Discriminant Bounds

Matt Tyler

Let K be an algebraic number field of degree $n = n_K$ over $\mathbb{Q}$ with r_1 real embeddings and r_2 conjugate pairs of complex embeddings. Let $D = D_K$ be the absolute value of the discriminant of K. The Dedekind zeta function of K is

$$\zeta_K(s) = \sum_{\mathfrak{a}} N\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}}, \tag{0.1}$$

and the generalized Riemann hypothesis (GRH) for K is the conjecture that every zero of $\zeta_K(s)$ inside the critical strip $0 < \operatorname{Re} s < 1$ is on the critical line $\operatorname{Re} s = \frac{1}{2}$. We write γ for the Euler-Mascheroni constant $\lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n\right) \approx 0.57721$.

The purpose of these notes is to bound D in terms of r_1 and r_2. The first such bound was found by Minkowski. Using the geometry of numbers, Minkowski showed that every ideal class of K contains an integral ideal of norm at most $\sqrt{D}\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}$. Since every ideal has norm at least 1, it follows that

$$D \geq \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2. \tag{0.2}$$

(In particular, $D > 1$ for $n > 1$, so there are no unramified extensions of $\mathbb{Q}$.) By Stirling's approximation $n! = \left(\frac{n}{e}\right)^n e^{-o(n)}$ and the relation $n = r_1 + 2r_2$, we find

$$D \geq A^{r_1} B^{2r_2} e^{o(n)} \quad \text{with } A = e^2 \text{ and } B = e^2\frac{\pi}{4}, \tag{0.3}$$

and it is bounds of this type that we will begin by considering.

Since Minkowski, much progress has been made in improving the constants A and B. Initially, most of the papers used geometry of numbers methods, culminating in the work of Rogers and Mulholland for totally real and totally complex fields, respectively. In the 1970's Stark introduced analytic methods, which were extended by Odlyzko to eventually give substantial improvements on previous lower bounds. Using the Guinand–Weil explicit formulas, Serre provided a general approach for proving such bounds, which led to improvements still, and provided insight for determining the best possible bounds that can be proved in this way. See Table 1 and the survey paper [9] for details.

Result	A	B
Minkowski (1891) [4]	$e^2 \approx 7.39$	$e^{2\frac{\pi}{4}} \approx 5.80$
Rogers-Mulholland (1960) [5, 10]	32.56	15.77
Stark (1974) [12]	$4\pi e^\gamma \approx 22.38$	$2\pi e^\gamma \approx 11.19$
Odlyzko (1975) [6]	50.66	19.96
with GRH	94.69	28.76
Odlyzko (1976) [7]	55	21
with GRH	136	34.5
Odlyzko (1977) [8]	60	22
with GRH	188	41
Serre (1975) [11]	$4\pi e^{1+\gamma} \approx 60.84$	$4\pi e^\gamma \approx 22.38$
with GRH	$8\pi e^{\pi/2+\gamma} \approx 215.33$	$8\pi e^\gamma \approx 44.76$

Table 1: Constants A and B for which $D \geq A^{r_1} B^{2r_2} e^{o(n)}$

In this paper, we will introduce Stark's analytic method and give an overview of Serre's approach to proving lower bounds. We will also show how to use methods in group cohomology to exhibit fields with small discriminants, and therefore give upper bounds as well.

1 Stark's analytic method

Stark's use of analytic techniques in the study of discriminant lower bounds began with the following explicit formula.

Proposition 1.1. *We have*

$$\log D = r_1 \left(\log \pi - \frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) \right) + 2r_2 \left(\log 2\pi - \frac{\Gamma'}{\Gamma}(s) \right) - \frac{2}{s} - \frac{2}{s-1} + 2{\sum_{\rho}}' \frac{1}{s-\rho} - 2\frac{\zeta_K'}{\zeta_K}(s),$$

where ρ runs over the zeroes of $\zeta_K(s)$ in the critical strip, and $\sum_\rho'$ indicates that the terms ρ and $\overline{\rho}$ are to be taken together.

Proof. Consider the completed zeta function

$$\Lambda_K(s) = s(s-1) D^{s/2} 2^{-r_2 s} \pi^{-ns/2} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \zeta_K(s), \tag{1.1}$$

which is an entire function of order 1 and satisfies the functional equation $\Lambda_K(1-s) =$

$\Lambda_K(s)$. By the Hadamard factorization theorem, we may write

$$\Lambda_K(s) = e^{\alpha+\beta s} \prod_\rho \left(1 - \frac{s}{\rho}\right) e^{s/\rho} \tag{1.2}$$

for some $\alpha, \beta \in \mathbb{C}$, where the product is over the non-trivial zeroes ρ of $\zeta_K(s)$. Taking the logarithmic derivative, we find

$$\frac{\Lambda_K'}{\Lambda_K}(s) = \beta + \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right), \tag{1.3}$$

with the sum converging absolutely. By the functional equation $\frac{\Lambda_K'}{\Lambda_K}(s) = -\frac{\Lambda_K'}{\Lambda_K}(1-s)$, we have

$$\beta + \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) = -\beta - \sum_\rho \left(\frac{1}{1-s-\rho} + \frac{1}{\rho}\right), \tag{1.4}$$

and since $1-\rho$ is a zero whenever ρ is, we obtain $\beta = -\sum_\rho{}' \frac{1}{\rho}$. Altogether, we find

$$\frac{\Lambda_K'}{\Lambda_K}(s) = \sum_\rho{}' \frac{1}{s-\rho}. \tag{1.5}$$

On the other hand, by the definition of $\Lambda_K(s)$, we have

$$\frac{\Lambda_K'}{\Lambda_K}(s) = \frac{1}{s} + \frac{1}{s-1} + \frac{1}{2}\log D - r_2 \log 2 - \frac{n}{2}\log\pi + \frac{r_1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) + r_2\frac{\Gamma'}{\Gamma}(s) + \frac{\zeta_K'}{\zeta_K}(s). \tag{1.6}$$

