Points of small height.

Francesco Amoroso - LMNO

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen
France

These slides and the relevant articles are on
www.math.unicaen.fr/~amoroso/height

Some References

1. Heights:
   - E. Bombieri and W. Gubler. "Heights in Diophantine Geometry", Cambridge University Press, 2006.
2. Diophantine Approximation:
   - M. Waldschmidt. "Diophantine approximation on linear algebraic groups", Grundlehren 326, Springer, 2000.
3. Algebraic Number Theory:
   - J. W. S. Cassels and A. Frölich. Algebraic number theory. Proceedings of an instructional conference organized by the London Mathematical Society, Academic Press, 1967.
4. Local Fields & Ramification Theory:
   - J. W. S. Cassels, "Local fields". LMS Student Texts, 3, 1986.
   - J. P. Serre "Corps locaux". Hermann, 1968.

First lecture:

- Mahler's measure and Weil's height
- Lehmer's Problem
- Abelian Lower Bound
- Relative Lower Bound
- Absolute Abelian Lower Bound
- Sketch of the proof of the Abelian Lower Bound

Mahler's measure

We start by recalling some basic facts on Mahler's measure and on Weil's height. See Bombieri-Gubler, op. cit. for references.

Given a non-zero polynomial

$$f(x) = f_D \prod_{j=1}^{D} (x - \alpha_j) \in \mathbb{C}[x]$$

its Mahler's measure is

$$M(f) = |f_D| \prod_{j=1}^{D} \max\{|\alpha_j|, 1\} = \exp \int_0^1 \log |f\left(e^{2\pi i t}\right)| dt \ .$$

The last equality follows from Jensen's formula.

Weil's height

Let α be an algebraic number of degree $D = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ with minimal polynomial over $\mathbb{Z}$

$$f(x) = f_D \prod_{j=1}^{D} (x - \alpha_j) \in \mathbb{Z}[x]$$

($\alpha_1 = \alpha$). The (absolute, logarithmic) Weil height of α is

$$\hat{h}(\alpha) = \frac{1}{D} \log M(f) = \frac{1}{D} \left(\log |f_D| + \sum_{j=1}^{D} \log^+ |\alpha_j| \right) ,$$

where $\log^+ x = \max(0, \log x)$ for $x > 0$ (and $\log^+ 0 = 0$). Thus $\hat{h}(\alpha) = \log H(\alpha)$, whith $H(\alpha)$ as in Widmer's lectures.

Some examples

- $\hat{h}(p/q) = \log \max(|p|, q)$ $(p,\ q \in \mathbb{Z},\ q > 0,\ (p,q) = 1)$
- $\hat{h}(\sqrt{2}) = \frac{1}{2}(\log^+ |\sqrt{2}| + \log^+ | - \sqrt{2}|) = \frac{1}{2}\log 2$
- More generally, $\hat{h}(2^{1/D}) = (\log 2)/D$
- a root of unity ζ has height $\hat{h}(\zeta) = 0$
- The polynomial $x^3 - x - 1$ has one positive real root

$$\theta = 1.324...$$

and the other two roots of absolute value < 1, i.e. θ is a *Pisot's* number. Thus $\hat{h}(\theta) = \frac{1}{3}\log\theta$. More precisely, θ is the smallest Pisot's number.

- Let $\rho = \frac{\pm\sqrt{14}\pm i\sqrt{2}}{4}$ one of the roots of $2x^4 - 3x^2 + 2$. Since $|\rho| = 1$, we have $\hat{h}(\rho) = \frac{\log 2}{4} = 0.173....$

Absolute values

Let $\mathbb{K}$ be a field. An absolute value of $\mathbb{K}$ is a (non trivial) map $|\cdot|: \mathbb{K} \to \mathbb{R}$ such that

- $|x| \geq 0$ and $|x| = 0$ iff $x = 0$
- $|xy| = |x||y|$
- $|x + y| \leq |x| + |y|$

If the strong inequality $|x + y| \leq \max\{|x|, |y|\}$ holds we say that $|\cdot|$ is non-archimedean.

An absolute value defines a topology on $\mathbb{K}$.

Two absolute values are equivalent, if they define the same topology.

A place is an equivalence class of absolute values. We denote by $\mathcal{M}_{\mathbb{K}}$ the set of places of $\mathbb{K}$.

Absolute values

Let now $\mathbb{K}$ be a number field.

An embedding $\sigma : \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$ defines an archimedean absolute value: $|\alpha|_\sigma = |\sigma\alpha|_{\mathbb{C}}$.

An integral prime ideal P defines a non-archimedean absolute value: $|\alpha|_P = (N_{\mathbb{K}/\mathbb{Q}}P)^{-\lambda}$, where the factorization of the fractional ideal (α) is

$$(\alpha) = P^\lambda \cdots$$

These are (up equivalence) all the absolute values of $\mathbb{K}$. Thus any $v \in \mathcal{M}_{\mathbb{K}}$ is the equivalence class (with respect to the induced topology) of:

- an embedding σ (archimedean place: we write $v \mid \infty$)
- a prime P (non-archimedean place: we write $v \nmid \infty$)

We identify v with σ and with P, respectively.

Absolute values

We let $\mathbb{K}_v$ be the completion of $\mathbb{K}$ at v. Thus, if $v \mid \infty$, $v = \sigma$, then $[\mathbb{K}_v : \mathbb{Q}_v] = 1$ if $\sigma(\mathbb{K}) \subset \mathbb{R}$ and $[\mathbb{K}_v : \mathbb{Q}_v] = 2$ otherwise. For $v \nmid \infty$, $v = P$, the degree $[\mathbb{K}_v : \mathbb{Q}_v]$ is the product of the ramification index and the inertia degree of P.

For $v \in \mathcal{M}_{\mathbb{K}}$, we choose a normalized absolute value in the class v as:

- $|\alpha|_v = |\sigma\alpha|$, if v is archimedean, $v = \sigma \colon \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$.
- $|\alpha|_v^{[\mathbb{K}_v:\mathbb{Q}_v]} = (N_{\mathbb{K}/\mathbb{Q}} P)^{-\lambda}$, if v is non-archimedean, $v = P$, and where the factorization of the fractional ideal (α) is

$$(\alpha) = P^{\lambda} \dots$$

This normalization agrees with the Product Formula ($\alpha \in \mathbb{K}^*$)

$$\prod_{v \in \mathcal{M}_{\mathbb{K}}} |\alpha|_v^{[\mathbb{K}_v:\mathbb{Q}_v]} = 1 \, .$$

An equivalent definition of Weil's height

$$\hat{h}(\alpha) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in \mathcal{M}_{\mathbb{K}}} [\mathbb{K}_v : \mathbb{Q}_v] \log^+ |\alpha|_v.$$

Let α, $\beta \in \overline{\mathbb{Q}}$. Then

- $\hat{h}(\alpha + \beta) \leq \hat{h}(\alpha) + \hat{h}(\beta) + \log 2$.
- $\hat{h}(\alpha\beta) \leq \hat{h}(\alpha) + \hat{h}(\beta)$.
- Moreover, if β is a root of 1, $\hat{h}(\alpha\beta) = \hat{h}(\alpha)$.
- For $n \in \mathbb{Z}$, $\hat{h}(\alpha^n) = |n|\hat{h}(\alpha)$.
- $\hat{h}(\alpha) = 0$ if and only if $\alpha = 0$ or α is a root of 1.
- $\hat{h}(\alpha) = \hat{h}(\beta)$ if α and β are algebraic conjugates.

Lehmer's problem

Let $f \in \mathbb{Z}[x]$, $f \neq 0$. Then $M(f) \geq 1$. Lehmer (1933) :

The following problem arises immediately. If ϵ is a positive quantity, to find a polynomial of the form

$$f(x) = x^r + a_1 x^{r-1} + \cdots + a_r$$

where the a's are integers, such that the absolute values of the product of those roots of f which lie outside the unit circle, lies between 1 and $1 + \epsilon$. (...) Whether or not the problem has a solution for $\varepsilon < 0.176$ we do not know.

Lehmer considers the polynomial

$$f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

which has one root $\tau > 1$. All other roots $\neq \tau, \tau^{-1}$ lie on the unit circle, i.e. τ is a *Salem's* number. Thus $M(f) = \tau = 1.176....$

Lehmer's problem

Let $f \in \mathbb{Z}[x]$ be a nonconstant irreducible polynomial. Assume $f \neq \pm x$ and that $\pm f$ is not a cyclotomic polynomial. By a theorem of Kronecker, $M(f) > 1$. Lehmer asks whether there exists an absolute constant $C > 1$ such that $M(f) \geq C$. Record : despite intensive computer search ... still Lehmer's polynomial!

We can rephrase Lehmer's problem using Weil's height instead of Mahler's measure. Let $\boldsymbol{\mu}$ be the set of roots of unity. Then an optimistic answer to Lehmer's problem is:

Conjecture (Lehmer)

Let $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ of degree D. Then there exists an absolute constant $c > 0$ such that

$$\hat{h}(\alpha) \geq \frac{c}{D}.$$

Dobrowolski's theorem

This should be the best possible lower bound for the height (without any further assumption on α), since

$$\hat{h}(2^{1/D}) = (\log 2)/D \ .$$

The best known result in the direction of Lehmer's conjecture is Dobrowolski's lower bound (1979)

$$\hat{h}(\alpha) \geq \frac{c}{D} \left(\frac{\log D}{\log \log D} \right)^{-3}$$

which holds for any $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ of degree $D \geq 2$. Here c is an absolute constant. In the original statement $c = 1/1200$; later Voutier shows that one can take $c = 1/4$.

Special Numbers

More generally, we can look for lower bounds for the height of numbers in special sets. Let S be a set of algebraic numbers. We consider, for $D \in \mathbb{N}$,

$$\inf\{\hat{h}(\alpha)\ , \alpha \in S \backslash \boldsymbol{\mu},\ \alpha \neq 0,\ [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D\}\ .$$

Smyth (1971) proved that if $\alpha \in \overline{\mathbb{Q}}^*$ is not a reciprocal number (*i.e.* if α^{-1} is not an algebraic conjugate of α), of degree D then

$$\hat{h}(\alpha) \geq \frac{\log \theta}{D}\ ,$$

where θ is the smallest Pisot's number, which we have defined before (it is the only real root of the equation $x^3 - x - 1 = 0$). This bound is optimal, since $\hat{h}(\theta) = \frac{1}{3}\log\theta$ (remark that Pisot's number are not-reciprocal).

Special Numbers

Also, Mignotte (1979) gave a positive answer to Lehmer's problem for any α of degree D such that there exists a prime $p \leq D \log D$ which splits completely in $\mathbb{Q}(\alpha)$.

More recently, Lehmer's problem was solved by Borwein, Dobrowolski and Mossinghoff (2004) for algebraic integers whose minimal polynomial has coefficients all congruent to 1 modulo a fixed $m \geq 2$.

Hence, Lehmer's problem is solved for:

- the set of non reciprocal numbers,
- the set of algebraic α such that there exists a "small" prime which splits completely in $\mathbb{Q}(\alpha)$,
- the set of algebraic integers whose minimal polynomial has coefficients all congruent to 1 modulo a fixed $m \geq 2$.

Special Numbers

For other sets S we know even more than Lehmer. For instance, if $\mathbb{Q}(\alpha)$ is a totally real field and $\alpha \neq \pm 1$, then, by a special case of a result of Schinzel's (1973),

$$\hat{h}(\alpha) \geq \frac{1}{2} \log \varphi = 0.240...$$

where φ is the golden ratio $\frac{1+\sqrt{5}}{2}$. Again, this result is optimal, since $\hat{h}(\varphi) = \frac{1}{2} \log \varphi$. More generally, let $\mathbb{K}$ be a CM field (a quadratic totally imaginary extension of a totally real field). Then, Schinzel's result extends to $\alpha \in \mathbb{K}^*$ such that $|\alpha| \neq 1$ (in a CM field $|\alpha|_v = 1$ for an archimedean place if and only if $|\alpha|_v = 1$ for any archimedean place). The condition $|\alpha| \neq 1$ can be very restrictive in some applications, but, at least for arbitrary CM field, it is necessary as the following example shows.

Special Numbers

Let $\rho = \frac{\pm\sqrt{14}\pm i\sqrt{2}}{4}$ one of the roots of $2x^4 - 3x^2 + 2$. As we have already remarked, $|\rho| = 1$, thus $\hat{h}(\rho) = \frac{\log 2}{4}$. Let $D \in \mathbb{N}$. Since all the algebraic conjugates of $\rho^{1/D}$ have absolute value 1, the field $\mathbb{Q}(\rho^{1/D})$ is a CM field and we have $\hat{h}(\rho^{1/D}) = \frac{\log 2}{4D}$.

Nevertheless, if $\mathbb{L}$ is not only a CM field but an abelian extension of the rational field, the condition $|\alpha| \neq 1$ can be relaxed assuming only $\alpha \notin \boldsymbol{\mu}$.

Theorem (Abelian Lower Bound, A.-Dvornicich, 2000)

Let $\mathbb{L}/\mathbb{Q}$ be an abelian extension. Then for any $\alpha \in \mathbb{L}^* \backslash \boldsymbol{\mu}$ we have

$$\hat{h}(\alpha) \geq \frac{\log 5}{12} = 0.134\ldots .$$

Height in cyclotomic extension

We remark that, by the Kronecker-Weber theorem, it is enough to prove this lower bound in an cyclotomic field. Is the bound $\hat{h}(\alpha) \geq \frac{\log 5}{12} = 0.134...$ sharp, for $\alpha \notin \boldsymbol{\mu}$ a non zero algebraic number in a cyclotomic field? We shall show that $\frac{\log 5}{12}$ cannot be replaced by any number $> \frac{\log 7}{12} = 0.162....$

Let $m \in \mathbb{N}$, $\zeta_m = \exp(2\pi i/m)$ and let $\mathbb{K}_m = \mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field of degree $\phi(m)$.

