Lower bounds for the height and class group.

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/exponent

Gauss' class number problem

Let $\Delta < 0$ be a fundamental discriminant :

$$\Delta = \begin{cases} m, & \text{if } m \equiv 1 \mod 4 \\ 4m, & \text{if } m \equiv 2,3 \mod 4 \end{cases}$$

for some square-free integer m.

Define $h(\Delta)$ as the cardinality of the class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{\Delta})$.

In the *Disquisitiones Arithmeticae* (1801) Gauss showed that $h(\Delta) < \infty$. He conjectured that

$$h(\Delta) \to \infty \quad \text{as} \quad \Delta \to -\infty \, .$$

A first non-effective proof of his conjecture follows from the works of Hecke (1929) and Heilbronn (1934).

Gauss' class number problem

More generally, the problem of finding an algorithm to determine all imaginary quadratic fields with a given class number is known as Gauss' class number problem.

It is now completely solved, after an impressive number of papers in the last two centuries.

We only mention that one of the first proof (Baker 1966) of

Theorem (Class Number One Theorem)

$h(\Delta) = 1$ *if and only if*

$$\Delta = -3, -4, -7, -8, -11, -19, -43, -67, -163\ .$$

use, among other things, diophantine methods (e.g. linear forms in logs). For more, see the excellent survey of Goldfeld, Bull. Amer. Math. Soc. **13** (1985), 23-57.

Exponent of the class group of quadratic fields.

Let $e(\Delta)$ be the exponent of the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$, i.e. the least positive integer e s.t. $g^e = 1$ for g in the class group.

Iwasawa : $e(\Delta) \to \infty \quad \text{as} \quad \Delta \to -\infty$?

Boyd-Kisilevsky and Weinberger: connection between this problem and the least prime quadratic residue modulo Δ. They use a diophantine argument:

Lemma

Let $\gamma \in \mathbb{Q}(\sqrt{\Delta})$ be an algebraic integer, $\gamma \notin \mathbb{Z}$. Then its norm $N(\gamma)$ satisfies:

$$|N(\gamma)| \geq |\Delta|/4 \, .$$

Exponent of the class group of quadratic fields.

Lemma

Let $\gamma \in \mathbb{Q}(\sqrt{\Delta})$ be an algebraic integer, $\gamma \notin \mathbb{Z}$. Then its norm $N(\gamma)$ satisfies:

$$|N(\gamma)| \geq |\Delta|/4 \ .$$

Proof. Assume for simplicity $\Delta = 4m$ ($m < 0$, $m \equiv 2, 3 \mod 4$). Then $\gamma = a + b\sqrt{m}$ with a, $b \in \mathbb{Z}$ and $b \neq 0$. Thus

$$N(\gamma) = a^2 + b^2|m| \geq |m| = |\Delta|/4 \ .$$

□

Let p be a prime such that $(\Delta/p) = 1$. Thus p splits in $\mathbb{Q}(\sqrt{\Delta})$. Let P be a prime ideal above p. Then $N(P) = p$ and P^e is a principal ideal, say (γ). Moreover, $\gamma \notin \mathbb{Z}$. Thus, by the lemma above,

$$p \geq (|\Delta|/4)^{1/e(\Delta)} \ .$$

Exponent of the class group of quadratic fields.

Assuming GRH we have

$$p = O(\log^2 \Delta) \ .$$

Combining with the lower bound for p we get a (conditional) positive answer to Iwasawa's problem :

Theorem (Boyd-Kisilevsky, 1972)

Under GRH,

$$e(\Delta) \gg \frac{\log |\Delta|}{\log \log |\Delta|} \ .$$

Class number problem for CM fields

A CM field K is a totally imaginary quadratic extension of a totally real field K^+.

Class number problem for CM fields (Stark):

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

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
- $K^+/\mathbb{Q}$ Galois, or, more generally:

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

  with k_i/k_{i-1} Galois.

Exponent of the class group of CM fields

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

$$e_K \to \infty \quad \text{as} \quad \mathrm{disc}(K) \to +\infty$$

and prove the following generalization of Boyd-Kisilevsky's theorem:

Theorem (Louboutin-Okazaki, 2003)

Assume GRH. Then,

$$e_K \gg_{D_K} \frac{\log|\mathrm{disc}(K)|}{\log\log|\mathrm{disc}(K)|}\,.$$

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

Exponent of the class group of CM fields

In a joint work with Dvornicich, we prove:

Theorem (A.-Dvornicich, 2003)

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

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

It is easily seen that this quantity is $\gg (\log|\mathrm{disc}(K)|)^{(1-\varepsilon)/2}$. 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 new general construction which we summarize as follows:

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

II) Assume the ideal class group of K “small”. Construct algebraic numbers of small Weil's height from prime ideals of small norm.

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

Our 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.

Plan of the next slides

1. Same basic facts on Weil's height.
2. From small norm to small height.
3. Louboutin-Okazaki's revisited.
4. Height in abelian extensions.
5. Exponent of cyclotomic fields and imaginary abelian fields.
6. Height of multiplicatively independent algebraic numbers.
7. Exponent of the class group of CM fields.
8. More results on the size of the class group of CM fields.
9. Other fields. Fields Generated by a Salem number.
10. Annihilator of the ideal class group of cyclotomic fields.