Combining (1.5) and (1.6) completes the proof. □

Stark's observation was that terms in this explicit formula which are difficult to estimate, namely $\sum_\rho{}' \frac{1}{s-\rho}$ and $\frac{\zeta_K'}{\zeta_K}(s)$, can actually be ignored. Indeed, for $s = \sigma > 1$, we have

$$\begin{aligned} -\frac{\zeta_K'}{\zeta_K}(\sigma) &= \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m\sigma}} > 0 \qquad \text{and} \\ \sum_\rho{}' \frac{1}{\sigma-\rho} &= \sum_\rho \frac{1}{2}\left(\frac{1}{\sigma-\rho} + \frac{1}{\sigma-\overline{\rho}}\right) = \sum_\rho \frac{\sigma - \operatorname{Re}\rho}{|\sigma-\rho|^2} > 0. \end{aligned} \tag{1.7}$$

Therefore, we find

$$\log D \geq r_1\left(\log\pi - \frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right)\right) + 2r_2\left(\log 2\pi - \frac{\Gamma'}{\Gamma}(s)\right) - \frac{2}{s} - \frac{2}{s-1}. \tag{1.8}$$

Letting $s = 1 + n^{-1/2}$, so that $\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) = -\gamma - \log 4 + o(1)$ and $\frac{\Gamma'}{\Gamma}(s) = -\gamma + o(1)$, we obtain the following bound.

Corollary 1.2 (Stark). $D \geq (4\pi e^{\gamma})^{r_1}(2\pi e^{\gamma})^{2r_2}e^{o(n)}$.

In a series of papers [6, 7, 8], Odlyzko improved on this bound using subtler estimates drawn from the explicit formula in Proposition 1.1 and its derivatives (see Table 1).

2 Serre's reformulation

In this section, following Serre, we use a special case of the Guinand–Weil explicit formulas to generalize Proposition 1.1 and obtain improved discriminant lower bounds.

Let $F : \mathbb{R} \to \mathbb{R}$ be a differentiable function such that $F(-x) = F(x)$, $F(0) = 1$, and for some constants $C, \epsilon > 0$, we have the decay condition

$$|F(x)|, |F'(x)| \leq Ce^{-(1/2+\epsilon)|x|}. \tag{2.1}$$

Define the Mellin transform

$$\Phi(s) = \int_{-\infty}^{\infty} F(x)e^{(s-1/2)x}dx, \tag{2.2}$$

and note that $\Phi(s) = \Phi(1-s)$. In this setting, we have the following explicit formula.

Theorem 2.1. *We have*

$$\begin{aligned}\log D = {} & r_1\frac{\pi}{2} + n(\gamma + \log 8\pi) \\ & - r_1\int_0^{\infty}\frac{1-F(x)}{2\cosh(x/2)}dx - n\int_0^{\infty}\frac{1-F(x)}{2\sinh(x/2)}dx - 2\Phi(0) \\ & + {\sum_{\rho}}'\Phi(\rho) + 2\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}F(m\log N\mathfrak{p}).\end{aligned}$$

Before proving this, let us see how it implies lower bounds for the discriminant. If we choose F so that $F(x) \geq 0$ and $\operatorname{Re}\Phi(\rho) \geq 0$ for all zeroes ρ of $\zeta_K(s)$, then we may ignore the last two terms in the equation above and obtain the inequality

$$\begin{gathered}\log D \geq r_1\left(\frac{\pi}{2} + \gamma + \log 8\pi - I_1 - I_2\right) + 2r_2\left(\gamma + \log 8\pi - I_2\right) - 2\Phi(0) \\ \text{where } I_1 = \int_0^{\infty}\frac{1-F(x)}{2\cosh(x/2)}dx \quad \text{and} \quad I_2 = \int_0^{\infty}\frac{1-F(x)}{2\sinh(x/2)dx}.\end{gathered} \tag{2.3}$$

(If we have information about the factorization of primes in K or the distribution of the zeroes of ζ_K, then we can do even better.)

First, let us assume the generalized Riemann hypothesis. Note that the Fourier transform $\hat{F}(\xi) = \int_{-\infty}^{\infty} F(x)e^{-ix\xi}dx$ is simply $\Phi(\frac{1}{2} - i\xi)$, so it suffices to choose F such that F and $\hat{F}$

are both positive on the real line. If we take $F(x) = e^{-(x/b)^2}$, with b chosen appropriately in terms of n (e.g. $b = \sqrt{\log n}$), then we may guarantee that $I_1 = o(1)$, $I_2 = o(1)$, and $\Phi(0) = o(n)$. Using (2.3), we have therefore proven the following.

Corollary 2.2. *Assuming the generalized Riemann hypothesis for K,*

$$D \geq (8\pi e^{\pi/2+\gamma})^{r_1}(8\pi e^{\gamma})^{2r_2}e^{o(n)}.$$

No other choice of F can give a better main term, but it is possible to improve the error term. Among those functions of the form $F(x) = G(x/b)$ with b depending on the signature (r_1, r_2) of K, it turns out that the best choice for G is the function

$$G(x) = \begin{cases} (1-|x|)\cos(\pi x) + \frac{1}{\pi}\sin|\pi x| & \text{if } |x| \leq 1, \\ 0 & \text{otherwise} \end{cases} \tag{2.4}$$

considered by Odlyzko.