We fix $m = 21$ and we recall that $\mathbb{K} = \mathbb{K}_{21}$ (of degree 12 over $\mathbb{Q}$) is one of the twenty-nine cyclotomic fields of class number one. Let us consider how the prime number 7 splits in the ring of integers of $\mathbb{K}$.

Since 7 splits completely in the quadratic imaginary field $\mathbb{Q}(\zeta_3)$ and ramifies in $\mathbb{Q}(\zeta_7)$, we have

Height in cyclotomic extension

$$(7) = P^6 \overline{P}^6 \,,$$

where P is a prime of norm $N_{\mathbb{K}/Q}(P) = 7$. Since $\mathbb{K}$ has class number one, $P = (\gamma)$ for an integer $\gamma \in \mathbb{K}$. Let $\lambda = \overline{\gamma}/\gamma$. Since $\mathbb{K}$ is a CM field, $|\lambda|_v = 1$ for $v \mid \infty$. We have

$$(\lambda) = \overline{P} P^{-1} \,.$$

Thus, if $v \nmid \infty$,

$$|\lambda|_v^{[\mathbb{K}_v:\mathbb{Q}_v]} = \begin{cases} N_{\mathbb{K}/\mathbb{Q}} P = 7, & \text{if } v = P; \\ (N_{\mathbb{K}/\mathbb{Q}} P)^{-1} = 7^{-1}, & \text{if } v = \overline{P}; \\ 1, & \text{otherwise.} \end{cases}$$

We deduce that

$$\hat{h}(\lambda) = \frac{1}{12} \sum_{v \in \mathcal{M}_{\mathbb{K}}} [\mathbb{K}_v : \mathbb{Q}_v] \log^+ |\lambda|_v = \frac{\log 7}{12} \,.$$

Height in cyclotomic extension

As a liminal remark, the minimal polynomial of λ over $\mathbb{Z}$ is $f(x) = 7x^{12} - 13x^6 + 7$. Thus, we can check the computation above of $\hat{h}(\lambda)$ by observing that all the roots of f lie on the unit circle. Whence $M(f) = 7$ and again $\hat{h}(\lambda) = \frac{\log 7}{12}$.

Let $\alpha \in \mathbb{K}_m^* \backslash \boldsymbol{\mu}$, not a root of unity. It seems quite likely that the bound $\hat{h}(\alpha) \geq \frac{\log 7}{12}$ should be the correct bound. For instance, Ishak, Mossinghoff, Pinner and Wiles (2010) show that $\hat{h}(\alpha) < \frac{\log 7}{12}$ implies $35 \mid m$.

They also refine the Abelian Lower Bound, replacing $\frac{\log 5}{12} = 0.134...$ by $0.155...$ (still less than $\frac{\log 7}{12} = 0.162...$).

Exponent of the class group of cyclotomic extensions

We can generalize the construction above of $\lambda \in \mathbb{K}_{21}$ of height $\frac{\log 7}{12}$ to an arbitrary cyclotomic extension $\mathbb{K}_m$. Let $p(m)$ be the smallest prime satisfying $p \equiv 1 \bmod m$. By a celebrated theorem of Linnik, $p(m) \leq m^L$, where $L > 0$ is an effective constant.It is well known that $p(m)$ splits completely in $\mathbb{K}_m$. Choose a prime $P \subset \mathcal{O}_{\mathbb{K}_m}$ over $p(m)$. Let e_m be the exponent of the class group of $\mathbb{K}_m$, *i.e.* the least positive integer e such that $g^e = 1$ for g in the class group. Then $P^{e_m} = (\gamma)$ and $\alpha = \overline{\gamma}/\gamma$ has height

$$\hat{h}(\alpha) = \frac{e_m \log p(m)}{\phi(m)} \leq \frac{e_m L \log m}{\phi(m)} .$$

By A.-Dvornicich lower bound $\hat{h}(\alpha) \geq \frac{\log 5}{12}$, we find

$$e_m \geq \frac{\log 5}{12L} \times \frac{\phi(m)}{\log m} \gg \frac{m}{\log m \log\log m} .$$

Masley-Montgomery revised

Using this principle, we see that a bound of the shape

$$\log p(m) = o(\phi(m))$$

implies that there is only finite cyclotomic fields of class number one.

Question

There exists an "elementary" proof of this result?

We don't know. But, using an explicit version of the Prime Number Theorem in arithmetic progression (McCurley, 1984), we can recover Masley-Montgomery theorem. In 1976 Masley and Montgomery proved that $\mathbb{K}_m$ has class number one if and only if m is one of the following twenty-nine numbers:

Masley-Montgomery revised

$$3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20,$$
$$21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$$

Assume that $\mathbb{K}_m$ has class number 1. We have (McCurley, 1984)

$$\log p(m) \leq 15.08 \log^2 m \quad \text{for} \quad m \geq 10^4 \ .$$

Moreover, by a result of Rosser-Schoenfeld (1961),

$$m/\phi(m) < e^{\gamma} \log\log m + 5/(2 \log\log m) \ .$$

for $m \neq 2 \times 3 \times \cdots \times 23$. We deduce that $m \geq 8 \cdot 10^4$. A direct computation of $p(m)$ for $m < 8 \cdot 10^4$ and refined lower bounds for the height in cyclotomic fields show that m belongs to the previous list of twenty-nine numbers.

Exponent of the class group of CM fields

Let $\mathbb{K}$ be a CM field of degree $D_{\mathbb{K}} = [\mathbb{K} : \mathbb{Q}]$ and exponent of the class group $e_{\mathbb{K}}$. Louboutin and Okazaki (2003) ask if $e_{\mathbb{K}} \to \infty$ as $|\mathrm{disc}(\mathbb{K})| \to +\infty$. Using a generalization of the previous construction and (more involved) lower bounds for the height we prove:

Theorem (A.-Dvornicich, 2003)

Assume GRH. Then for any $\varepsilon > 0$ the exponent $e_{\mathbb{K}}$ of the class group of $\mathbb{K}$ satisfies:

$$e_{\mathbb{K}} \gg_{\varepsilon} \max\left\{ \frac{\log|\mathrm{disc}(\mathbb{K})|}{D_{\mathbb{K}} \log\log|\mathrm{disc}(\mathbb{K})|}, D_{\mathbb{K}}^{1-\varepsilon} \right\} .$$

The quantity on the R.H.S is $\gg (\log|\mathrm{disc}(\mathbb{K})|)^{(1-\varepsilon)/2}$. Thus the theorem gives a (conditional) positive answer to Louboutin-Okazaki's question.

Relative Lower Bound

We can "mix" the Abelian Lower Bound with Dobrowolski's result.

Theorem (Relative Lower Bound, A.-Zannier, 2000)

Let $\mathbb{K}$ be any number field and let $\mathbb{L}/\mathbb{K}$ be an abelian extension. Then for any $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$, we have

$$\hat{h}(\alpha) \geq \frac{c(\mathbb{K})}{D} \left(\frac{\log D}{\log \log 3D} \right)^{-13},$$

where $c(\mathbb{K})$ is a positive constant depending only on $\mathbb{K}$ and where $D = [\mathbb{L}(\alpha) : \mathbb{L}]$.

Taking $\mathbb{L} = \mathbb{Q}$, we recover Dobrowolski's theorem, with a worst exponent on the remainder term. Taking $\mathbb{K} = \mathbb{Q}$ and $\alpha \in \mathbb{L}$ we recover the Abelian Lower Bound, up to a constant.

Absolute Abelian Lower Bound

More recently, the first author and E. Delsinne refine the error term in this inequality and compute a lower bound for $c(\mathbb{K})$. As the proof of the original paper suggested, this lower bound depends on the degree *and* on the discriminant of $\mathbb{K}$.

Let again $\mathbb{L}$ be an abelian extension of a number field $\mathbb{K}$. As a very special case of the result of the Relative Lower Bound, the height in $\mathbb{L}^*\backslash\boldsymbol{\mu}$ is bounded from below by a positive function depending only on $\mathbb{K}$. The following question arises. Is it true that we can choose a function depending only on the degree $[\mathbb{K}:\mathbb{Q}]$? The answer is yes.

Theorem (Absolute Abelian Lower Bound, A.-Zannier, 2010)

Let $\mathbb{K}$ be a number field of degree d over $\mathbb{Q}$ and let $\mathbb{L}/\mathbb{K}$ be an abelian extension. Then, for $\alpha \in \mathbb{L}^*\backslash\boldsymbol{\mu}$,

$$\hat{h}(\alpha) > 3^{-d^2-2d-5}.$$

Remarks on the Absolute Abelian Lower Bound

Let $f(d)$, $g(d)$ be two real functions. In order to simplify the discussion below, we write $f(d) \lll g(d)$ if $f(d) \leq g(d)(\log 3d)^c$ for some $c > 0$. We use the symbol $\ggg$ similarly.

• The Absolute Abelian Lower Bound has some amusing consequences. For instance, let $\mathbb{L}/\mathbb{Q}$ be a dihedral extension of degree, say, $2n$. Then $\mathbb{L}$ is an abelian extension of its quadratic subfield $\mathbb{K}$ fixed by the normal cyclic subgroup of order n. Thus for any $\alpha \in \mathbb{L}^* \backslash \boldsymbol{\mu}$ we have

$$\hat{h}(\alpha) \geq 3^{-13}.$$

Remarks on the Absolute Abelian Lower Bound

• In the special case of *cyclotomic* extensions of a number field $\mathbb{K}$ of degree d, we can deduce the a stronger Absolute Abelian Lower Bound from the Relative Lower Bound.

Remark

Let ζ be a root of unity and let $\alpha \in \mathbb{K}(\zeta)^* \backslash \boldsymbol{\mu}$. Then

$$\hat{h}(\alpha) \gg\gg 1/d \ .$$

Proof. By Galois' Theory, $\mathbb{K}(\zeta)$ is an extension of $\mathbb{Q}(\zeta)$ of degree bounded by d. Since $\mathbb{Q}(\zeta)$ is an abelian extension of $\mathbb{Q}$, by the Relative Lower Bound we have:

$$\hat{h}(\alpha) \gg\gg 1/d \ .$$

□

A (false) Conjecture

• A natural generalization of both Lehmer's conjecture and of the Abelian Lower Bound could be the following. Let $\mathbb{K}$ be a number field of degree d over $\mathbb{Q}$ and let $\mathbb{L}/\mathbb{K}$ be an abelian extension. Then, for $\alpha \in \mathbb{L}^* \backslash \boldsymbol{\mu}$,

$$\hat{h}(\alpha) > \frac{c}{d}$$

for some absolute constant $c > 0$. Unfortunately, this statement is false. Let x be a sufficiently large positive real number. Let m be the product of all primes up to x and let $d = \phi(m)$. By elementary analytic number theory $m \geq c_1 d \log\log d$. Let $\mathbb{K} = \mathbb{Q}(\zeta_m)$ (of degree d over $\mathbb{Q}$) and let $\alpha = 2^{1/m}$. Define $\mathbb{L} = \mathbb{K}(\alpha)$. Then $\mathbb{L}/\mathbb{K}$ is cyclic, $\alpha \in \mathbb{L}^* \backslash \boldsymbol{\mu}$ and

$$\hat{h}(\alpha) = \frac{\log 2}{m} \leq \frac{\log 2}{c_1 d \log\log d} .$$

Thus we cannot have $\hat{h}(\alpha) > c/d$ for any absolute constant $c > 0$.

Abelian Kummer's extensions

• The previous example cannot be substantially improved by "taking roots" in a fixed field $\mathbb{K}$.

Remark

Let $\mathbb{K}$ be a number field of degree d. Let $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$ such that $\alpha^n \in \mathbb{K}$ for some positive integer n. Then, if $\mathbb{K}(\alpha)/\mathbb{K}$ is abelian,

$$\hat{h}(\alpha) \gg\gg 1/d \ .$$

Proof. Let $m \in \mathbb{N}$. We denote by $\boldsymbol{\mu}_m$ the group of m-th roots of unity.

Abelian Kummer's extensions

Let r be the number of n-roots of unity contained in $\mathbb{K}$. Thus $\boldsymbol{\mu}_n \cap \mathbb{K}^* = \boldsymbol{\mu}_r$. Since $\mathbb{K}(\alpha)/\mathbb{K}$ is abelian, the extension $\mathbb{K}(\alpha, \zeta_n)/\mathbb{K}$ is also abelian. By a theorem of Schinzel, there exists $\gamma \in \mathbb{K}$ such that

$$\alpha^{nr} = \gamma^n \ .$$

Let $\delta = [\mathbb{K} : \mathbb{Q}(\zeta_r)] = d/\varphi(r)$. Since $\mathbb{Q}(\zeta_r)/\mathbb{Q}$ is abelian, by the Relative Lower Bound we have:

$$\hat{h}(\gamma) \gg\gg 1/\delta \ .$$

By elementary analytic number theory, $r \lll \varphi(r)$. Thus

$$\hat{h}(\alpha) = \frac{\hat{h}(\gamma)}{r} \gg\gg 1/d \ .$$

□

Abelian Kummer's extensions

The remarks above suggest the following conjecture:

Conjecture

Let $\mathbb{K}$ be a number field of degree d. Let $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$ such that $\mathbb{K}(\alpha)/\mathbb{K}$ is an abelian extension. Then

$$\hat{h}(\alpha) \gg\gg 1/d \ .$$

Caught Algebraic Beetles

- $\theta = 1.324...$, the positive root of $x^3 - x - 1$. It is the smallest Pisot's number. $\hat{h}(\theta) = \frac{1}{3}\log\theta$.
- $\rho = \frac{\pm\sqrt{14}\pm i\sqrt{2}}{4}$ one of the roots of $2x^4 - 3x^2 + 2$. Then $\mathbb{Q}(\rho)$ is a CM field. For all $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ of degree 2 or 4 such that $\mathbb{Q}(\alpha)$ is CM, we have $\hat{h}(\alpha) \geq \hat{h}(\rho) = \frac{\log 2}{4} = 0.173....$
- $\tau = 1.176...$ the positive root of Lehmer's polynomial $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$. Conjecturally, the smallest Salem number. Conjecturally, $M(f) \geq \tau$ for all integral irreducible polynomials $f \neq \pm 1, \pm x$.
- φ, the golden ratio $\frac{1+\sqrt{5}}{2}$. For all α of absolute value $\neq 1$ such that $\mathbb{Q}(\alpha)$ is a CM field, we have $\hat{h}(\alpha) \geq \hat{h}(\varphi) = 0.240....$
- λ, one of the roots of $7x^{12} - 13x^6 + 7$. Then $\mathbb{Q}(\lambda) = \mathbb{K}(\zeta_{21})$. Conjecturally, for all non-zero $\alpha \notin \boldsymbol{\mu}$ such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is abelian, we have $\hat{h}(\alpha) \geq \hat{h}(\lambda) = \frac{\log 7}{12} = 0.162....$

The Main Principle

Let α be a non-zero *integer*, $\alpha \neq \pm 1$. We look for a lower bound for $\hat{h}(\alpha)$. Of course, $\hat{h}(\alpha) = \log|\alpha| \geq \log 2 = 0.693....$ Forget this inequality and let p be a prime number. Then, by Fermat's Little Theorem (FℓT in the sequel)

$$\alpha^p \equiv \alpha \bmod p \, .$$

Moreover $\gamma = \alpha^p - \alpha \neq 0$, since $\alpha \neq \pm 1$. Applying the Product Formula to γ we get

$$1 = |\gamma| \cdot \prod_{\ell \text{ prime}} |\gamma|_\ell \leq p^{-1}|\alpha^p - \alpha| \leq \frac{2}{p}|\alpha|^p \, .$$

Thus

$$\hat{h}(\alpha) \geq \frac{\log(p/2)}{p} \, .$$

Choosing $p = 5$ we obtain $\hat{h}(\alpha) \geq 0.183....$ This principle underlies the proofs of all the previous lower bounds for the height.

