predicted.*

Precisely speaking,  $f$  is conjectured to be chosen so that its level  $N$  is equal to  $N(\rho)$ , the “Artin conductor outside  $p$ ” of  $\rho$ , and the weight  $k$  is bounded by  $p^2 - 1$  (or 4 if  $p = 2$ ) (in fact, the weight is predicted more precisely).

Since there are only finitely many eigenforms of a given weight and level, we have

**Corollary 16** (to the Conjecture). *Let  $N$  be a positive integer. Then there exist only finitely many isomorphism classes of odd and irreducible continuous representations  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$  with  $N(\rho)|N$ .*

In [9], Moon proposes a problem generalizing this to the case of arbitrary continuous semi-simple Galois representations  $\rho : G_K \rightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$  of an algebraic number field  $K$ .

Some results relating the above are:

**Theorem 17** (Tate [23]). *If  $p = 2$  and  $N(\rho) = 1$ , then the Conjecture is true.*

Serre noted (in his Œuvres Vol. III, p. 710) that the same method yielded the case of  $p = 3$  and  $N(\rho) = 1$ .

**Theorem 18** (Brueggeman [3]). *If  $p = 5$  and  $N(\rho) = 1$ , then the Conjecture is true.*

On the finiteness, we have

**Theorem 19** (Moon [9]). *Assume that the Generalized Riemann Hypothesis is true. Then there exist only finitely many isomorphism classes of semi-simple representations  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_4(\overline{\mathbb{F}}_2)$  which are unramified outside 2.*

She has some more results for a few other values of the characteristic  $p$  and the degree  $d$ .

In proving these theorems, the basic strategy is to estimate the discriminant of the field  $K/\mathbb{Q}$  corresponding to the kernel of  $\rho$ ; one from above algebraically (using class field theory, etc.), and the other from below, this being the Odlyzko bound, hence is analytic in nature.

For arbitrary  $p$  and  $d$ , we have:

**Theorem 20** ([10]). *Let  $K$  be an algebraic number field, and let  $N$  be a non-zero ideal of  $K$ . Then there exist only finitely many isomorphism classes of semi-simple representations  $\rho : G_K \rightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$  with  $N(\rho)|N$  and solvable image.*

For representations with values in  $\mathrm{GL}_d(\mathbb{C})$ , a similar statement holds *without* the assumption of solvability.

Let us conclude with a sketch of the proof of the theorem. By a theorem in group theory, the image of  $\rho$  contains a normal subgroup of bounded index which is conjugate to a subgroup of the upper triangular matrices. For the quotient, we apply the Hermite-Minkowski theorem.

For the upper triangular part, we apply successively the conductor estimate given in [9] and reduce to Theorem 6, the finiteness of the abelian extensions of a given conductor.

#### REFERENCES

- [1] V. Abrashkin, *Modular representations of the Galois group of a local field and the generalization of the Shafarevich conjecture*, Math. USSR Izv. **53**(1989), 1138-1186
- [2] V. Abrashkin, *Ramification in étale cohomology*, Invent. math. **101**(1990), 631-640
- [3] S. Brueggeman, *The nonexistence of certain Galois extensions unramified outside 5*, J. Number Theory **75**(1999), 47-52
- [4] G. Faltings, *Entlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. math. **73**(1983), 349-366
- [5] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur  $\mathbb{Z}$* , Invent. math. **81**(1985), 515-538
- [6] J.-M. Fontaine, *Schémas propres et lisses sur  $\mathbb{Z}$* , in: Proc. Indo-French Conf. on Geometry, Hindustan Book Agency, New Dehli, 1993, pp. 43-56
- [7] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in: Proc. Conf. on elliptic curves and modular forms, Hong Kong, 1993, International Press, 1995, pp. 41-78
- [8] J.-F. Mestre, *Formules explicites et minoration de conducteurs de variétés algébriques*, Compositio Math. **58**(1986), 209-232
- [9] H. Moon, *Finiteness results on certain mod  $p$  Galois representations*, to appear in J. Number Theory
- [10] H. Moon and Y. Taguchi, *Mod  $p$  Galois representations of solvable image*, to appear in Proc. A.M.S.
- [11] A.M. Odlyzko, *Lower bounds for discriminants of number fields*, Acta Arith. **29**(1976), 275-297
- [12] G. Poitou, (d'après A.M. Odlyzko) *Minorations de discriminants*, Sémin. Bourbaki, 1975/76 Exp. 479, Springer Lecture Notes in Math., Vol. 567(1977), pp. 136-153
- [13] K. Ribet, *On modular representations of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  arising from modular forms*, Invent. math. **100**(1990), 431-476
- [14] T. Saito *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J. **57**(1988), 151-173
- [15] J.-P. Serre, "Corps Locaux", Hermann, Paris, 1968
- [16] J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo  $\ell$* , Journées arith. Bordeaux, Astérisque **24-25**(1975), 109-117
- [17] J.-P. Serre, *Minorations de discriminants*, Œuvres, Vol. III, Springer-Verlag, 1986, pp. 240-243
- [18] J.-P. Serre, *Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54**(1987), 179-230
- [19] J.-P. Serre and J. Tate, *Good reduction of Abelian varieties*, Ann. Math. **88**(1968), 492-517
- [20] I. Shafarevich, *Algebraic number fields*, Proc. I.C.M., Stockholm 1962; Also in: "Collected Mathematical Papers", Springer-Verlag, 1989, pp. 283-294

- [21] H.M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. math. **23**(1974), 135-152
- [22] T. Takagi, “Algebraic Number Theory”, 2nd ed. (in Japanese), Iwanami Shoten, Tokyo, 1971
- [23] J. Tate, *The non-existence of certain Galois extensions of  $\mathbb{Q}$  unramified outside 2*, Contemp. Math. **174**(1994), 153-156
- [24] A. Weil, *Sur les “formules explicites” de la théorie des nombres premiers*, Comm. Sem. Math. Univ. Lund, Tomes supplémentaire (1952), 252-265; Also in: “Œuvres Scientifiques”, Springer-Verlag, 1979, Vol. II, pp. 48-61
- [25] A. Wiles, *Modular elliptic curves and Fermat’s Last Theorem*, Ann. Math. **141**(1995), 443-551

Department of Mathematics  
Hokkaido University  
Sapporo, 060-0810, Japan