Let us now consider the question of what can be shown without assuming the Riemann hypothesis for K. We must choose F so that $F(x) \geq 0$ and $\operatorname{Re}\Phi(s) \geq 0$ for all s in the critical strip $0 \leq \operatorname{Re} s \leq 1$. Since $\operatorname{Re}\Phi(s)$ is harmonic and $\Phi(s) = \Phi(1-s)$, $\operatorname{Re}\Phi(s)$ is positive in the critical strip if and only if it is positive on the line $\operatorname{Re} s = 1$. If we let $f(x) = F(x)\cosh(x/2)$, then

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} F(x)\frac{e^{(1/2-i\xi)x} + e^{(-1/2-i\xi)x}}{2}dx = \frac{\Phi(1-i\xi) + \Phi(-i\xi)}{2} = \operatorname{Re}\Phi(1-i\xi), \tag{2.5}$$

so we may choose any function f such that f and $\hat{f}$ are both positive and let $F(x) = \frac{f(x/b)}{\cosh(x/2)}$. For the appropriate choice of b in terms of n, we may obtain

$$\begin{aligned} I_1 &= \int_0^{\infty} \frac{1 - f(x/b)/\cosh(x/2)}{2\cosh(x/2)}dx = \int_0^{\infty} \frac{1 - 1/\cosh(x/2)}{2\cosh(x/2)}dx + o(1) = \frac{\pi}{2} - 1 + o(1), \\ I_2 &= \int_0^{\infty} \frac{1 - f(x/b)/\cosh(x/2)}{2\sinh(x/2)}dx = \int_0^{\infty} \frac{1 - 1/\cosh(x/2)}{2\sinh(x/2)}dx + o(1) = \log 2 + o(1), \end{aligned} \tag{2.6}$$

and $\Phi(0) = o(n)$. Combining this with (2.3), we have the following bound.

Corollary 2.3. $D \geq (4\pi e^{1+\gamma})^{r_1}(4\pi e^{\gamma})^{2r_2}e^{o(n)}$.

Again, the leading term here is optimal among all choices of F, but the error term can be improved. In particular, Tartar showed that among a certain class of functions of the form $g(x/b)$, the best choice of g is

$$g(x) = \frac{9}{x^6}(\sin x - x\cos x)^2. \tag{2.7}$$

In practice, for fields of small degree, the estimates given by this choice of g are very close to the actual minimum value of D. The estimates assuming GRH are even closer.

We conclude with the proof of the explicit formula.

Proof of Theorem 2.1. For any $T > 0$ such that both T and $-T$ avoid the imaginary part of any zero $\rho = a + ib$ of Λ_K, we have

$$\sum_{|b|<T} \Phi(\rho) = \frac{1}{2\pi i} \int_{R_T} \Phi(s) \frac{\Lambda_K'}{\Lambda_K}(s) ds, \tag{2.8}$$

where R_T is the boundary of the rectangle $(-\delta, 1+\delta) \times (-T, T)$ for some choice of $\delta \in (0, \epsilon)$ (recall that $\Phi(s)$ is holomorphic on $-\epsilon < \operatorname{Re} s < 1 + \epsilon$ by (2.1)). On the horizontal lines of R_T, we have $|\Phi(s)| = O(\frac{1}{T})$ and $\left|\frac{\Lambda_K'}{\Lambda_K}(s)\right| = O(\frac{1}{\log T})$, so we may let $T \to \infty$ and use the functional equations $\Phi(s) = \Phi(1-s)$ and $\Lambda_K(s) = \Lambda_K(1-s)$ to find

$$\sum_{\rho}{}' \Phi(\rho) = \frac{1}{\pi i} \int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s) \frac{\Lambda_K'}{\Lambda_K}(s) ds. \tag{2.9}$$

We will split up $\frac{\Lambda_K'}{\Lambda_K}(s)$ as

$$\begin{aligned} \frac{\Lambda_K'}{\Lambda_K}(s) = &\left(\frac{1}{s} + \frac{1}{s-1}\right) \\ &+ \left(\frac{1}{2}\log D - r_2 \log 2 - \frac{n}{2}\log \pi\right) \\ &+ \left(\frac{r_1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s}{2}\right) + r_2 \frac{\Gamma'}{\Gamma}(s)\right) \\ &+ \left(\frac{\zeta_K'}{\zeta_K}(s)\right). \end{aligned} \tag{2.10}$$

and evaluate the integral with respect to each of these four summands in turn.

First,

$$\frac{1}{\pi i} \int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s) \left(\frac{1}{s} + \frac{1}{s-1}\right) = \Phi(0) + \Phi(1) = 2\Phi(0) \tag{2.11}$$

by Cauchy's theorem and the functional equation $\Phi(s) = \Phi(1-s)$.

Next, by Fourier inversion applied to the function $F(x)e^{(1/2+\delta)x}$, we find

$$\frac{1}{\pi i} \int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s) ds = \frac{1}{\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} F(x) e^{(1/2+\delta+it)x} dx dt = 2F(0) = 2, \tag{2.12}$$

For the third summand, we will have to do some real work. Let

$$\psi(s) = \frac{\Gamma'}{\Gamma}(s) = -\int_0^\infty \left(\frac{e^{-xs}}{1-e^{-x}} - \frac{e^{-x}}{x}\right) dx, \tag{2.13}$$

so that we have

$$\begin{aligned}
\psi(1/2+it) &= -\int_0^\infty \left(\frac{e^{-itx}}{2\sinh(x/2)} - \frac{e^{-x}}{x}\right) dx, \\
\psi(1/4+it/2) &= -\int_0^\infty \left(\frac{e^{x/2}e^{-itx}}{\sinh(x)} - \frac{e^{-2x}}{x}\right) dx \\
&= -\int_0^\infty \left(\frac{e^{x/2}e^{-itx}}{\sinh(x)} - \frac{e^{-x}}{x}\right) dx - \log 2, \quad \text{and hence} \\
\psi(1/4+it/2) - \psi(1/2+it) + \log 2 &= -\int_0^\infty \frac{e^{-itx}}{2\cosh(x/2)} dx.
\end{aligned} \tag{2.14}$$