Denominators

We shall deduce some metric properties from generalizations of the Main Principle. To do that, we need "good local denominators". We make use of the following lemma:

Lemma (Strong Approximation)

Let $\mathbb{E}$ be a number field and let Σ be a finite set of non-archimedean place of $\mathbb{E}$. Then, for any $\alpha_1, \ldots, \alpha_n \in \mathbb{E}$ there exists $\beta \in \mathcal{O}_{\mathbb{E}}$ such that $\beta\alpha_j$ is an algebraic integer for $j = 1, \ldots, n$ and

$$|\beta|_v = \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}^{-1}$$

for $v \in \Sigma$.

Proof. It is an easy corollary of the Strong Approximation Theorem, Cassels-Frölich op. cit., chapter II, 15, p.67. □

Sketch of the proof of the Abelian Lower Bound

We shall sketch a proof of a somewhat weaker result.

Theorem

Let $m \in \mathbb{N}$, $m \not\equiv 2 \bmod 4$. Consider the m-th cyclotomic field $\mathbb{K}_m = \mathbb{Q}(\zeta_m)$. Then for any $\alpha \in \mathbb{K}_m^* \backslash \boldsymbol{\mu}$ we have

$$\hat{h}(\alpha) \geq \frac{\log(2.5)}{10} = 0.039\ldots .$$

Proof. Since Weil's height is invariant by multiplication by roots of unities, we may assume that

$$\forall \zeta \in \boldsymbol{\mu},\ \forall n < m, \quad \zeta\alpha \notin \mathbb{K}_n\ . \tag{1}$$

Let $p \geq 3$ be a prime number. We show that $2p\hat{h}(\alpha) \geq \log(p/2)$. Choosing $p = 5$ we obtain the announced result.

Non-ramified primes

Assume first that $p \nmid m$. Let $\sigma \in \mathrm{Gal}(\mathbb{K}_m/\mathbb{Q})$ be the Frobenius automorphism, $\sigma\zeta_m = \zeta_m^p$. For any integer $\gamma \in \mathbb{K}_m$ we have $\gamma = f(\zeta_m)$ for some $f \in \mathbb{Z}[x]$. Hence

$$\gamma^p \equiv f(\zeta_m^p) \equiv f(\sigma\zeta_m) \equiv \sigma\gamma \,(\mathrm{mod}\, p).$$

Let fix a $v \in \mathcal{M}_{\mathbb{K}_m}$ dividing p. Thus $|\gamma^p - \sigma\gamma|_v \leq 1/p$ for any integer $\gamma \in \mathbb{K}_m$.

By the Strong Approximation Lemma, there exists an algebraic integer $\beta = \beta_v \in \mathbb{K}_m$ such that $\alpha\beta$ is integer and $|\beta|_v = \max\{1, |\alpha|_v\}^{-1}$. Thus

$$\begin{aligned} |\alpha^p - \sigma\alpha|_v &= |\beta|_v^{-p} |(\alpha\beta)^p - \sigma(\alpha\beta) + (\sigma\beta - \beta^p)\sigma\alpha|_v \\ &\leq |\beta|_v^{-p} \max\left(|(\alpha\beta)^p - \sigma(\alpha\beta)|_v, |\beta^p - \sigma\beta|_v |\sigma\alpha|_v\right) \\ &\leq p^{-1} \max(1, |\alpha|_v)^p \max(1, |\sigma\alpha|_v). \end{aligned}$$

Non-ramified primes

Combining this upper bound with trivial estimates for $v \nmid p$ we get

$$|\alpha^p - \sigma\alpha|_v \leq c(v) \max(1, |\alpha|_v)^p \max(1, |\sigma\alpha|_v)$$

where

$$c(v) = \begin{cases} p^{-1} & \text{if } v \mid p \\ 1 & \text{if } v \nmid p \text{ and } v \nmid \infty \\ 2 & \text{if } v \mid \infty \ . \end{cases}$$

Moreover $\alpha^p \neq \sigma\alpha$, since α is not a root of unity. Indeed, let $a \neq b$ be natural numbers such that α^a is a conjugate of α^b.Then $a\hat{h}(\alpha) = b\hat{h}(\alpha)$ which implies $\hat{h}(\alpha) = 0$.

Applying the Product Formula to $\alpha^p - \sigma\alpha$ we get

$$0 \leq p\hat{h}(\alpha) + \hat{h}(\sigma\alpha) - \log p + \log 2 \leq 2p\hat{h}(\alpha) - \log(p/2) \ .$$

Ramified primes

Assume now that $p|m$. Let σ be a generator of $\mathrm{Gal}(\mathbb{K}_m/\mathbb{K}_{m/p})$. Thus, for any integer $\gamma = f(\zeta_m) \in \mathbb{Z}[\zeta_m]$

$$\gamma^p \equiv f(\zeta_m^p) \equiv f(\sigma\zeta_m^p) \equiv \sigma\gamma^p \,(\mathrm{mod}\, p)$$

i.e. $|\gamma^p - \sigma\gamma^p|_v \leq 1/p$ for any $v \in \mathcal{M}_{\mathbb{K}}$ dividing p. Using the Strong Approximation Lemma as in the first part of the proof, we get

$$|\alpha^p - \sigma\alpha^p|_v \leq c(v)\max(1, |\alpha|_v)^p \max(1, |\sigma\alpha|_v)^p$$

Suppose that $\sigma\alpha^p = \alpha^p$. Since σ fix $\mathbb{K}_{m/p}$ we have $\sigma\zeta_m = \eta\zeta_m$ for a primitive p-root of unity η. Then $\sigma\alpha = \eta^u\alpha$ for some integer u. It follows that $\sigma(\alpha/\zeta_m^u) = \alpha/\zeta_m^u$, hence $\alpha/\zeta_m^u \in \mathbb{K}_{m/p} \subsetneq \mathbb{K}_m$, which contradicts the minimality of n (cf. (1)). Applying the Product Formula to $\alpha^p - \sigma\alpha^p \neq 0$, we obtain again

$$0 \leq p\hat{h}(\alpha) + p\hat{h}(\sigma\alpha) - \log p + \log 2 = 2p\hat{h}(\alpha) - \log(p/2).$$

□

Second lecture:

- Sketch of the proof of Dobrowolski's Theorem
- Sketch of the proof of the Relative Lower Bound (first part)

Sketch of the proof of Dobrowolski's Theorem

We reformulate the main result of Dobrowolski in an equivalent form, replacing $(\log D/\log\log D)^{-3}$ by the decreasing function $f(D) = \left(\log(16D)/\log\log(16D)\right)^{-3}$.

Theorem

For any $\alpha \in \overline{\mathbb{Q}}^* \setminus \boldsymbol{\mu}$ of degree D we have

$$\hat{h}(\alpha) \geq \frac{c}{D}\left(\frac{\log 16D}{\log\log 16D}\right)^{-3}$$

for some absolute constant $c > 0$.

Proof. We can assume that α is an algebraic integer, since otherwise $\hat{h}(\alpha) \geq (\log 2)/D$.

Rausch's reduction.

Moreover, it is enough to prove this theorem under the additional assumption $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] = D$ for all natural n, as we now show.

We follow an argument of Rausch (1985). Assume that for some $n > 1$ we have $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] < D$. Then $r = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^n)] > 1$. Let β be the norm of α from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\alpha^n)$. Then $\beta = \zeta\alpha^r$ for some root of unity ζ and $\hat{h}(\beta) = \hat{h}(\alpha^r) = r\hat{h}(\alpha)$. Since $D' = [\mathbb{Q}(\beta) : \mathbb{Q}] < D$, by induction we have $D'\hat{h}(\beta) \geq cf(D')$. Since $f(D) = \big(\log(16D)/\log\log(16D)\big)^{-3}$ is a decreasing function, we deduce that

$$D\hat{h}(\alpha) = [\mathbb{Q}(\alpha^n) : \mathbb{Q}]\hat{h}(\beta) \geq D'\hat{h}(\beta) \geq cf(D') \geq cf(D).$$

Thus, from now on we assume

$$\forall n \in \mathbb{N}, \quad [\mathbb{Q}(\alpha^n) : \mathbb{Q}] = D\ .$$

Congruences

Let f be the minimal polynomial of α over $\mathbb{Z}$ and let p be a prime number. Then, by FℓT

$$f(x)^p \equiv f(x^p) \bmod p\mathbb{Z}[x].$$

Thus

$$|f(\alpha^p)|_v \leq p^{-1}$$

for any $v \mid p$. Let $F \in \mathbb{Z}[x]$ be a non-zero polynomial of degree $\leq L$ vanishing on α with multiplicity $\geq T$ for some *parameters* L and T with $L \geq DT$. Then

$$|F(\alpha^p)|_v \leq p^{-T}$$

for any $v \mid p$. Moreover $|F(\alpha^p)|_v \leq 1$ for $v \nmid \infty$ and

$$|F(\alpha^p)|_v \leq \|F\|_1 \max(1, |\alpha|_v)^{pL}$$

if $v \mid \infty$, where $\|F\|_1$ denotes the sum of the absolute values of the coefficients of F.

Sketch of the proof of Dobrowolki's Theorem

Assume

$$F(\alpha^p) \neq 0.$$

Then, by the Product Formula,

$$0 \leq -T \log p + \log \|F\|_1 + pL\hat{h}(\alpha) \, . \tag{2}$$

This gives

$$\hat{h}(\alpha) \geq \frac{T \log p - \log \|F\|_1}{pL}.$$

We choose $L = D$, $T = 1$ and $F = f$. The non vanishing condition $F(\alpha^p) \neq 0$ is satisfied. Indeed, if α is not a root of unity, then α^p is not a conjugate of α, as we have already remarked. Thus we get

$$\hat{h}(\alpha) \geq \frac{\log p - \log \|f\|_1}{pD} \, .$$

Siegel's Lemma

Unfortunately, $\log \|f\|_1$ can be as large as a power of D, even if the height of α is very small. Thus, to get a positive lower bound, we must choose p exponential in D^c and the argument ends with a poor lower bound of the shape $\hat{h}(\alpha) \geq \exp(-D^c)$.

The use of Siegel's Lemma, a classical tool in diophantine approximation, enormously improves the quality of this bound. Using this lemma we find a non-zero polynomial $F \in \mathbb{Z}[x]$ of degree $\leq L$ vanishing on α with multiplicity $\geq T$ as required and such that

$$\log \|F\|_\infty \leq \frac{DT}{L+1-DT}(T \log(L+1) + L\hat{h}(\alpha)). \qquad (3)$$

Here $\|F\|_\infty$ denotes the maximum of the absolute values of the coefficients of F.

Conventions

The proof now follows the scheme of a classical transcendence proof:

- Auxiliary Function
- Extrapolation
- Zero's Lemma.

During the proof we assume that the height of α is pathologically small and at the end we get a contradiction. We use in a non standard way the symbols $\approx$, $\ll$ and $\gg$. We write $A \approx B$ if and only if $c_1 B < A < c_2 B$ with c_1, $c_2 > 0$. The constants c_1,c_2 are eventually assumed to be sufficiently large (or small) in such a way that the forthcoming assumptions are verified. Similarly, $A \ll B$ (or $B \gg A$) if and only if $A \leq cB$ where $c > 0$ has the same meaning as before.

Auxiliary Function

Since $\|F\|_1 \leq (L+1)\|F\|_\infty$, the bound (15) of Siegel's Lemma gives

$$\log \|F\|_1 \leq \log(L+1) + \frac{DT}{L+1-DT}(T\log(L+1) + L\hat{h}(\alpha)) \, .$$

This inequality cannot give anything better than

$$\log \|F\|_1 \ll \log(L+1) \, .$$

Therefore, it is reasonable to choose L and T in such a way that

$$\frac{DT^2}{L+1-DT} \approx 1 \, ,$$

say $L = DT^2$, and to assume $L\hat{h}(\alpha) \leq T\log(L+1)$. This implies $\log(L+1) \approx \log D$ (at least if $\log T \ll \log D$). In this setting, $\log \|F\|_1 \ll \log D$ under the assumption $D\hat{h}(\alpha) \ll (\log D)/T$.