Mahler's measure

Given a non-zero polynomial

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

its Mahler measure is

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

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 Weil height of α is

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

where $\log^+ x = \max(0, \log x)$ for $x > 0$ (and $\log^+ 0 = 0$).

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

  $$\theta \approx 1.3247$$

  and the other two roots of absolute value < 1, i.e. θ is a *Pisot's* number. Thus $\hat{h}(\theta) = \frac{1}{3}\log\theta$.
- The roots of $2x^4 - 3x^2 + 2$ have absolute value 1. Let α one of them. Then $\hat{h}(\alpha) = \frac{\log 2}{4} \approx 0.1732$.

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 $\theta > 1$. All other roots $\neq \theta, \theta^{-1}$ lie on the unit circle, i.e. θ is a *Salem's* number. Thus $M(f) = \theta \approx 1.176$.

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. Kronecker : $M(f) > 1$. Lehmer asks whether there exists an absolute constant $C > 1$ such that $M(f) \geq C$. Record : despite intensive computer's search ... still Lehmer's polynomial!

Conjecture (Lehmer)

Let α be a non-zero algebraic number of degree D which is not a root of unity. Then there exists an absolute constant $c > 0$ such that

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

This should be the best possible lower bound for the height (without any further assumption on α), since $\hat{h}(2^{1/D}) = (\log 2)/D$.

Dobrowolski's theorem

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 α of degree $D \geq 2$ as in Lehmer's conjecture. Here c is an absolute constant. In the original statement $c = 1/1200$; later Voutier shows that one can take $c = 1/4$.

Absolute values

Let K be a field. An absolute value of K is a map $|\cdot|\colon K \to \mathbb{R}$ 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 K.

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

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

Absolute values

Let now K be a number field.

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

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

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

These are (up equivalence) all the absolute values of K. Thus any $v \in \mathcal{M}_K$ is the class of equivalence (with respect to the topology induced) 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 K_v be the completion of K at v. Thus, if $v \mid \infty$, $v = \sigma$, then $[K_v : \mathbb{Q}_v] = 1$ if $\sigma(K) \subset \mathbb{R}$ and or $[K_v : \mathbb{Q}_v] = 2$ otherwise. For $v \nmid \infty$, $v = P$, the degree $[K_v : \mathbb{Q}_v]$ is the product of the ramification index and the inertial degree of P.

For $v \in \mathcal{M}_K$, we choose a normalized absolute values in the class v as:

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

This normalization agrees with the product formula ($\alpha \in K^*$)

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

An other definition of Weil's height

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

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 α is a root of 1.
- $\hat{h}(\alpha) = \hat{h}(\beta)$ if α and β are algebraic conjugates.

A more involved example

Let $K = \mathbb{Q}(\zeta_{21})$ be the 21-th cyclotomic field of degree $\phi(21) = 12$. Let us consider how the prime number 7 splits in the ring of integers of K. Since 7 splits completely in the quadratic imaginary field $\mathbb{Q}(\zeta_3)$ and ramifies in $\mathbb{Q}(\zeta_7)$, we have

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

where P is a prime of norm $N_{K/Q}(P) = 7$. Since K is one of the twenty-nine cyclotomic fields of class number one, $P = (\gamma)$ for some integer $\gamma \in K$. Let $\alpha = \overline{\gamma}/\gamma$. Since K is a CM field, $|\alpha|_v = 1$ for $v \mid \infty$. We have

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

Thus, if $v \nmid \infty$,

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

A more involved example

We deduce that

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

The minimal polynomial of α over $\mathbb{Z}$ is $f(x) = 7x^{12} - 13x^6 + 7$.

We can check the computation above of $\hat{h}(\alpha)$ by observing that all the roots of f lie on the unit circle. Thus $M(f) = 7$ and again $\hat{h}(\alpha) = \frac{\log 7}{12}$.

We come back to α later when we discuss lower bounds for the height in abelian fields.

For the moment, we are interested in generalizations of the construction above in more general CM fields.

The Main Principle

Proposition (Main Principle)

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

1. $\hat{h}(\alpha) = \frac{e_K}{D_K} \log N_{K/\mathbb{Q}} P > 0$
2. $K = \mathbb{Q}(\alpha)$

The Main Principle

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

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

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

Thus

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

□

Effective Prime Ideal Theorem

Let 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 K, then there exists distinct integral prime ideals $P_1, \dots, P_n$ of degree 1, non-ramified over $\mathbb{Q}$, and such that

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

This result is the (fundamental) contribution from Analytic Number Theory to the Height Method. In what follows, we tacitly assume GRH.