In particular, we have the special values

$$\begin{aligned}
\int_0^\infty \left(\frac{1}{2\sinh(x/2)} - \frac{e^{-x}}{x}\right) dx &= -\psi(1/2) = \gamma + 2\log 2 \quad \text{and} \\
\int_0^\infty \frac{dx}{2\cosh(x/2)} &= -\psi(1/4) + \psi(1/2) - \log 2 = \frac{\pi}{2}.
\end{aligned} \tag{2.15}$$

Therefore, we may compute

$$\begin{aligned}
\frac{1}{\pi i}\int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s)\psi(s)ds &= \frac{1}{\pi i}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty} \Phi(s)\psi(s)ds \\
&= \frac{1}{\pi}\int_{-\infty}^{\infty} \Phi(1/2+it)\psi(1/2+it)dt \\
&= \frac{1}{\pi}\int_{-\infty}^{\infty} \hat{F}(t)\int_0^\infty \left(\frac{-e^{-itx}}{2\sinh(x/2)} + \frac{e^{-x}}{x}\right) dxdt \\
&= \frac{1}{\pi}\int_0^\infty \frac{1}{2\sinh(x/2)}\left(\int_{-\infty}^{\infty} \hat{F}(t)(1-e^{-itx})dt\right) dx - 2(\gamma + 2\log 2) \\
&= 2\int_0^\infty \frac{1-F(x)}{2\sinh(x/2)} dx - 2\gamma - 4\log 2,
\end{aligned} \tag{2.16}$$

and similarly

$$\frac{1}{\pi i}\int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s)\left(\psi(s/2) - \psi(s) + \log 2\right) ds = 2\int_0^\infty \frac{1-F(x)}{2\cosh(x/2)} dx - \pi. \tag{2.17}$$

Altogether, using the relation

$$\frac{r_1}{2}\psi(s/2) + r_2\psi(s) = \frac{n}{2}\psi(s) + \frac{r_1}{2}(\psi(s/2) - \psi(s) + \log 2) - \frac{r_1}{2}\log 2, \tag{2.18}$$

this gives

$$\begin{aligned}\frac{1}{\pi i}\int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s)\left(\frac{r_1}{2}\psi(s/2) + r_2\psi(s)\right) ds = n\int_0^\infty \frac{1-F(x)}{2\sinh(x/2)}dx + r_1\int_0^\infty \frac{1-F(x)}{2\cosh(x/2)}dx \\ - n\gamma - 2n\log 2 - r_1\frac{\pi}{2} - r_1\log 2.\end{aligned} \tag{2.19}$$

As for the final summand, we have $\frac{\zeta_K'}{\zeta_K}(s) = -\sum_{\mathfrak{p}}\sum_{m=1}^\infty \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{ms}}$. For each individual term $\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{ms}}$, we have

$$\begin{aligned}\frac{1}{\pi i}\int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s)\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{ms}}ds &= \frac{1}{\pi}\log N\mathfrak{p}\int_{-\infty}^\infty \frac{1}{N\mathfrak{p}^{m(1+\delta+it)}}\int_{-\infty}^\infty F(x)e^{(1/2+\delta+it)x}dx\,dt \\ &= \frac{1}{\pi}\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}\int_{-\infty}^\infty\int_{-\infty}^\infty F(u+m\log N\mathfrak{p})e^{(1/2+\delta)u}e^{itu}du\,dt \\ &= 2\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}F(m\log N\mathfrak{p}),\end{aligned} \tag{2.20}$$

with the second equality coming from the substitution $u = x - m\log N\mathfrak{p}$ and the third coming from Fourier inversion applied to the function $F(u+m\log N\mathfrak{p})e^{(1/2+\delta)u}$. Summing over $\mathfrak{p}$ and m, we find

$$\frac{1}{\pi i}\int_{1+\delta-i\infty}^{1+\delta+i\infty} \Phi(s)\frac{\zeta_K'}{\zeta_K}(s)ds = -2\sum_{\mathfrak{p}}\sum_{m=1}^\infty \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}F(m\log N\mathfrak{p}). \tag{2.21}$$

Putting (2.11), (2.12), (2.19), and (2.21) together with (2.9) gives the equation

$$\begin{aligned}\sum_\rho{}' \Phi(\rho) &= 2\Phi(0) \\ &\quad + \log D - 2r_2\log 2 - n\log\pi \\ &\quad + n\int_0^\infty \frac{1-F(x)}{2\sinh(x/2)}dx + r_1\int_0^\infty \frac{1-F(x)}{2\cosh(x/2)}dx - n\gamma - 2n\log 2 - r_1\frac{\pi}{2} - r_1\log 2 \\ &\quad - 2\sum_{\mathfrak{p}}\sum_{m=1}^\infty \frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}F(m\log N\mathfrak{p}),\end{aligned} \tag{2.22}$$

which rearranges to give the formula claimed. □

3 Upper bounds and Golod–Shafarevich

So far, we have studied inequalities of the form $D_K \geq A^{r_1} B^{2r_2} e^{o(n)}$. In particular, if we let d_n be the minimum value of the root discriminant $D_K^{1/n}$ over all number fields K of degree n, then this implies $\liminf_{n\to\infty} d_n \geq \min(A, B)$. For some time, it was conjectured that $d_n \to \infty$ as $n \to \infty$. For example, the cyclotomic field $\mathbb{Q}(\zeta_\ell)$ given by adjoining a primitive ℓ^{th} root of unity has root discriminant

$$D_{\mathbb{Q}(\zeta_\ell)}^{1/\phi(\ell)} = \frac{\ell}{\prod_{p|\ell} p^{1/(p-1)}} \geq \sqrt{\ell} \geq \sqrt{\phi(\ell)}, \tag{3.1}$$

and it is known that the root discriminant tends to infinity for abelian extensions. However, Golod and Shafarevich [1] showed, in their solution to the class field tower problem in 1964, that $\liminf_{n\to\infty} d_n$ is finite, and in fact bounded from above by $\sqrt{120120} \approx 346.58$, as we will see. Using similar techniques, this was subsequently refined by Martinet [3] in 1978, who showed

$$\liminf_{n\to\infty} d_n \leq 2^{3/2}\ 11^{4/5}\ 23^{1/2} \approx 92.37, \tag{3.2}$$

and Hajir and Maire [2] in 2001, who showed

$$\liminf_{n\to\infty} d_n \leq 5^{1/4}\ 13^{1/4}\ 17^{1/8}\ 19^{1/8}\ 23^{1/4}\ 31^{1/8}\ 331^{1/4} \approx 83.89. \tag{3.3}$$