Extrapolation

We fix a third parameter N with $\log N \ll \log\log D$. We assume $p \in [N/2, N]$. We want to show that $F(\alpha^p) = 0$. Assume the contrary. Then, by the Product Formula (2),

$$0 \ll -T\log\log D + \log D + NT^2 D\hat{h}(\alpha)\ . \tag{4}$$

Fix $T \approx \log D/\log\log D$ and assume $NT^2 D\hat{h}(\alpha) \leq \log D$, *i.e.*

$$T \approx \frac{\log D}{\log\log D}, \quad \text{and} \quad D\hat{h}(\alpha) \ll \frac{(\log\log D)^2}{N\log D}\ .$$

Note the upper bound for $D\hat{h}(\alpha)$ implies the previous assumption $D\hat{h}(\alpha) \ll \log D/T \approx \log\log D$. Then (4) cannot hold. This forces F to vanishes on α^p for all $p \in [N/2, N]$. Since $F \in \mathbb{Z}[x]$, it must vanishes on the algebraic conjugates of α^p, too.

Zero's Lemma and conclusion

Since α is not a root of unity, α^{p_1} and α^{p_2} are not conjugates for primes $p_1 \neq p_2$. Then the set Σ of the conjugates of α^p ($p \in [N/2, N]$) satisfies (recall that $\forall p$, $[\mathbb{Q}(\alpha^p) : \mathbb{Q}] = D$)

$$\#\Sigma = \sum_{N/2 \leq p \leq N} D \gg \frac{DN}{\log N}$$

by the Prime Number Theorem. Since the number of zeros of F cannot exceed its degree,

$$\frac{DN}{\log N} \ll \#\Sigma \leq \deg(F) \leq L\,.$$

We choose $\frac{DN}{\log N} \approx L$, *i.e.* $N \approx \frac{(\log D)^2}{\log\log D}$. We get a contradiction which shows that

$$D\hat{h}(\alpha) \gg \frac{\log\log D}{N \log D} \gg \left(\frac{\log D}{\log\log D}\right)^{-3}\,.$$

Sketch of the proof of the Relative Lower Bound

We shall give a sketch of:

Theorem (Relative Lower Bound)

Let $\mathbb{K}$ be a number field and let $\mathbb{L}/\mathbb{K}$ be abelian. Then for $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$, we have

$$\hat{h}(\alpha) \geq \frac{C(\mathbb{K})}{D} \left(\frac{\log(2D)}{\log\log(5D)} \right)^{-7},$$

where $D = [\mathbb{L}(\alpha) : \mathbb{L}]$ and $C(\mathbb{K}) > 0$.

We follow the proof of A.-Delsinne 2007. This proof simplifies the diophantine step and improves the exponent on the remainder term.

Setting

We fix the algebraic closure $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. For any prime p, we fix an algebraic closure $\overline{\mathbb{Q}_p}$. Given a number field $\mathbb{E}$ and $v \in \mathcal{M}_{\mathbb{E}}$, $v \nmid \infty$, we view $\mathbb{E} \subseteq \overline{\mathbb{Q}}$ and $\mathbb{E}_v \subseteq \overline{\mathbb{Q}_p}$. Let $\mathbb{L}/\mathbb{K}$ be abelian and $P \subset O_{\mathbb{K}}$ be prime. We denote by p the rational prime under P. We let $\mathcal{P}$ be the set of primes $P \subset O_{\mathbb{K}}$ such that $e(P|p) = f(P|p) = 1$. Let $P \in \mathcal{P}$ and $Q \subset \mathcal{O}_{\mathbb{L}}$ over P.

- Since $\mathbb{L}/\mathbb{K}$ is Galois, the completion $\mathbb{L}_P$ of $\mathbb{L}$ at Q and the ramification index $e_P(\mathbb{L}) = e(Q|P)$ depend only on P.
- Since $P \in \mathcal{P}$, we have $\mathbb{K}_P = \mathbb{Q}_p$.

Thus $\mathbb{L}_P/\mathbb{Q}_p$ is abelian. By Kronecker-Weber, $\mathbb{L}_P \subseteq \mathbb{Q}_p(\zeta_m)$ for some $m \in \mathbb{N}$, $m \not\equiv 2 \bmod 4$. We take $m = m_P(\mathbb{L})$ to be minimal with this property and we define $q_P(\mathbb{L})$ as the maximal power of p dividing m , *i.e.* $m = q_P(\mathbb{L}) \cdot n$, $p \nmid n$. Then P ramifies in $\mathbb{L}$ iff $p|m$. Thus $q_P(\mathbb{L}) = 1$ for all but finitely many $P \in \mathcal{P}$. Define $q(\mathbb{L}) = \sum_{P \in \mathcal{P}} (q_P(\mathbb{L}) - 1)$ and remark that for $\mathbb{L}' \subseteq \mathbb{L}$ abelian extensions of $\mathbb{K}$ we have $q(\mathbb{L}') \leq q(\mathbb{L})$.

Reduction

• **Choose of α.** We choose $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ which contradicts the Relative Lower Bound and such that

$$D = [\mathbb{L}(\alpha) : \mathbb{L}] \text{ is minimal,} \tag{5}$$

i.e. any $\beta \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ of degree $D' < D$ over an abelian extension of $\mathbb{K}$ satisfy the Relative Lower Bound. Then, since the function $t \mapsto t \log(2t)^7 / \log\log(5t)^7$ increases,

$$\forall \zeta \in \boldsymbol{\mu}, \quad \forall \mathbb{L}'/\mathbb{K} \text{ abelian}, \quad [\mathbb{L}'(\zeta\alpha) : \mathbb{L}'] \geq D \ .$$

• **Choose of $\mathbb{L}$.** We choose $\mathbb{L}$ such that

$$q(\mathbb{L}) = \min\{q(\mathbb{L}') \text{ such that } \mathbb{L}'/\mathbb{K} \text{ abelian and } \exists \zeta \in \boldsymbol{\mu},\ [\mathbb{L}'(\zeta\alpha) : \mathbb{L}]' = D\} \ . \tag{6}$$

Since $\mathbb{L} \mapsto q(\mathbb{L})$ increases on the abelian extensions $\mathbb{L}/K$, we can replace $\mathbb{L}$ by $\mathbb{L} \cap \mathbb{K}(\alpha)$ and assume

$$\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\alpha) \quad (i.e.\ \mathbb{K}(\alpha) = \mathbb{L}(\alpha)) \ . \tag{7}$$

Setting (again)

For the same reason, we can also assume $[\mathbb{L} : \mathbb{K}]$ minimal. This implies

$$\forall \zeta \in \boldsymbol{\mu},\ \mathbb{K}(\zeta\alpha) \subseteq \mathbb{K}(\alpha) \Rightarrow \mathbb{K}(\zeta\alpha) = \mathbb{K}(\alpha)\ . \tag{8}$$

Indeed, if $\mathbb{K}(\zeta\alpha) \subsetneq \mathbb{K}(\alpha)$, then $\mathbb{L}_0 = \mathbb{L} \cap \mathbb{K}(\zeta\alpha)$ is abelian over $\mathbb{K}$, $[\mathbb{K}(\zeta\alpha) : \mathbb{L}_0] = D$ and $[\mathbb{L}_0 : \mathbb{K}] < [\mathbb{L} : \mathbb{K}]$.

From now on we fix an algebraic number α which does not satisfy the Relative Lower Bound and an abelian extension $\mathbb{L}/\mathbb{K}$ which satisfies conditions (5), (6), (7) and (8). We put $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ and $e_P = e_P(\mathbb{L})$ for $P \in \mathcal{P}$.

We identify G with the set of morphisms $\mathbb{L} \to \overline{\mathbb{Q}} \subset \mathbb{C}$ which let $\mathbb{K}$ be fixed. Given a subset $S \subseteq G$ we denote by $\overline{S}$ the set of $\tau : \mathbb{L}(\alpha) \to \overline{\mathbb{Q}}$ such that $\tau_{|\mathbb{L}}$ is in S. Thus $|\overline{S}| = D|S|$.

We denote by $\mathbb{E}$ a number filed containing the normal closure of $\mathbb{L}(\alpha)/\mathbb{K}$. We work with valuation $v \in \mathcal{M}_{\mathbb{E}}$.

Rausch's reduction

Rausch's reduction shows that

$$\forall n \in \mathbb{N}, \quad \mathbb{L}(\alpha^n) = \mathbb{L}(\alpha)\ . \tag{9}$$

Moreover, for any prime p

$$[\mathbb{K}(\alpha) : \mathbb{K}(\alpha^p)] = 1 \text{ or } p\ . \tag{10}$$

Indeed, assume $r = [\mathbb{K}(\alpha) : \mathbb{K}(\alpha^p)] \in (1, p)$. Arguing as usual, we find a p-th root ζ such that $\zeta\alpha^r \in \mathbb{K}(\alpha^p)$. By Bézout's identity, there exist λ, $\mu \in \mathbb{Z}$ such that $\lambda p + \mu r = 1$. Hence

$$\zeta^\mu \alpha = \alpha^{\lambda p} \cdot \left(\zeta\alpha^r\right)^\mu \in \mathbb{K}(\alpha^p) \subsetneq \mathbb{K}(\alpha).$$

This contradicts (8).

Congruences

Let $P \in \mathcal{P}$ and let $Q \subset \mathcal{O}_{\mathbb{L}}$ over P. Since $\mathbb{L}/\mathbb{K}$ is abelian the Frobenius automorphism $\phi_P = \phi(Q|P)$ depends only on P. We have

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}}, \quad \forall Q \subset \mathcal{O}_{\mathbb{L}} \text{ over P }, \quad \gamma^p \equiv \phi_P \gamma \bmod Q \, . \tag{11}$$

We prove a second congruence, useful for large ramification index.

$\exists H_P < G$ of cardinality $\min\{e_P, p\}$ such that

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}}, \quad \forall \sigma \in H_P, \quad \gamma^p \equiv \sigma \gamma^p \bmod P\mathcal{O}_{\mathbb{L}} \, . \tag{12}$$

Proof. We recall that:

- $m = m_P(\mathbb{L})$ is the smallest $m \in \mathbb{N}$ s.t. $\mathbb{L}_P \subseteq \mathbb{Q}_p(\zeta_m)$;
- $q = q_P(\mathbb{L})$ satisfies $m = q \cdot n$, $p \nmid n$;
- P ramifies in $\mathbb{L}$ iff $p|m$ iff $p|q$.

Congruences: large ramification index

If P does not ramify in $\mathbb{L}$ the lemma is trivial ($e_P = 1$, take $H_P = \{\mathrm{Id}\}$). Assume $p|q$ and let $\Sigma_p = \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p}))$. Then Σ_p is cyclic of order p or $p-1$ depending on whether $p^2|q$ (wild ramification) or not (time ramification). By the minimality of m, Σ_p does not fix $\mathbb{L}_P$, and hence induces by restriction a nontrivial group

$$H_P^* = \mathrm{Gal}(\mathbb{L}_P/\mathbb{L}_P \cap \mathbb{Q}_p(\zeta_{m/p})) \, .$$

By ramification theory, $|H_P^*| = e_P$ if $p^2 \nmid q$ and $|H_P^*| = p$ if $p^2|q$. Since $\mathbb{L}/\mathbb{K}$ is abelian, the decomposition group D_P of a prime of $\mathcal{O}_\mathbb{L}$ over P depends only on P. We have $\mathrm{Gal}(\mathbb{L}_P/\mathbb{K}_P) \cong D_P$. We define H_P as the isomorphic image of H_P^* in $D_P < G$.

By the previous arguments we have:

$$\begin{cases} |H_P| = e_P \text{ divide } |\Sigma_P| = p-1, & \text{if } p^2 \nmid q \\ |H_P| = |\Sigma_p| = p, & \text{if } p^2|q \, . \end{cases} \tag{13}$$

Congruences: large ramification index

We must prove that

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}}, \quad \forall \sigma \in H_P, \quad \gamma^p \equiv \sigma\gamma^p \bmod P\mathcal{O}_{\mathbb{L}} \ .$$

It is enough to verify $\gamma^p \equiv \sigma\gamma^p \pmod{P\mathcal{O}}$ for $\gamma \in \mathcal{O}$ and $\sigma \in \Sigma_p$, where $\mathcal{O} = \mathbb{Z}_p[\zeta_m]$ is the ring of integers of $\mathbb{Q}_p(\zeta_m)$. To prove this last congruence, write $\gamma = f(\zeta_m)$, where $f \in \mathbb{Z}_p[x]$. Let $\sigma \in H_P$; since σ fixes $\mathbb{Q}_p(\zeta_{m/p})$ we have $\sigma\zeta_m^p = \zeta_m^p$. Combining these facts with FℓT , we find

$$\sigma\gamma^p = \sigma f(\zeta_m)^p \equiv \sigma f(\zeta_m^p) = f(\zeta_m^p) \equiv \gamma^p \pmod{P\mathcal{O}} \ .$$

□

We now prove that:

$$\forall \tau \in \overline{H_P} \text{ such that } \tau_{|\mathbb{L}} \neq \mathrm{Id}, \quad \tau\alpha^p \neq \alpha^p \ . \tag{14}$$

Non triviality of H_P on α^p

Proof. Let $\sigma \in H_P \backslash \mathrm{Id}$ and let τ extending σ to $\mathbb{L}(\alpha)$. Thus $\mathbb{L}_0 = \mathbb{L}^{<\sigma>} \subsetneq \mathbb{L}$. Assume $\tau\alpha^p = \alpha^p$. Thus the minimal polynomial of α^p over $\mathbb{L}$ has coefficients in $\mathbb{L}_0$. We have:

- $\mathbb{L}(\alpha^p) = \mathbb{L}(\alpha) = \mathbb{L}_0(\alpha) = \mathbb{K}(\alpha)$ (use (7) and (9)).
- $[\mathbb{L}_0(\alpha^p) : \mathbb{L}_0] = [\mathbb{L}(\alpha^p) : \mathbb{L}] = [\mathbb{L}(\alpha) : \mathbb{L}] = D$.
- $[\mathbb{L}(\alpha) : \mathbb{L}_0(\alpha^p)] > 1$ (use $\mathbb{L}_0 \subsetneq \mathbb{L}$).
- $[\mathbb{K}(\alpha) : \mathbb{K}(\alpha^p)] = p$ (otherwise $\mathbb{K}(\alpha^p) = \mathbb{K}(\alpha) = \mathbb{L}(\alpha)$ by (10), and τ would fix $\mathbb{K}(\alpha) = \mathbb{L}(\alpha)$ and a fortiori $\mathbb{L}$).

These facts imply (make a diagram!)

$$[\mathbb{L} : \mathbb{L}_0] = [\mathbb{L}(\alpha) : \mathbb{L}_0(\alpha^p)] = p \, .$$

Therefore, by (13),

$$|\Sigma_p| = p \, .$$

Non triviality of H_P on α^p

Let as before $Q \subset \mathcal{O}_{\mathbb{L}}$, $Q|P$. Since $\mathbb{L}_P(\zeta_q) \subseteq \mathbb{Q}_p(\zeta_m)$, the group Σ_p induces by restriction a nontrivial subgroup of $\mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{K})$, which is necessarily cyclic of order p, generated by some ρ. Let $\mathbb{L}' = \mathbb{L}(\zeta_q)^{<\rho>} \supseteq \mathbb{L}_0$. Then $\rho\zeta_q = \eta\zeta_q$ for some primitive p-th root of unity η (recall that $p \nmid n$).

We claim that there exists an integer u such that $\zeta_q^{-u}\alpha \in \mathbb{L}'(\alpha^p)$. By Galois' theory, $[\mathbb{L}(\zeta_q, \alpha) : \mathbb{L}'(\alpha^p)] \mid p$. If $\alpha \in \mathbb{L}'(\alpha^p)$ the claim is trivial. If $\alpha \notin \mathbb{L}'(\alpha^p)$ we have $[\mathbb{L}(\zeta_q, \alpha) : \mathbb{L}'(\alpha^p)] = p$ and the restriction $\mathrm{Gal}(\mathbb{L}(\zeta_q, \alpha)/\mathbb{L}'(\alpha^p)) \to \mathrm{Gal}(\mathbb{L}(\zeta_q)/\mathbb{L}')$ is a group isomorphism. Let $\mathrm{Gal}(\mathbb{L}(\zeta_q, \alpha)/\mathbb{L}'(\alpha^p)) =< \tilde{\rho} >$. Then,

$$\tilde{\rho}\zeta_q = \eta\zeta_q \quad \text{and} \quad \tilde{\rho}\alpha = \eta^u\alpha$$

for some $u \in \mathbb{N}$. Hence $\zeta_q^{-u}\alpha$ is left fixed by $\tilde{\rho}$ and so belongs to $\mathbb{L}'(\alpha^p)$, as claimed.

Non triviality of H_P on α^p

Thus

$$[\mathbb{L}'(\zeta_q^{-u}\alpha) : \mathbb{L}'] \leq [\mathbb{L}'(\alpha^p) : \mathbb{L}'] \leq [\mathbb{L}_0(\alpha^p) : \mathbb{L}_0] = D.$$

Since $\mathbb{L}'_P \subseteq \mathbb{Q}_p(\zeta_{m/p})$ and $\mathbb{L}' \subseteq \mathbb{L}(\zeta_q)$, we also have

$$q_P(\mathbb{L}') \leq q/p < q = q_P(\mathbb{L})$$

and

$$q_\ell(\mathbb{L}') \leq q_\ell(\mathbb{L}(\zeta_q)) = q_\ell(\mathbb{L}), \quad \text{for} \quad \ell \in \mathcal{P},\ \ell \neq P\ .$$

Therefore

$$[\mathbb{L}'(\zeta_q^{-u}\alpha) : \mathbb{L}'] \leq D \quad \text{and} \quad q(\mathbb{L}') < q(\mathbb{L}) = q,$$

which contradicts the minimal property (6). This conclude the proof of (14).

□

Third lecture:

- Sketch of the proof of the Relative Lower Bound (second part)
- Sketch of the proof of the Absolute Abelian Lower Bound (first part)

Setting

- $\mathbb{L}/\mathbb{K}$ abelian
- $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ such that $\mathbb{L} \subseteq \mathbb{K}(\alpha)$
- $D = [\mathbb{L}(\alpha) : \mathbb{L}]$. We can assume: $\forall n$, $[\mathbb{L}(\alpha^n) : \mathbb{L}] = D$.
- $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$
- $e_P = e_P(\mathbb{L})$ for $P \in \mathcal{P}$ the set of $P \subset O_{\mathbb{K}}$ such that $e(P|p) = f(P|p) = 1$.

We identify G with the set of morphisms $\mathbb{L} \to \overline{\mathbb{Q}} \subset \mathbb{C}$ which let $\mathbb{K}$ be fixed. Given a subset $S \subseteq G$ we denote by $\overline{S}$ the set of $\tau : \mathbb{L}(\alpha) \to \overline{\mathbb{Q}}$ such that $\tau_{|\mathbb{L}}$ is in S. Thus $|\overline{S}| = D|S|$.

We denote by $\mathbb{E}$ a number filed containing the normal closure of $\mathbb{L}(\alpha)/\mathbb{K}$. We work with valuation $v \in \mathcal{M}_{\mathbb{E}}$.

Congruence

Let $P \in \mathcal{P}$ and let $Q \subset \mathcal{O}_{\mathbb{L}}$ over P. Since $\mathbb{L}/\mathbb{K}$ is abelian the Frobenius automorphism $\phi_P = \phi(Q|P)$ depends only on P. We have

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}}, \quad \forall Q \subset \mathcal{O}_{\mathbb{L}} \text{ over P }, \quad \gamma^p \equiv \phi_P \gamma \bmod Q \ . \tag{11}$$

We have a second congruence, useful for large ramification index. $\exists H_P < G$ of cardinality $\min\{e_P, p\}$ such that

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}}, \quad \forall \sigma \in H_P, \quad \gamma^p \equiv \sigma \gamma^p \bmod P\mathcal{O}_{\mathbb{L}} \ . \tag{12}$$

Moreover,

$$\forall \tau \in \overline{H_P} \text{ such that } \tau_{|\mathbb{L}} \neq \mathrm{Id}, \quad \tau\alpha^p \neq \alpha^p \ . \tag{14}$$

Metric Properties

Let $\tau : \mathbb{L}(\alpha) \to \overline{\mathbb{Q}}$. We fix a valuation $v|P$. Then

1. if $\tau_{|\mathbb{L}} = \Phi_P^{-1}$ we have

$$|F(\tau\alpha^p)|_v \leq p^{-T/e_P} \max\{1, |\tau\alpha|_v\}^{pL}$$

for any $F \in \mathcal{O}_{\mathbb{E}}[x]$, of degree $\leq L$, vanishing on the D conjugates of α over $\mathbb{L}$ with multiplicity $\geq T$.

2. If $\tau_{|\mathbb{L}} \in H_P$, for any $\sigma \in H_P$ we have

$$\prod_{\substack{\rho : \mathbb{L}(\alpha) \to \overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}} = \sigma}} |\tau\alpha^p - \rho\alpha^p|_v \leq p^{-1} \max\{1, |\tau\alpha|_v\}^{pD} \times \prod_{\substack{\rho : \mathbb{L}(\alpha) \to \overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}} = \sigma}} \max\{1, |\rho\alpha|_v\}^p$$

We sketch the proof of these inequalities. We first assume that $\alpha \in \mathcal{O}_{\mathbb{E}}$. Thus the minimal polynomial $f(x) = f_0 + f_1 x + \cdots + x^D$ of α over $\mathbb{L}$ has coefficients in $\mathcal{O}_{\mathbb{L}}$.

Proof of the First Metric Property

Let $\tau_{|\mathbb{L}} = \Phi_P^{-1}$ and $Q \subset \mathcal{O}_{\mathbb{L}}$ over P. Using FℓT we get

$$0 = f(\alpha)^p \equiv f_0^p + f_1^p \alpha^p + \cdots + \alpha^{pD} \bmod p\mathcal{O}_{\mathbb{E}} \ .$$

By definition of the Frobenius Automorphism (cf (11))

$$f_j^p \equiv \Phi_P(f_j) \bmod Q\mathcal{O}_{\mathbb{L}}$$

for $j = 1, \ldots, D-1$. Thus

$$0 \equiv f^{\Phi}(\alpha^p) = \tau^{-1} f(\tau\alpha^p) \bmod Q\mathcal{O}_{\mathbb{E}}$$

which implies $|f(\tau\alpha^p)|_v \leq p^{-1/e_P}$. Since f is monic, by Gauss' Lemma (on $\mathcal{O}_{\mathbb{L}_v}$) we have $F = f^T G$ for some $G \in \mathcal{O}_{\mathbb{L}_v}$. Hence, $|F(\tau\alpha^p)|_v \leq p^{-T/e_P}$. This proves the First Metric Property.

Proof of the Second Metric Property

Let now $\tau_{|\mathbb{L}} \in H_P$ and $\sigma \in H_P$. Using FℓT twice we get

$$\prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}}=\sigma}} (\tau\alpha^p - \rho\alpha^p) \equiv \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}}=\sigma}} (\tau\alpha - \rho\alpha)^p = f^\sigma(\tau\alpha)^p$$

$$\equiv \sigma(f_0^p) + \sigma(f_1^p)(\tau\alpha)^p + \cdots + (\tau\alpha)^{pD} \bmod p\mathcal{O}_{\mathbb{E}}$$

By definition of H_P (cf (12)), we have $\sigma(f_j^p) \equiv \tau(f_j^p) \bmod P\mathcal{O}_{\mathbb{L}}$ for $j = 1, \ldots, D-1$. Thus, using again FℓT ,

$$\prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}}=\sigma}} (\tau\alpha^p - \rho\alpha^p) \equiv f^\tau(\tau\alpha)^p = 0 \bmod P\mathcal{O}_{\mathbb{E}} \ .$$

This proves the Second Metric Property.

Proof of the Metric Properties: denominator.

If α is not an algebraic integer, we must choose a "good denominator" at v for its minimal polynomial f. By the Strong Approximation Lemma, $\exists \beta \in \mathcal{O}_{\mathbb{L}}$ such that $\beta f_j \in \mathcal{O}_{\mathbb{L}}$ for $j = 1, \dots, D-1$ and, for $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$,

$$|\sigma(\beta)|_v = \max\{1, |\sigma(f_0)|_v, \dots, |\sigma(f_{D-1})|_v\}^{-1}$$

$$= \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}}=\sigma}} \max\{1, |\rho\alpha|_v\}^{-1} .$$

Let

$$g(x) = \beta f(x) = g_0 + g_1 x + \cdots g_D x^D \in \mathcal{O}_{\mathbb{L}}[x] .$$

The proof of the Metric Properties for non integer α follows working with g instead of f.

Diophantine approximation

We use the symbols $\approx$, $\ll$ and $\gg$ with the same meaning as in Dobrowolski's proof. Now the implicit constants depend on $\mathbb{K}$.

We fix the parameters

$$N \approx \frac{\log(D)^4}{\log\log(D)^3} \qquad \text{and} \qquad E \approx \frac{\log(D)}{\log\log(D)}$$

We let $\Lambda = \{P \in \mathcal{P} \text{ such that } \sqrt{N} \leq p \leq N\}$. By the Prime Ideal Theorem

$$|\{P \subseteq \mathcal{O}_{\mathbb{K}} \text{ such that } \sqrt{N} \leq N_{\mathbb{Q}}^{\mathbb{K}} P \leq N\}| \approx \frac{N}{\log N} \ .$$

There are only a finite number of primes ideals P with $e(P|p) > 1$. Moreover, if $f(P|p) > 1$, then $N_{\mathbb{Q}}^{\mathbb{K}} P \geq p^2$. Thus

$$|\{P \subseteq \mathcal{O}_{\mathbb{K}} \text{ s.t. } f(P|p) > 1 \text{ and } N_{\mathbb{Q}}^{\mathbb{K}} P \leq \sqrt{N}\}| \leq [\mathbb{K} : \mathbb{Q}]\sqrt{N} \ll \sqrt{N} \ .$$

The considerations above show that $|\Lambda| \approx N/\log N$.

Small ramification

We first assume $\forall P \in \Lambda$, $e_P \leq E$. Under this assumption, the proof closely follows Dobrowolski's proof, with a main difference. The classical Siegel's lemma would give a non-zero polynomial $F \in \mathcal{O}_{\mathbb{L}}[x]$ vanishing on the conjugates of α over L with a prescribed multiplicity, but the height of its coefficients will depend on the discriminant of L. To avoid this dependence, we use the Absolute Siegel's Lemma, which is a corollary of a deep result of Zhang's (see the lecture of Sinnou David).

We argue by contradiction, assuming $D\hat{h}(\alpha) \ll \left(\frac{\log D}{\log\log D}\right)^{-7}$.

Let L, T be two parameters with $L \geq DT$. Using the Absolute Siegel's Lemma lemma we find a non-zero polynomial F with algebraic integer coefficients, of degree $\leq L$, vanishing on the D conjugates of α over $\mathbb{L}$ with multiplicity $\geq T$ and such that:

Auxiliary Function

$$h(F) \leq \frac{DT}{L+1-DT}(T\log(L+1) + L\hat{h}(\alpha)) + \log L\,. \qquad (15)$$

Here $h(F)$ denotes the Weil height of the vector of coefficients of F. That is, if $F = F_0 + \cdots + F_L x^L \in \mathbb{E}[x]$,

$$h(F) = \frac{1}{[\mathbb{E}:\mathbb{Q}]} \sum_{v \in \mathcal{M}_{\mathbb{E}}} [\mathbb{E}_v : \mathbb{Q}_v] \log \max\{|F_0|_v, \ldots, |F_L|_v\}\,.$$

We choose

$$T \approx \left(\frac{\log D}{\log\log D}\right)^2 \qquad \text{and} \qquad L = DT^2 \approx D\left(\frac{\log D}{\log\log D}\right)^4\,.$$

Thus $\frac{DT^2}{L+1-DT} \approx 1$. Since $L\hat{h}(\alpha) \ll \log D$ we have $h(F) \ll \log D$.