In this section, we will discuss the connection between the class field tower problem and upper bounds for $\liminf_{n\to\infty} d_n$, and we will demonstrate Golod and Shafarevich's approach to proving such a bound.

As before, let K be a number field. Let K_1 be the Hilbert class field of K, which is the maximal unramified abelian extension of K. Recall that there is a natural isomorphism between $\mathrm{Gal}(K_1/K)$ and the class group Cl_K of K given by the reciprocity map from class field theory, so in particular, the degree $[K_1 : K]$ is the class number of K. Let K_2 be the Hilbert class field of K_1, and continue in this fashion to obtain a tower of fields

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots \tag{3.4}$$

for which each field is the Hilbert class field of its predecessor. Let $K_\infty = \bigcup_n K_n$, which is an extension of K of possibly infinite degree. The class field tower problem asks whether this class field tower always stabilizes. In other words, it asks whether it is possible for K_∞ to have infinite degree over K.

Let p be a prime. Because p-groups are easier to understand than general solvable groups, we will actually consider p-extensions, which are Galois extensions whose Galois group is a p-group. The *Hilbert p-class field* K_1^p of K is the maximal unramified abelian p-extension of K, and we define the *p-class field tower*

$$K \subseteq K_1^p \subseteq K_2^p \subseteq K_3^p \subseteq \dots \tag{3.5}$$

and $K_\infty^p = \bigcup_n K_n^p$ as before. Note that $K_n^p \subseteq K_n$ and $K_\infty^p \subseteq K_\infty$, so if the p-class field tower is infinite, then so is the class field tower.

Example. Consider the field $K = \mathbb{Q}(\sqrt{-30})$, for which the class field tower has length 2 and consists of the fields

$$\begin{aligned} K &= \mathbb{Q}(\sqrt{-30}), \\ K_1 &= \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt{5}), \quad \text{and} \\ K_2 &= \mathbb{Q}\left(\sqrt{2}, \sqrt{-2+\sqrt{-3}+\sqrt{5}}\right) = K_\infty. \end{aligned} \tag{3.6}$$

Since each of these extensions is a 2-extension, this is also the 2-class field tower of K, and in particular $K_\infty^2 = K_\infty = K_2$.

Usually, the class field tower of K is used for determining whether K can be embedded in a number field with class number 1, but the connection between class field towers and discriminant upper bounds comes from the following lemma.

Lemma 3.1. *If L/K is an unramified extension of number fields, then $D_L^{1/[L:\mathbb{Q}]} = D_K^{1/[K:\mathbb{Q}]}$.*

Proof. For any extension L/K of number field, the relative discriminant $D_{L/K}$ satisfies $D_L = N_{K/\mathbb{Q}}(D_{L/K}) D_K^{[L:K]}$. If L/K is unramified, then $D_{L/K} = (1)$. □

In particular, each field in the p-class field tower of K has the same root discriminant, so if this tower is infinite, then $\liminf_{n\to\infty} d_n \leq D_K^{1/[K:\mathbb{Q}]}$.

As an aside, together with the ideas from the preceding section, this gives one way of upper bounding the class number. For example, if D_K is small enough that all fields of higher degree must have a larger root discriminant, then the Hilbert class field of K must be K itself, so Cl_K must be trivial.

Our main result in this section is a criterion under which K has an infinite p-class field tower. Given a group G, we define G/p to be the maximal abelian quotient of G of exponent p, regarded as a vector space over $\mathbb{F}_p$, and we let $d^p G = \dim G/p$.

Theorem 3.2. *If K has a finite p-class field tower, then*

$$d^p \mathrm{Cl}_K < 2 + 2\sqrt{1 + d^p \mathfrak{o}_K^\times}$$

where $\mathfrak{o}_K$ is the ring of integers of K.

Note that by Dirichlet's unit theorem, $\mathfrak{o}_K^\times \cong \mathbb{Z}^{r_1+r_2-1} \times W_K$ where W_K is the group of roots of unity in K, so

$$d^p \mathfrak{o}_K^\times = \begin{cases} r_1 + r_2 - 1 & \text{if } \zeta_p \notin K, \\ r_1 + r_2 & \text{if } \zeta_p \in K, \end{cases} \tag{3.7}$$

where ζ_p is a primitive p^{th} root of unity.

For example, consider the field $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$ a fundamental discriminant. Since $d^2 \mathfrak{o}_K^\times = 1$, K has an infinite class field tower so long as $d^2 \operatorname{Cl}_K \geq 2 + 2\sqrt{2}$. By Gauss's genus theory, $d^2 \operatorname{Cl}_K = t - 1$ where t is the number of ramified primes in K, so letting

$$D = -8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = -120120, \tag{3.8}$$

we obtain the following.

Corollary 3.3. $\liminf_{n\to\infty} d_n \leq \sqrt{120120}$.