Extrapolation

Let $P \in \Lambda$ and $\tau\colon L(\alpha) \to \overline{\mathbb{Q}}$ such that $\tau_{|L} = \Phi_P^{-1}$. We want to show that $F(\tau\alpha^p) = 0$. Assume the contrary. Let $v \mid P$. By the First Metric Property,

$$|F(\tau\alpha^p)|_v \leq C(v) \max\{1, |\tau\alpha|_v\}^{pL} .$$

with $C(v) = p^{-T/e_P} \leq p^{-T/E}$. This inequality trivially holds with $C(v) = 1$ for the other ultrametric places. Let finally $v \mid \infty$. Then

$$|F(\tau\alpha^p)|_v \leq (L+1) \max\{|F_0|_v, \ldots, |F_L|_v\} \max\{1, |\tau\alpha|_v\}^{pL} .$$

By the Product Formula,

$$0 \leq \log(L+1) - \frac{T \log p}{E[\mathbb{K} : \mathbb{Q}]} + pL\hat{h}(\alpha) + h(F)$$

Since $\frac{T \log p}{E[\mathbb{K}:\mathbb{Q}]} \gg \log D$, $\log(L+1) + h(F) \ll \log D$ and $pL\hat{h}(\alpha) \ll \log D$ we get a contradiction.

Zero's lemma and conclusion

Since α is not a root of unity, α^{p_1} and α^{p_2} are not conjugates for primes $p_1 \neq p_2$. Then the set Σ of $\tau\alpha^P$ ($P \in \Lambda$, $\tau : \mathbb{L}(\alpha) \to \overline{\mathbb{Q}}$ such that $\tau_{|L} = \Phi_P^{-1}$) satisfies

$$\#\Sigma = D|\Lambda| \gg \frac{DN}{\log N} \gg D\left(\frac{\log D}{\log\log D}\right)^4 .$$

Thus $\#\Sigma > L$. Since the number of zeros of F cannot exceed its degree, we get a contradiction which shows that

$$D\hat{h}(\alpha) \gg \left(\frac{\log D}{\log\log D}\right)^{-7} .$$

This conclude the proof of the Relative Lower Bound, under the additional assumption $\forall P \in \Lambda$, $e_P \leq E$.

Large ramification

Assume now that there exists $P \in \Lambda$ such that $e_P \geq E$. Remark that $p \geq \sqrt{N} \geq E$. Thus $|H_P| = E$. We use the Interpolation Determinant Method of Laurent.

We define Δ as the square of a Vandermonde determinant of size $L = DE$:

$$\Delta = \prod_{\tau \in \overline{H_P}} \prod_{\rho \in \overline{H_P} \setminus \{\tau\}} |\tau\alpha^p - \rho\alpha^p|_v = \prod_{\tau \in \overline{H_P}} \delta_\tau \ .$$

By (14), $\Delta \neq 0$. We want to apply the product formula to Δ.

Let $v|P$. Then

$$|\delta_\tau|_v = \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}} \neq \tau_{|\mathbb{L}}}} |\tau\alpha^p - \rho\alpha^p|_v \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}} = \tau_{|\mathbb{L}},\ \rho \neq \tau}} |\tau\alpha^p - \rho\alpha^p|_v$$

$$= \prod_{\substack{\sigma \in H_P \\ \sigma \neq \tau_{|\mathbb{L}}}} \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}} = \sigma}} |\tau\alpha^p - \rho\alpha^p|_v \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}} \\ \rho_{|\mathbb{L}} = \tau_{|\mathbb{L}},\ \rho \neq \tau}} |\tau\alpha^p - \rho\alpha^p|_v$$

Large ramification

$$|\delta_\tau|_v = \prod_{\substack{\sigma\in H_P\\ \sigma\neq\tau_{|\mathbb{L}}}} \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}}\\ \rho_{|\mathbb{L}}=\sigma}} |\tau\alpha^p - \rho\alpha^p|_v \prod_{\substack{\rho\colon \mathbb{L}(\alpha)\to\overline{\mathbb{Q}}\\ \rho_{|\mathbb{L}}=\tau_{|\mathbb{L}},\ \rho\neq\tau}} |\tau\alpha^p - \rho\alpha^p|_v$$

$$\leq p^{-(E-1)} \max\{1, |\tau\alpha|_v\}^{2(L-1)} \prod_{\rho\in H_P\setminus\{\tau\}} \max\{1, |\rho\alpha|_v\}^p$$

(use the Second Metric Property and the Ultrametric Inequality). Thus

$$|\Delta|_v \leq C(v) \prod_{\tau\in\overline{H_P}} \max\{1, |\tau\alpha|_v\}^{2p(L-1)} . \qquad (*)$$

with $C(v) = p^{-L(E-1)}$. For the other finite places $(*)$ still holds with $C(v) = 1$ (use the Ultrametric Inequality).

Let now $v \mid \infty$. By Hadamard's inequality (*a determinant is bounded in absolute value by the product of the L_2 norms of its rows*), we see that $(*)$ holds with $C(v) = L^L$.

Large ramification

Thus $|\Delta|_v \leq C(v) \prod_{\tau \in \overline{H_P}} \max\{1, |\tau\alpha|_v\}^{2p(L-1)}$ with $C(v) = p^{-L(E-1)}$ if $v \mid P$, $C(v) = 1$ if $v \nmid \infty$ and $v \nmid P$, and $C(v) = L \log L$ if $v \mid \infty$. The Product Formula gives:

$$0 \leq L \log L - \frac{L(E-1)}{[\mathbb{K} : \mathbb{Q}]} \log p + 2p(L-1) \sum_{\tau \in \overline{H_P}} \hat{h}(\tau\alpha) \ .$$

Since $\sum_{\tau \in \overline{S}} \hat{h}(\tau\alpha) = L\hat{h}(\alpha)$ and $p(L-1) \leq NL = DNE$,

$$2DNE\hat{h}(\alpha) \geq \frac{(E-1)}{[\mathbb{K} : \mathbb{Q}]} \log p - \log L \gg \log D \ .$$

We deduce:

$$D\hat{h}(\alpha) \gg \frac{\log D}{NE} \gg \left(\frac{\log \log D}{\log D} \right)^4 \ .$$

Proof the Absolute Abelian Lower Bound

We give a sketch of the proof of:

Theorem (Absolute Abelian Lower Bound)

Let $\mathbb{K}$ be a number field of degree d over $\mathbb{Q}$ and let $\mathbb{L}/\mathbb{K}$ be an abelian extension. Then, for $\alpha \in \mathbb{L}^* \backslash \boldsymbol{\mu}$,

$$\hat{h}(\alpha) > 3^{-d^2-2d-6}.$$

The proof of this theorem requires some new arguments: we shall need a finer use of ramification theory and a new descent argument to eliminate dependence on the discriminant of $\mathbb{K}$.

We fix a a prime ideal $P \subset \mathcal{O}_{\mathbb{K}}$ of norm q over $\mathbb{Q}$. Assume first thet P is not ramified in $\mathbb{L}$. Let $Q \subset \mathcal{O}_{\mathbb{L}}$ over P. Since $\mathbb{L}/\mathbb{K}$ is abelian the Frobenius automorphism $\phi_P = \phi(Q|P)$ depends only on P. As in the proof of the Relative Lower Bound, we have

$$\forall \gamma \in \mathcal{O}_{\mathbb{L}}, \quad \gamma^q \equiv \phi_P \gamma \bmod P\mathcal{O}_{\mathbb{L}} .$$

Proof the Absolute Abelian Lower Bound

Assume from now on that P ramifies in $\mathbb{L}$ and consider the subgroup

$$H_P = \{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \text{ such that } \forall \gamma \in \mathcal{O}_{\mathbb{L}},\ \sigma\gamma^q \equiv \gamma^q \bmod P\mathcal{O}_{\mathbb{L}}\}\ .$$

If $\mathbb{K}_P = \mathbb{Q}_p$, then $\mathbb{L}$ is locally contained in a cyclotomic extension of $\mathbb{Q}$ by Kronecker-Weber. Using this fact, we showed in the proof of the Relative Lower Bound that H_P is non-trivial. Here we need a generalization of this result, dropping the assumption $\mathbb{K}_P = \mathbb{Q}_p$, which introduces a dependence on the discriminant of $\mathbb{K}$. This is done using the ramification theory.

Higher ramification groups

Let $\mathbb{L}/\mathbb{K}$ be normal with Galois group G. Let P be a prime ideal of $\mathbb{K}$ and let Q be a prime ideal of $\mathbb{L}$ over P of norm q over $\mathbb{Q}$. Define $G_{-1} = G_{-1}(Q|P) = D(Q|P)$ and, for $k = 0, 1, \ldots,$

$$G_k = G_k(Q|P) = \{\sigma \in G \text{ such that } \forall \gamma \in \mathcal{O}_{\mathbb{L}},\ \sigma\gamma \equiv \gamma \bmod Q^{k+1}\}\ .$$

Then $G \supseteq G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots$ and $G_0 = I(Q|P)$. Moreover, for all $k \geq 0$, G_k is a normal subgroup of G_{-1}. Writing $e = |G_0| = e_0 p^a$ with $p \nmid e_0$ we have $|G_0/G_1| = e_0$. Let π be a uniformizer at Q (*i.e.* $\pi \in Q \setminus Q^2$). Let

$$\begin{aligned} \theta_0 \colon G_0/G_1 &\to (\mathcal{O}_{\mathbb{L}}/Q)^* \\ \sigma &\mapsto \sigma(\pi)/\pi \bmod Q \end{aligned}$$

and, for $k \geq 1$,

$$\begin{aligned} \theta_k \colon G_k/G_{k+1} &\to Q^k/Q^{k+1} \\ \sigma &\mapsto \sigma(\pi)/\pi - 1 \bmod Q \end{aligned}$$

Higher ramification groups

It is well known that the maps θ_k are well-defined, injective and do not depend on the choice of the uniformizer

Assume G_{-1} abelian. Then

1. The image of θ_0 is contained in $(\mathcal{O}_{\mathbb{K}}/P)^*$.
2. For all $k \geq 1$, the image of θ_k is contained in a $\mathcal{O}_{\mathbb{K}}/P$ vector space of dimension 1.

In particular, for $k = 0, 1, \ldots,$

$$|G_k/G_{k+1}| \leq q \tag{16}$$

For 1), see for instance, Cassels, op. cit., corollary 2, page 136. We prove 2). If G_k/G_{k+1} is trivial the result is clear. Let $v_0 \neq 0$ and v in $\mathrm{Im}(\theta_k)$. Since $\dim_{\mathcal{O}_{\mathbb{L}}/Q} Q^k/Q^{k+1} = 1$, $\exists \lambda \in \mathcal{O}_{\mathbb{L}}/Q$ such that $v = \lambda v_0$. A straightforward computation shows that $\mathrm{Im}(\theta_k)$ is fixed by G_{-1}. Since $\mathrm{Gal}(\mathcal{O}_{\mathbb{L}}/Q/\mathcal{O}_{\mathbb{K}}/P) \cong G_{-1}/G_0$, we infer that $\lambda \in \mathcal{O}_{\mathbb{K}}/P$. Thus $\mathrm{Im}(\theta_k)$ is contained in the $\mathcal{O}_{\mathbb{K}}/P$-vector space spanned by v_0.

The group H_P

We now assume $\mathbb{L}/\mathbb{K}$ abelian and we prove that

$$H_P := \{\sigma \in G \text{ such that } \forall \gamma \in \mathcal{O}_{\mathbb{L}},\ \sigma\gamma^q \equiv \gamma^q \bmod P\mathcal{O}_{\mathbb{L}}\} \neq \{\mathrm{Id}\}\ .$$

Proof. Since G is abelian, the higher ramification groups do not depend on the choice of Q over P. Assume first that P is tamely ramified in $\mathbb{L}$. Thus $e = e_0 = |G_0/G_1| \leq q$, by (16). Let $\sigma \in G_0$ and $\gamma \in \mathcal{O}_{\mathbb{L}}$; then

$$(\sigma\gamma - \gamma)^q \in Q^q \subseteq Q^e$$

and

$$(\sigma\gamma - \gamma)^q \equiv \sigma\gamma^q - \gamma^q \bmod p\mathcal{O}_{\mathbb{L}}\ .$$

This implies

$$\sigma\gamma^q \equiv \gamma^q \bmod P\mathcal{O}_{\mathbb{L}}\ .$$

Thus $H_P \supset G_0$. On the other hand, G_0 is non-trivial because P ramifies in $\mathbb{L}$ by assumption.

The group H_P

Let now assume $p \mid e$. By Hasse-Arf theorem (Serre, op. cit., section 7, Th. 1', p.101)

$$\forall j \geq 1,\ G_j \neq G_{j+1} \Longrightarrow \frac{1}{e}\sum_{i=1}^{j} |G_i| \in \mathbb{Z}\ .$$

Let $k \geq 1$ such that $G_k \neq G_{k+1} = \{\mathbf{1}\}$. We also define $h = 0$ if $G_k = G_1$ and otherwise we define $h \geq 1$ by

$$G_h \neq G_{h+1} = \cdots = G_k \neq G_{k+1} = \{\mathbf{1}\}\ .$$

Then

$$\frac{1}{e}\sum_{i=1}^{h} |G_i| \in \mathbb{Z} \quad \text{and} \quad \frac{1}{e}\sum_{i=1}^{k} |G_i| \in \mathbb{Z}\ .$$

Thus, using (16),

$$e \leq \sum_{i=h+1}^{k} |G_i| = (k-h)|G_k| = (k-h)|G_k/G_{k+1}| \leq kq\ .$$

The group H_P and a conditional lower bound

Therefore, for any $\sigma \in G_{k-1}$ and for any $\gamma \in \mathcal{O}_{\mathbb{L}}$

$$(\sigma\gamma - \gamma)^q \in Q^{kq} \subseteq Q^e.$$

As before, this implies

$$\sigma\gamma^q \equiv \gamma^q \bmod P\mathcal{O}_{\mathbb{L}} .$$

Thus $\{\mathbf{1}\} \neq G_{k-1} \subseteq H_P \subseteq G_0$. This proves that H_P is non trivial.

□

From now on we fix $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ and we assume $\mathbb{K}(\alpha)/\mathbb{K}$ be abelian. Let as before P be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ of norm q over $\mathbb{Q}$. Assume further

$$\mathbb{K}(\alpha) = \mathbb{K}(\alpha^q) . \tag{17}$$

Then, arguing as in the proof of the Abelian Lower bound,

$$\hat{h}(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{2q} . \tag{18}$$

A conditional lower bound. Case I : P not ramified.

Proof. Let $(p) = P \cap \mathbb{Z}$ and let $e = e(P/p)$.

Assume first that P does not ramify in $\mathbb{K}(\alpha)$. Let ϕ_P be the Frobenius automorphism of a prime over P. As in the proof of the Abelian Lower Bound we have

$$|\alpha^q - \phi(\alpha)|_v \leq c(v) \max(1, |\alpha|_v)^q \max(1, |\phi(\alpha)|_v)$$

with $c(v) = p^{-1/e}$ if $v \mid P$, $c(v) = 1$ if $v \nmid P$, $v \nmid \infty$ and $c(v) = 2$ if $v \mid \infty$. Since α is not a root of unity, $\alpha^q - \phi(\alpha) \neq 0$. Applying the Product Formula we get

$$0 \leq (q+1)\hat{h}(\alpha) + \log 2 - \frac{1}{d} \log q$$

i.e.

$$\hat{h}(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{q+1} \geq \frac{\log\left(q^{1/d}/2\right)}{2q} \ .$$

A conditional lower bound. Case II : P ramified.

Assume now that P is ramified in $\mathbb{K}(\alpha)$ and let σ be a non trivial automorphism in the subgroup H_P. Then (again as in the proof of the Abelian Lower Bound)

$$|\alpha^q - \sigma(\alpha)^q|_v \leq c(v) \max(1, |\alpha|_v)^q \max(1, |\sigma(\alpha)|_v)^q$$

with $c(v)$ as in the case I.

Assume $\sigma(\alpha)^q = \alpha^q$. Since $\sigma(\alpha) \neq \alpha$ we have $\mathbb{K}(\alpha^q) \subsetneq \mathbb{K}(\alpha)$, which contradicts hypothesis (17). Thus $\sigma(\alpha)^q \neq \alpha^q$.

Applying the product formula to $\alpha^q - \sigma(\alpha)^q \neq 0$, we get

$$0 \leq 2q\hat{h}(\alpha) + \log 2 - \frac{1}{d} \log q \ .$$

Therefore

$$\hat{h}(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{2q} \ .$$

□

Fourth lecture:

- Sketch of the proof of the Absolute Abelian Lower Bound (second part)
- Application: exponent of the class group of CM fields

A conditional lower bound

Let $\mathbb{K}$ be a number field. Let $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ and assume $\mathbb{K}(\alpha)/\mathbb{K}$ be abelian of Galois group G.

Proposition

Let P be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ of norm q over $\mathbb{Q}$. Assume further

$$\mathbb{K}(\alpha) = \mathbb{K}(\alpha^q)\ . \tag{17}$$

Then,

$$\hat{h}(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{2q}\ . \tag{18}$$

We want to show that a slightly weaker version of (18) still holds without assuming (17). The proof of the main theorem will follow.

Radicals reduction. I. Box Principle

We need the following elementary lemma:

Lemma (Box Principle)

Let B, k be integers with $B \geq 5$. Then, for every subgroup H of $(\mathbb{Z}/k\mathbb{Z})^*$ of index $\leq B$, there are integers h_1, h_2 such that $\overline{h}_1$, $\overline{h}_2 \in H$ and

$$2 < h_1 - h_2 < 30B \log B \ .$$

Proof. Write $k = k_1 l_1^{a_1} \cdots l_s^{a_s}$ where k_1 is divisible only by primes $\leq B^5$ and where l_i are distinct primes $> B^5$. We identify $(\mathbb{Z}/k\mathbb{Z})^*$ with $(\mathbb{Z}/k_1\mathbb{Z})^*(\mathbb{Z}/l_1^{a_1}\mathbb{Z})^* \cdots (\mathbb{Z}/l_s^{a_s}\mathbb{Z})^*$. Put $H_1 = H \cap (\mathbb{Z}/k_1\mathbb{Z})^*$ so that $[(\mathbb{Z}/k_1\mathbb{Z})^* : H_1] \leq B$.

I. Box Principle

By a result of Rosser and Schoenfeld's (1962), for any $x > 1$ we have $\prod_{l \le x}(1 - 1/l) > \frac{e^{-\gamma}}{\log x}(1 - (\log x)^{-2})$ where γ is Euler's constant and l runs through prime numbers. Since $B \ge 5$,

$$\frac{k_1}{\phi(k_1)} = \prod_{l \le B^5} \left(1 - \frac{1}{l}\right)^{-1} < 10 \log B \ , \qquad (*)$$

By the box principle, there exist integers $x_1 < x_2 < x_3 < x_4$ such that $x_i \bmod k_1 \in H_1$ and

$$x_4 - x_1 \le \frac{k_1}{\frac{1}{3}|H_1|} \le \frac{3Bk_1}{\phi(k_1)} < 30B \log B \ .$$

Then $x \bmod k_1$, $x + t \bmod k_1 \in H_1$ and $2 < t < 30B \log B$.

I. Box Principle

Fix $l = l_i$ and $a = a_i$ for $i \in \{1, \dots, s\}$. Put $H_l = H \cap (\mathbb{Z}/l^a\mathbb{Z})^*$. Again, $b = [(\mathbb{Z}/l^a\mathbb{Z})^* : H_l] \leq B$. Let $r : (\mathbb{Z}/l^a\mathbb{Z})^* \to \mathbb{F}_l^*$ be the reduction $\bmod l$. Since $[(\mathbb{Z}/l^a\mathbb{Z})^* : \ker(r)] = l - 1 \geq B$, we have $\ker(r) \subseteq H_l$. Thus $[\mathbb{F}_l^* : r(H_l)] = b$ and $r(H_l) = \{u^b \mid u \in \mathbb{F}_l^*\}$.

The projective curve $\mathcal{C} : X^b - Y^b = tZ^b$ over $\mathbb{F}_l$ is nonsingular, because $0 < t < l$, and its genus is $g = (b-1)(b-2)/2 \leq B^2$. By a theorem of Weil's, $\mathcal{C}$ has $\geq l + 1 - 2g\sqrt{l}$ points. At least $l + 1 - 2g\sqrt{l} - 3b$ of them have $XYZ \neq 0$. Since $l \geq B^5$ and $B \geq 5$, this lower bound is > 0. Hence there $\exists x_l \in \mathbb{Z}$ such that $x_l \bmod l \in r(H_l)$ and $x_l + t \bmod l \in r(H_l)$. Since $\ker(r) \subseteq H_l$, this implies $x_l \bmod l^a \in H_l$ and $x_l + t \bmod l^a \in H_l$.

It is now enough to pick with the Chinese Theorem an h_2 congruent to x modulo k_1 and to x_l modulo l^a, for each l dividing k_2, and to put $h_1 = h_2 + t$. □

II. Kummer's theory

Let $\Gamma = \{\rho \in G \ : \ \rho(\alpha)/\alpha \in \boldsymbol{\mu}\} < G$.

Lemma (Kummer)

Let $k \in \mathbb{N}$ such that any root of unity of the shape $\rho(\alpha)/\alpha$ for $\rho \in \Gamma$ has order dividing k. Let $\sigma \in \mathrm{Gal}(\mathbb{K}(\zeta_k)/\mathbb{K})$ and let $g \in \mathbb{Z}$ such that $\sigma\zeta_k = \zeta_k^g$. Then, for any extension $\tilde{\sigma} \in \mathrm{Gal}(\mathbb{K}(\alpha, \zeta_k)/\mathbb{K})$ of σ, we have

$$\tilde{\sigma}\alpha/\alpha^g \in \mathbb{K}(\alpha)^\Gamma \ .$$

Proof. Let $\rho \in \Gamma$. Then $\rho\alpha = \zeta_k^u \alpha$ for some $u \in \mathbb{Z}$. Put $\alpha' = \tilde{\sigma}\alpha \in \mathbb{K}(\alpha)$. Then, since $\mathbb{K}(\alpha, \zeta_k)/\mathbb{K}$ is abelian,

$$\rho\alpha'/\alpha' = \rho\tilde{\sigma}\alpha/\tilde{\sigma}\alpha = \tilde{\sigma}(\rho\alpha/\alpha) = \sigma\zeta_k^u = \zeta_k^{ug} = (\rho\alpha/\alpha)^g \ .$$

Thus α'/α^g is fixed by ρ for all $\rho \in \Gamma$, and therefore it lies in $\mathbb{K}(\alpha)^\Gamma$. □

An unconditional lower bound

Using the previous lemmas we prove a weaker but unconditional version of (18).

$$\hat{h}(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{184d\log(3d)q} \ .$$

Proof. We choose $k \in \mathbb{N}$ such that any root of unity of the shape $\rho(\alpha)/\alpha$ for $\rho \in \Gamma$ has order dividing k. We identify $\mathrm{Gal}(\mathbb{K}(\zeta_k)/\mathbb{K})$ to a subgroup of $(\mathbb{Z}/k\mathbb{Z})^*$ of index $\leq d$. Choosing $B = 3d \geq 6$ in the Box Principle Lemma we see that $\exists \sigma_1$, $\sigma_2 \in \mathrm{Gal}(\mathbb{K}(\zeta_k)/\mathbb{K})$ such that $\sigma_i \zeta_k = \zeta_k^{g_i}$ and $g = g_2 - g_1$ satisfies

$$2 < g < 90d\log(3d) \ . \tag{19}$$

By Kummer's Lemma we have

$$\tilde{\sigma}_2(\alpha) = c\,\alpha^g \tilde{\sigma}_1(\alpha) \tag{20}$$

with $c \in \mathbb{K}(\alpha)^\Gamma$. We want to apply (18) to with $\alpha \leftarrow c$.

An unconditional lower bound

To do that we need that $c \notin \boldsymbol{\mu}$ and that $\mathbb{K}(c) = \mathbb{K}(c^q)$. Let us verify these requirements. We argue by contradiction.

- $c \in \boldsymbol{\mu}$. Then, by (20),

$$g\hat{h}(\alpha) = \hat{h}(\alpha^g) = \hat{h}(\tilde{\sigma}_2(\alpha)/\tilde{\sigma}_1(\alpha)) \leq 2\hat{h}(\alpha) \, .$$

Since $g > 2$ by (19) we get $\alpha \in \boldsymbol{\mu}$. Contradiction.

- $\mathbb{K}(c^q) \subsetneq \mathbb{K}(c)$. Let $\tau \in \mathrm{Gal}(\mathbb{K}(c)/\mathbb{K}(c^q))\backslash\{\mathrm{Id}\}$. Then $\exists \theta \in \boldsymbol{\mu}\backslash\{1\}$ such that $\tau(c) = \theta c$. Let $\tilde{\tau} \in \mathrm{Gal}(\mathbb{K}(\alpha)/\mathbb{K})$ extending τ and set $\eta = \tilde{\tau}(\alpha)/\alpha$. Apply (20) and its conjugate by $\tilde{\tau}$, taking into account that we are working in an abelian extension of $\mathbb{K}$. We obtain $\tilde{\sigma}_2(\eta) = \theta\eta^g\tilde{\sigma}_1(\eta)$. Hence $g\hat{h}(\eta) \leq 2\hat{h}(\eta)$ which implies $\hat{h}(\eta) = 0$ by (19). Thus $\eta \in \boldsymbol{\mu}$. But then $\tilde{\tau} \in \Gamma$. Thus $\tilde{\tau}$ fixes $c \in \mathbb{K}(\alpha)^\Gamma$ and $\theta = 1$. Contradiction.

An unconditional lower bound

Applying (18) with $\alpha \leftarrow c$ we get $\hat{h}(c) \geq \log(q^{1/d}/2)/(2q)$. By (19) and (20), $\hat{h}(c) \leq (g+2)\hat{h}(\alpha) \leq 92d\log(3d)\hat{h}(\alpha)$. Thus

$$\hat{h}(\alpha) \geq \frac{\log\left(q^{1/d}/2\right)}{184d\log(3d)q}\,. \tag{21}$$

□

Now it is easy to prove the Absolute Abelian Lower Bound. Let p be a prime number such that $3^d \leq p < 2\cdot 3^d$ and let $P \subset \mathcal{O}_{\mathbb{K}}$ be a prime over p. Then $3^d \leq p \leq q \leq p^d < 3^{d^2+d}$. Thus, by (21),

$$\hat{h}(\alpha) > \frac{\log(3/2)}{184d\log(3d)\cdot 3^{d^2+d}} \geq 3^{-d^2-2d-5}\,,$$

since $\log(3/2) \geq 1/3$ and $184d\log(3d) \leq 3^{d+4}$.

Open Problems

1. Let $\mathbb{K}$ be a number field of degree d over $\mathbb{Q}$ and let $\mathbb{L}/\mathbb{K}$ be an abelian extension. Let $\alpha \in \mathbb{L}^* \backslash \boldsymbol{\mu}$. What is the right lower bound for $\hat{h}(\alpha)$ in term of d?
2. Prove a Relative Absolute Lower Bound:
   Let $\mathbb{K}$ be a number field of degree d over $\mathbb{Q}$ and let $\mathbb{L}/\mathbb{K}$ be an abelian extension. Let $\alpha \in \overline{\mathbb{Q}}^* \backslash \boldsymbol{\mu}$ of degree D over $\mathbb{L}$. Then

$$\hat{h}(\alpha) \geq \frac{C(d)}{D} (\log D)^{-c} .$$

Class number problem for CM fields

A CM field $\mathbb{K}$ is a totally imaginary quadratic extension of a totally real field $\mathbb{K}^+$.