Before embarking on the proof of Theorem 3.2, we will need some results about the homology of p-groups. Recall that for a group G and a $\mathbb{Z}[G]$-module A, the *homology groups* $H_i(G, A)$ are characterized by the following properties.

i. $H_0(G, A) = A/I_G A$ with I_G the augmentation ideal $\ker(\mathbb{Z}[G] \to \mathbb{Z}) = \langle \sigma - 1 \mid \sigma \in G \rangle$.

ii. For every short exact sequence $0 \to A \to B \to C \to 0$, there is a natural exact homology sequence

$$\cdots \to H_1(G, A) \to H_1(G, B) \to H_1(G, C) \to A/I_G A \to B/I_G B \to C/I_G C \to 0.$$

iii. If A is a direct summand of $\mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ for some abelian group X on which G acts trivially, then $H_i(G, A) = 0$ for all $i \geq 1$.

From the short exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, we find $H_1(G, \mathbb{Z}) = H_0(I_G, G) = I_G/I_G^2$. The map $\sigma \mapsto \sigma - 1$ induces an isomorphism $G^{\text{ab}} \to I_G/I_G^2$, so we also have

iv. $H_1(G, \mathbb{Z}) = G^{\text{ab}}$.

Fix now a prime p and a finite p-group G. For convenience, we will write $H_i(A)$ for the group $H_i(G, A)$. Recalling our notation from earlier, we let $\mathbb{Z}/p$ denote the cyclic group of order p. The homology groups $H_i(\mathbb{Z}/p)$ are annihilated by p, and therefore may be regarded as vector spaces over $\mathbb{F}_p$, and we define $d_i^p G = \dim H_i(\mathbb{Z}/p)$. We first compute $d_1^p G$ and $d_2^p G$, and in particular show that this notation generalizes the notion of $d^p G$ from before.

Lemma 3.4. *We have*

$$d_1^p G = d^p G \quad \textit{and}$$
$$d_2^p G = d^p G + d^p H_2(\mathbb{Z}).$$

Proof. The short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \to \mathbb{Z}/p \to 0 \tag{3.9}$$

induces the exact homology sequence

$$H_i(\mathbb{Z}) \xrightarrow{p} H_i(\mathbb{Z}) \to H_i(\mathbb{Z}/p) \to H_{i-1}(\mathbb{Z}) \xrightarrow{p} H_{i-1}(\mathbb{Z}), \tag{3.10}$$

and hence the short exact sequence

$$0 \to H_i(\mathbb{Z})/p \to H_i(\mathbb{Z}/p) \to H_{i-1}(\mathbb{Z})[p] \to 0. \tag{3.11}$$

Letting $i = 1$ and noting that $H_0(\mathbb{Z}) = \mathbb{Z}$ and $H_1(\mathbb{Z}) = G^{\mathrm{ab}}$, we find

$$H_1(\mathbb{Z}/p) = H_1(\mathbb{Z})/p = G/p, \tag{3.12}$$

which gives the first equality. Letting $i = 2$ and noting that $\dim A[p] = \dim A/p$ for any finite abelian group A, we obtain the second. □

Example. Returning to the case where $K = \mathbb{Q}(\sqrt{-30})$, we find that the Galois group $G = \mathrm{Gal}(K_\infty^2/K)$ is isomorphic to the quaternion group of order 8. In this case, we have

$$\begin{aligned} H_1(\mathbb{Z}) &= (\mathbb{Z}/2)^2, \quad H_1(\mathbb{Z}/2) = (\mathbb{Z}/2)^2, \\ H_2(\mathbb{Z}) &= 0, \quad \text{and} \quad H_2(\mathbb{Z}/2) = (\mathbb{Z}/2)^2. \end{aligned} \tag{3.13}$$

Note that

$$d_1^2 G = 2 = d^2 G \quad \text{and} \quad d_2^2 G = 2 = d^2 G + d^2 H_2(\mathbb{Z}), \tag{3.14}$$

as in the lemma.

We now give non-commutative versions of Nakayama's lemma and the Hilbert syzygy theorem.

Lemma 3.5. *If A is a G-module with $pA = 0$, then the minimal number of generators of A as a G-module is $\dim H_0(A)$. More precisely, $\{a_i\}$ generate A as a G-module if and only if their images in $A/I_G A$ generate $A/I_G A$ as a vector space.*

Proof. Suppose $\{a_i\}$ generate A/IA, and let B be the G-submodule of A generated by $\{a_i\}$. The short exact sequence

$$0 \to B \to A \to A/B \to 0 \tag{3.15}$$

induces the exact homology sequence

$$H_0(B) \to H_0(A) \to H_0(A/B) \to 0. \tag{3.16}$$

The map $H_0(B) \to H_0(A)$ is the same as the map $B/I_G B \to A/I_G A$, which is surjective, so $H_0(A/B) = 0$. It follows that $A = B$ because otherwise, $\mathrm{Hom}(A/B, \mathbb{Z}/p)$ would be non-zero, and hence so would $\mathrm{Hom}_G(A/B, \mathbb{Z}/p)$ since G is a p-group, but $\mathrm{Hom}_G(A/B, \mathbb{Z}/p)$ is the dual of $H_0(A/B) = 0$. □

Lemma 3.6. *If A is a G-module with $pA = 0$, then there exists a resolution*

$$\cdots \to Y_2 \xrightarrow{\partial} Y_1 \xrightarrow{\partial} Y_0 \to A \to 0$$

with each Y_n free of rank $\dim H_i(A)$ over $\mathbb{Z}[G]/p$ and $\partial Y_{i+1} \subseteq I_G Y_i$.