Class number problem for CM fields (Stark):

$$h_{\mathbb{K}} \to \infty \quad \text{as} \quad \mathrm{disc}(\mathbb{K}) \to +\infty \ .$$

Solved by Stark (1974) (effective versions of the Brauer-Siegel theorem) and Odlyzko (1975) (lower bound for the discriminant), under one of the following assumptions :

- GRH or Artin's conjecture on L-functions
- $\mathbb{K}^+/\mathbb{Q}$ Galois, or, more generally:

$$\mathbb{Q} = k_0 \subset k_1 \subset \cdots \subset k_t = \mathbb{K}^+$$

with k_i/k_{i-1} Galois.

Exponent of the class group of CM fields

Let $\mathbb{K}$ be a CM field of degree $D_{\mathbb{K}} = [\mathbb{K} : \mathbb{Q}]$. Let $e_{\mathbb{K}}$ be the exponent of its ideal class group. Louboutin and Okazaki (2003) ask if

$$e_{\mathbb{K}} \to \infty \quad \text{as} \quad \operatorname{disc}(\mathbb{K}) \to +\infty \, .$$

In this direction, they prove:

Theorem (Louboutin-Okazaki, 2003)

Assume GRH. Then,

$$e_{\mathbb{K}} \gg_{D_{\mathbb{K}}} \frac{\log |\operatorname{disc}(\mathbb{K})|}{\log \log |\operatorname{disc}(\mathbb{K})|} \, .$$

where the constant involved in $\gg_{D_{\mathbb{K}}}$ depends on the degree $D_{\mathbb{K}} = [\mathbb{K} : \mathbb{Q}]$ only.

Exponent of the class group of CM fields

Theorem (A.-Dvornicich, 2003)

Let $\mathbb{K}$ be a CM field of degree $D_{\mathbb{K}} = [\mathbb{K} : \mathbb{Q}]$. Then, assuming the Generalized Riemann Hypothesis for the Dedekind zeta function of $\mathbb{K}$, for any $\varepsilon > 0$ the exponent $e_{\mathbb{K}}$ of the class group of $\mathbb{K}$ satisfies:

$$e_{\mathbb{K}} \gg_{\varepsilon} \max\left\{ \frac{\log|\mathrm{disc}(\mathbb{K})|}{D_{\mathbb{K}} \log\log|\mathrm{disc}(\mathbb{K})|}, D_{\mathbb{K}}^{1-\varepsilon} \right\} .$$

It is easily seen that the R.H.S. is $\gg (\log|\mathrm{disc}(\mathbb{K})|)^{(1-\varepsilon)/2}$. Thus the theorem gives a (conditional) positive answer to Louboutin-Okazaki's conjecture.

The Height Method

The proof of this result is a special case of a general construction which we summarize as follows:

I) Assume the ideal class group of $\mathbb{K}$ "small". Construct algebraic numbers of small Weil's height from prime ideals of small norm.

II) Construct prime ideals of small norm by analytic methods.

III) Use lower bounds for the height to get a contradiction.

This method provides also informations on the size of the class group and on its Galois structure. It applies to more general fields, for instance field generated by a Salem number i.e. an algebraic number $\theta > 1$ whose algebraic conjugates $\neq \theta, \theta^{-1}$ lie on the unit circle.

The Main Principle

Proposition (Main Principle)

Let $\mathbb{K}$ be a CM field of degree $D_{\mathbb{K}} = [\mathbb{K} : \mathbb{Q}]$ and exponent of the class group $e_{\mathbb{K}}$. Let P be an integral prime ideal of degree 1. Then $\exists \alpha \in \mathbb{K}^*$ such that

1. $\hat{h}(\alpha) = \frac{e_{\mathbb{K}}}{D_{\mathbb{K}}} \log N_{\mathbb{K}/\mathbb{Q}} P$ *(thus $\alpha \notin \boldsymbol{\mu}$).*
2. $\mathbb{K} = \mathbb{Q}(\alpha)$.

The Main Principle

Proof. Let $P^{e_{\mathbb{K}}} = (\gamma)$ and $\alpha = \overline{\gamma}/\gamma$. Since P is of degree 1 we have $\overline{P} \neq P$ and moreover $\mathbb{K} = \mathbb{Q}(\alpha)$ (easy lemma).

Since $\mathbb{K}$ is a CM field, $|\alpha|_v = 1$ for $v \mid \infty$. If $v \nmid \infty$,

$$|\alpha|_v^{[\mathbb{K}_v:\mathbb{Q}_v]} = \begin{cases} (N_{\mathbb{K}/\mathbb{Q}}P)^{e_{\mathbb{K}}}, & \text{if } v = P; \\ (N_{\mathbb{K}/\mathbb{Q}}P)^{-e_{\mathbb{K}}}, & \text{if } v = \overline{P}; \\ 1, & \text{otherwise.} \end{cases}$$

Thus

$$D_{\mathbb{K}}\hat{h}(\alpha) = \sum_{v \in \mathcal{M}_{\mathbb{K}}} [\mathbb{K}_v : \mathbb{Q}_v] \log^+ |\alpha|_v = e_{\mathbb{K}} \log N_{\mathbb{K}/\mathbb{Q}}P \ .$$

□

Effective Prime Ideal Theorem

Let $\mathbb{K}$ be any number field. A theorem of Lagarias-Odlyzko (1977) implies:

Theorem (Effective Prime Ideal Theorem)

Let n be a positive integer. If the Generalized Riemann Hypothesis holds for the Dedekind zeta function of $\mathbb{K}$, then there exists distinct integral prime ideals $P_1, \ldots, P_n$ of degree 1, non-ramified over $\mathbb{Q}$, and such that

$$\log |N_{\mathbb{K}/\mathbb{Q}} P_j| \ll \log \log |\mathrm{disc}(\mathbb{K})| + \log n \, .$$

This result is the (fundamental) contribution from Analytic Number Theory to the Height Method.

Height and Discriminant

Proposition (Discriminant Lower Bound for the height)

Let $\alpha \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{Q}(\alpha)$. Then

$$\hat{h}(\alpha) \geq \frac{\log |\mathrm{disc}(\mathbb{K})| - D_{\mathbb{K}} \log D_{\mathbb{K}}}{2D_{\mathbb{K}}(D_{\mathbb{K}} - 1)} \, .$$

Proof. It is a very special case of a result of Silverman (1984), already quoted on the lecture of Martin Widmer.

Louboutin-Okazaki revisited

By the Main Principle and by the Effective Prime Ideal Theorem, we find $\alpha \in \mathbb{K}^*$ s.t. $\mathbb{K} = \mathbb{Q}(\alpha)$ and $\hat{h}(\alpha) \ll \frac{e_{\mathbb{K}}}{D_{\mathbb{K}}} \log\log|\mathrm{disc}(\mathbb{K})|$. The Discriminant Lower Bound for the height gives

$$\hat{h}(\alpha) \geq \frac{\log|\mathrm{disc}(\mathbb{K})| - D_{\mathbb{K}} \log D_{\mathbb{K}}}{2D_{\mathbb{K}}(D_{\mathbb{K}} - 1)} .$$

Thus

Proposition (Discriminant Lower Bound for the exponent)

In a CM field

$$e_{\mathbb{K}} \gg \frac{\log|\mathrm{disc}(\mathbb{K})| - D_{\mathbb{K}} \log D_{\mathbb{K}}}{D_{\mathbb{K}} \log\log|\mathrm{disc}(\mathbb{K})|} .$$

This implies Louboutin-Okazaki's result

$$e_{\mathbb{K}} \gg_{D_k} \frac{\log|\mathrm{disc}(\mathbb{K})|}{\log\log|\mathrm{disc}(\mathbb{K})|} .$$

More than Lehmer

The Discriminant Lower Bound for the exponent is efficient only if $\log|\mathrm{disc}(\mathbb{K})|$ is large, say $\geq 2D_{\mathbb{K}}\log D_{\mathbb{K}}$. For "small" discriminants we need other bounds. But even Lehmer's conjecture is not enough! Indeed, the use of Lehmer's conjectural bound $\hat{h}(\alpha) \gg 1/D_{\mathbb{K}}$ in the formula

$$\hat{h}(\alpha) \ll \frac{e_{\mathbb{K}}}{D_{\mathbb{K}}}\log\log|\mathrm{disc}(\mathbb{K})|$$

gives only

$$e_{\mathbb{K}} \gg \frac{1}{\log\log|\mathrm{disc}(\mathbb{K})|}$$

which tends to zero !

Exponent of imaginary abelian extensions

Assume for the moment $\mathbb{K}/\mathbb{Q}$ abelian.

By the Main Principe and by the Effective Prime Ideal Theorem, we find a non-root of unity $\alpha \in \mathbb{K}^*$ such that $\mathbb{K} = \mathbb{Q}(\alpha)$ and

$$\hat{h}(\alpha) \ll \frac{e_{\mathbb{K}}}{D_{\mathbb{K}}} \log\log|\mathrm{disc}(\mathbb{K})| \ .$$

By the Abelian Lower Bound:

$$\hat{h}(\alpha) \geq \frac{\log 5}{12} \ .$$

We obtain

$$e_{\mathbb{K}} \gg \frac{D_k}{\log\log|\mathrm{disc}(\mathbb{K})|} \ .$$

Exponent of imaginary abelian extensions

Collecting together this last lower bound and the Discriminant Lower Bound for the exponent, we get

$$e_k \gg \max\left\{\frac{\log|\mathrm{disc}(\mathbb{K})| - D_{\mathbb{K}}\log D_{\mathbb{K}}}{D_{\mathbb{K}}\log\log|\mathrm{disc}(\mathbb{K})|}, \frac{D_k}{\log\log|\mathrm{disc}(\mathbb{K})|}\right\}$$

$$\gg \max\left\{\frac{\log|\mathrm{disc}(\mathbb{K})|}{D_{\mathbb{K}}\log\log|\mathrm{disc}(\mathbb{K})|}, \frac{D_k}{\log\log D_{\mathbb{K}}}\right\} .$$

(To verify the last inequality, treat separately the cases $\log|\mathrm{disc}(\mathbb{K})| < D^2$ and $\log|\mathrm{disc}(\mathbb{K})| \geq D^2$).

Non-abelian CM fields

Main problem. There are examples of CM fields and of not-root of unities $\alpha \in \mathbb{K}^*$ such that $\hat{h}(\alpha) \ll 1/D_{\mathbb{K}}$. Helpfully we can still obtain a good lower bound for the exponent, modifying the method as follow:

1. The Effective Prime Ideal Theorem gives distinct integral primes ideals $P_1, \ldots, P_n$ such that $P_i \neq \overline{P_j}$ for $i \neq j$ and

$$\log N_{\mathbb{K}/\mathbb{Q}} P_j \ll \log\log|\mathrm{disc}(\mathbb{K})| + \log n \ .$$

2. Let $P_j^{e_{\mathbb{K}}} = (\gamma_j)$ and $\alpha_j = \overline{\gamma_j}/\gamma_j$. Then, by the Main Principle,

$$\hat{h}(\alpha_j) \ll \frac{e_{\mathbb{K}}}{D_{\mathbb{K}}}(\log\log|\mathrm{disc}(\mathbb{K})| + \log n) \ .$$

Moreover $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent.

Height of multiplicatively independent algebraic numbers

Theorem (A. - David, 1999)

Let $\mathbb{K}$ be a field of degree $D_{\mathbb{K}} = [\mathbb{K} : \mathbb{Q}]$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{K}^*$ multiplicatively independent. Then

$$\hat{h}(\alpha_1) \cdots \hat{h}(\alpha_n) \geq D_{\mathbb{K}}^{-1} \big(c(n) \log(3D_{\mathbb{K}})\big)^{-k(n)}$$

In the original paper, $c(n)$ was not computed and $k(n) \approx n^n$. Recently (A.-Viada, Commentarii Math. Helv. 2012 (?)), the proof was radically simplified and the constants $c(n)$, $k(n)$ improved:

$$c(n) = 1050n^5 \qquad k(n) = n^2(n+1)^2 \ .$$

We only need a weaker version of this theorem. Let $\mathbb{K}$ and $\alpha_1, \ldots, \alpha_n$ be as before. Then, for any $\varepsilon > 0$

$$\max\{\hat{h}(\alpha_1), \ldots, \hat{h}(\alpha_n)\} \geq c(n, \varepsilon) D_{\mathbb{K}}^{-1/n-\varepsilon} \ .$$

Non-abelian CM fields

Using this theorem, we obtain:

$$e_{\mathbb{K}} \geq \frac{c'(n,\varepsilon) D_{\mathbb{K}}^{1-1/n-\varepsilon}}{\log\log|\mathrm{disc}(\mathbb{K})| + \log n}$$

for any $\varepsilon > 0$.

Collecting together this last lower bound and the Discriminant Lower Bound for the exponent, we get

$$e_k \gg \max\left\{ \frac{\log|\mathrm{disc}(\mathbb{K})| - D_{\mathbb{K}}\log D_{\mathbb{K}}}{D_{\mathbb{K}}\log\log|\mathrm{disc}(\mathbb{K})|}, \frac{c'(n,\varepsilon) D_{\mathbb{K}}^{1-1/n-\varepsilon}}{\log\log|\mathrm{disc}(\mathbb{K})| + \log n} \right\}$$

$$\gg_{\varepsilon} \max\left\{ \frac{\log|\mathrm{disc}(\mathbb{K})|}{D_{\mathbb{K}}\log\log|\mathrm{disc}(\mathbb{K})|}, D_{\mathbb{K}}^{1-3\varepsilon} \right\} .$$

This conclude the proof of the lower bound for the exponent of the class group of a CM field. For more on the Height Method, see www/math.unicaen.fr/~amoroso/exponent