Proof. By the previous lemma, there is a free module X of rank $\dim H_0(A)$ over $\mathbb{Z}[G]$ and a surjection $X \to A$, which induces a surjection $X/p \to A$ since $pA = 0$. Let $Y_0 = X/p$, and note that $H_i(Y_0) = 0$ for $i \geq 1$. Let B be the kernel of $Y_0 \to A$, so that we have the exact homology sequence

$$\cdots \to H_{i+1}(Y_0) \to H_{i+1}(A) \to H_i(B) \to H_i(Y_0) \to \cdots, \tag{3.17}$$

and hence

$$H_{i+1}(A) = H_i(B) \quad \text{for } i \geq 1. \tag{3.18}$$

For $i = 0$, we have the exact sequence

$$0 \to H_1(A) \to H_0(B) \to H_0(Y_0) \to H_0(A) \to 0. \tag{3.19}$$

Since $H_0(Y) \to H_0(A)$ is a surjective map of $\mathbb{Z}/p$-modules of the same dimension, it is an isomorphism, so (3.18) also holds for $i = 0$, and the map $H_0(B) \to H_0(Y_0)$ is the zero map, which means $B \subseteq I_G Y_0$.

Applying the same process to B, we obtain a free module Y_1 of rank $\dim H_0(B) = \dim H_1(A)$ over $\mathbb{Z}[G]/p$ and a surjection $Y_1 \to B$ with kernel C such that $C \subseteq I_G Y_1$ and

$$H_i(C) = H_{i+1}(B) = H_{i+2}(A) \quad \text{for } i \geq 0. \tag{3.20}$$

Letting $Y_1 \xrightarrow{\partial} Y_0$ be the composition $Y_1 \to B \to Y_0$, we have $\partial Y_1 \subseteq Y_0$. Continuing in this fashion, we obtain the lemma by induction. □

In particular, applying the lemma to $A = \mathbb{Z}/p$, we find that there is an exact sequence

$$Y_2 \xrightarrow{\partial} Y_1 \xrightarrow{\partial} Y_0 \to \mathbb{Z}/p \to 0 \tag{3.21}$$

with Y_i free of rank $d_i^p G$ over $\mathbb{Z}[G]/p$ and $\partial Y_{i+1} \subseteq I_G Y_i$. The kernel of $Y_0 \to \mathbb{Z}/p$ is contained in $I_G Y_0$, which is of codimension 1 since $Y_0/I_G Y_0 = H_0(Y_0) = \mathbb{Z}/p$, and is therefore equal to $I_G Y_0$. As a consequence, we actually have an exact sequence

$$Y_2 \xrightarrow{\partial} Y_1 \to I_G Y_0 \to 0, \tag{3.22}$$

with Y_i free of rank $d_i^p G$ over $\mathbb{Z}[G]/p$ and $\partial Y_2 \subseteq I_G Y_1$, and it is this exact sequence which we will need.

Our goal now is to prove the following theorem, which we will see is the group-theoretic form of Theorem 3.2.

Theorem 3.7. *For any finite p-group G,*

$$d_2^p G > \frac{1}{4}(d_1^p G)^2.$$

For the proof, we will require the notion of the *Poincaré polynomial* of a finite G-module A with $pA = 0$, which is defined by

$$P_A(t) = \sum_{n=0}^{\infty} c_n(A)t^n \quad \text{where } c_n(A) = \dim I_G^n A / I_G^{n+1} A. \tag{3.23}$$

(Since A is finite, $c_n(A) = 0$ for $n \gg 0$, so $P_A(t)$ is indeed a polynomial.) Note that

$$P_A(t)\frac{1}{1-t} = \sum_{n=0}^{\infty} s_n(A)t^n \quad \text{where } s_n(A) = \dim A / I_G^{n+1} A. \tag{3.24}$$

Example. With G once again the quaternion group, a (somewhat lengthy) computation shows that the Poincaré polynomial of $\mathbb{Z}[G]/2$ is $1 + 2t + 2t^2 + 2t^3 + t^4$.

Proof. Tensoring (3.22) with $\mathbb{Z}[G]/I_G^{n+1}$, we obtain the exact sequence

$$Y_2/I_G^{n+1}Y_2 \xrightarrow{\partial} Y_1/I_G^{n+1}Y_1 \to I_G Y_0/I_G^{n+2}Y_0 \to 0. \tag{3.25}$$

In fact, since $\partial(I_G^n Y_2) \subseteq I_G^n(\partial Y_2) \subseteq I_G^{n+1}Y_1$, we even have the exact sequence

$$Y_2/I_G^{n}Y_2 \xrightarrow{\partial} Y_1/I_G^{n+1}Y_1 \to I_G Y_0/I_G^{n+2}Y_0 \to 0. \tag{3.26}$$

Comparing dimensions, we find

$$s_n(Y_1) \le s_{n-1}(Y_2) + s_n(I_G Y_0), \tag{3.27}$$

and hence

$$P_{Y_1}(t)\frac{1}{1-t} \le P_{Y_2}(t)\frac{t}{1-t} + P_{I_G Y_0}(t)\frac{1}{1-t} \quad \text{for } 0 < t < 1. \tag{3.28}$$

Let $d = d_1^p G$, $r = d_2^p G$, and $P(t) = P_{Y_0}(t)$, and note that

$$\begin{aligned} P_{I_G Y_0}(t) &= \frac{P(t)-1}{t} && \text{because } c_0(Y_0) = \dim H_0(Y_0) = 1, \\ P_{Y_1}(t) &= dP(t) && \text{because } Y_1 = Y_0^d, \text{ and} \\ P_{Y_2}(t) &= rP(t) && \text{because } Y_2 = Y_0^r. \end{aligned} \tag{3.29}$$

Multiplying (3.28) by $(1-t)$ and rewriting in terms of $P(t)$, we find

$$dP(t) \leq rtP(t) + \frac{P(t)-1}{t} \quad \text{for } 0 < t < 1, \tag{3.30}$$

or equivalently,

$$1 \leq P(t)(rt^2 - dt + 1) \quad \text{for } 0 < t < 1. \tag{3.31}$$

Since $P(t)$ has positive coefficients, we conclude

$$0 < rt^2 - dt + 1 \quad \text{for } 0 < t < 1. \tag{3.32}$$

By Lemma 3.4, $d \leq r < 2r$, so we may substitute $t = \frac{d}{2r}$ to find $r > \frac{1}{4}d^2$, as claimed. □

With the homological legwork taken care of, we may now deduce Theorem 3.2 from class field theory.

Proof of Theorem 3.2. Suppose K has a finite p-class field tower, and let $G = \mathrm{Gal}(K_\infty^p/K)$, which is a finite p-group. Since G^{ab} is the Galois group of K_1^p/K, which is the p-Sylow subgroup of Cl_K, we find $d^pG = d^p \mathrm{Cl}_K$, and hence our goal is to show

$$d^pG < 2 + 2\sqrt{1 + d^p\mathfrak{o}_K^\times}. \tag{3.33}$$

Rearranging, this inequality gives

$$\frac{1}{4}(d^pG)^2 - d^pG < d^p\mathfrak{o}_K^\times. \tag{3.34}$$

By Lemma 3.4 and Theorem 3.7, we know

$$\frac{1}{4}(d^pG)^2 - d^pG = \frac{1}{4}(d_1^pG)^2 - d^pG < d_2^pG - d^pG = d^pH_2(\mathbb{Z}), \tag{3.35}$$

so it suffices to show

$$d^pH_2(\mathbb{Z}) \leq d^p\mathfrak{o}_K^\times. \tag{3.36}$$

Indeed, this follows from class field theory. For convenience, write L for K_∞^p. Let $C_L = \mathbb{A}_L^\times/L^\times$ be the idéle class group of L, and let

$$U_L = \{\alpha \in \mathbb{A}_L^\times \mid \alpha_\mathfrak{p} \in \mathfrak{o}_{L,\mathfrak{p}}^\times \text{ for all finite primes } \mathfrak{p}\} \tag{3.37}$$

be the group of idéle units. Since L/K is unramified, U_L is cohomologically trivial, and since L is its own Hilbert p-class field, the ideal class group Cl_L is cohomologically trivial. Therefore, the exact sequences

$$1 \to \mathfrak{o}_L^\times \to U_L \to U_L/\mathfrak{o}_L^\times \to 1 \quad \text{and} \quad 1 \to U_L/\mathfrak{o}_L^\times \to C_L \to \mathrm{Cl}_L \to 1 \tag{3.38}$$

imply

$$\hat{H}^i(\mathfrak{o}_L^\times) = \hat{H}^{i-1}(U_L/\mathfrak{o}_L^\times) = \hat{H}^{i-1}(C_L). \tag{3.39}$$

Tate's theorem of cohomology in class field theory states $\hat{H}^{i-1}(C_L) = \hat{H}^{i-3}(\mathbb{Z})$, so letting $i = 0$ and recalling that $\hat{H}^{-3}(\mathbb{Z}) = H_2(\mathbb{Z})$, we find

$$H_2(\mathbb{Z}) = \hat{H}^0(\mathfrak{o}_L^\times) = \mathfrak{o}_K^\times / N_{L/K}\mathfrak{o}_L^\times, \tag{3.40}$$

and hence $d^p H_2(\mathbb{Z}) \leq d^p \mathfrak{o}_K^\times$, as claimed. □

Altogether, we have now shown

$$22.38 \leq \liminf_{n\to\infty} d_n \leq 346.58. \tag{3.41}$$

For our upper bound, we made use of a tower of fields, each with the same root discriminant, and necessarily with highly composite degrees. In fact, it is still unknown whether $d_p \to \infty$ as $p \to \infty$ with p prime.

Another natural question to ask is what happens for discriminants of polynomials rather than number fields. More precisely, let d'_n be the minimum value of the root discriminant $D_f^{1/n}$ over all monic integral polynomials f of degree n. If θ is a root of f, then

$$D_f = D_{\mathbb{Z}[\theta]} = [\mathfrak{o}_{K(\theta)} : \mathbb{Z}[\theta]]^2 D_{K(\theta)}, \tag{3.42}$$

which means $d'_n \geq d_n$ and all the lower bounds for d_n apply to d'_n as well. However, it is still not known whether $d'_n \to \infty$ as $n \to \infty$.

References

[1] E. S. Golod and I. R. Shafarevich. On class field towers. *Izv. Akad. Nauk SSSR*, 28:261–272, 1964.

[2] F. Hajir and C. Maire. Tamely ramified towers and discriminant bounds for number fields. *Compositio Mathematica*, 128(1):35–53, 2001.

[3] J. Martinet. Tours de corps de classes et estimations de discriminants. *Inventiones Mathematicae*, 44(1):65–73, 1978.

[4] H. Minkowski. Théorèmes arithmétiques. *C.R. Acad. Sci. Paris*, 112:209–212, 1891.

[5] H. P. Mulholland. On the product of n complex homogeneous linear forms. *Journal of the London Mathematical Society*, 35(2):241–250, 1960.

[6] A. M. Odlyzko. Some analytic estimates of class numbers and discriminants. *Inventiones Mathematicae*, 29(3):275–286, 1975.

[7] A. M. Odlyzko. Lower bounds for discriminants of number fields. *Acta Arithmetica*, 29(3):275–297, 1976.

[8] A. M. Odlyzko. Lower bounds for discriminants of number fields, ii. *Tohoku Math. J. (2)*, 29(2):209–216, 1977.

[9] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results. *Journal de théorie des nombres de Bordeaux*, 2(1):119–141, 1990.

[10] C. A. Rogers. The product of n real homogeneous linear forms. *Acta Mathematica*, 82:185–208, 1950.

[11] J.-P. Serre. Minorations de discriminants. *Oeuvres - Collected Papers III*, page 240–243, 1975.

[12] H. M. Stark. Some effective cases of the brauer-siegel theorem. *Inventiones Mathematicae*, 23(2):135–152, 1974.