A first bound for the height

Proposition (Discriminant Lower Bound for the height)

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

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

Proof. A proof follows combining results of Mahler and Simon. Let $f(x) = f_D \prod_{j=1}^{D}(x - \alpha_j) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Define

$$\mathrm{disc}(\alpha) = (-1)^{D(D-1)/2} \left(f_D^{D-1} \det(\alpha_i^{j-1}) \right)^2 \in \mathbb{Z} \, .$$

Then $|\mathrm{disc}(K)| \leq |\mathrm{disc}(\alpha)|$, even for non integer α (Simon, 2002). Mahler (1964) provides an upper bound for $|\mathrm{disc}(\alpha)|$. Let us quickly sketch his proof.

A first bound for the height

By Hadamard's inequality,

$$
\begin{aligned}
|\det(\alpha_i^{j-1})| &\leq \prod_{i=1}^{D} \sqrt{1+|\alpha_i|^2+\cdots+|\alpha_i^{D-1}|^2} \\
&\leq D^{D/2} \prod_{i=1}^{D} \max\{1,|\alpha_i|\}^{D-1} \; .
\end{aligned}
$$

Thus

$$
|\mathrm{disc}(\alpha)| \leq D^D |f_D|^{2(D-1)} \prod_{i=1}^{D} \max\{1,|\alpha_j|\}^{2(D-1)} = D^D M(f)^{2(D-1)} \; .
$$

Combining the two inequalities for $\mathrm{disc}(\alpha)$ we get

$$
\log|\mathrm{disc}(K)| \leq D\log D + (2D-2)\log M(f) = D\log D + 2(D-1)D\hat{h}(\alpha) \; .
$$

□

Louboutin-Okazaki revisited

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

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

Thus

Proposition (Discriminant Lower Bound for the exponent)

In a CM field

$$e_K \gg \frac{\log|\mathrm{disc}(K)| - D_K \log D_K}{D_K \log\log|\mathrm{disc}(K)|} .$$

This implies Louboutin-Okazaki's result

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

Cyclotomic extensions

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

$$\hat{h}(\alpha) \ll \frac{e_K}{D_K} \log\log|\mathrm{disc}(K)|$$

gives only

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

which tends to zero !

Let $m \in \mathbb{N}$, $m \not\equiv 2 \mod 4$. Consider the m-th cyclotomic field $K_m = \mathbb{Q}(\zeta_m)$ of degree $\phi(m)$.

Cyclotomic extensions

Then

$$\log|\mathrm{disc}(K_m)| \sim \phi(m)\log m$$

as $m \to +\infty$. Thus the Discriminant Lower Bound for the exponent gives no information. This is natural, since $\hat{h}(\zeta_m) = 0$!

Helpfully, in a cyclotomic extension much more than Lehmer is known:

Theorem (A.-Dvornicich, 2000)

For any $\alpha \in K_m^*$ which is not a root of unity we have

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

By Kronecker-Weber theorem, this lower bound for the height holds in an arbitrary abelian extension.

More on height in cyclotomic extension

Is the bound $\hat{h}(\alpha) \geq \frac{\log 5}{12} = 0.134\ldots$ sharp? Recall that the roots $\alpha \in K_{21}$ of $7x^{12} - 13x^6 + 7$ satisfy $\hat{h}(\alpha) = \frac{\log 7}{12} = 0.166\ldots$. It seems quite likely that this should be the correct lower bound.

Let $\alpha \in K_m$, not a root of unity. We have more precise lower bounds depending on m. For instance,

$$\hat{h}(\alpha) \geq \begin{cases} \log(7/2)/8 = 0.156\ldots, & \text{if } 7 \nmid m; \\ \log(5/2)/6 = 0.152\ldots, & \text{if } 7 \mid m \text{ and } 5 \nmid m; \\ \log(11/2)/12 = 0.142\ldots, & \text{if } 35 \mid m \text{ and } 11 \nmid m\ . \end{cases}$$

Ishak-Mossinghoff-Pinner-Wiles (2010) prove several refined bounds. For example,

$$\hat{h}(\alpha) \geq 0.155\ldots\ .$$

Moreover, they show that $\hat{h}(\alpha) < \frac{\log 7}{12}$ implies $35 \mid m$.

Sketch of the proof of the abelian lower bound

Let $\alpha \in K_m^*$ not a root of unity. Since Weil's height is invariant by multiplication by roots of unities, we may assume that $\forall \zeta$ root of unity, $\forall n < m$ we have $\zeta\alpha \notin K_n$. 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 lower bound $\hat{h}(\alpha) \geq \log(5/2)/10 = 0.039\ldots$.

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

$$\gamma^p \equiv f(\zeta_m^p) \equiv f(\sigma\zeta_m) \equiv \sigma\gamma \pmod p.$$

Let fix a $v \in \mathcal{M}_K$ dividing p. Thus $|\gamma^p - \sigma\gamma|_v \leq 1/p$ for any integer $\gamma \in K_m$. By the Strong Approximation Theorem, there exists an algebraic integer $\beta = \beta_v \in K$ such that $\alpha\beta$ is integer and $|\beta|_v = \max\{1, |\alpha|_v\}^{-1}$. Thus

Sketch of the proof of the abelian lower bound

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

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. Thus, applying the product formula to $\alpha^p - \sigma\alpha$,

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

Sketch of the proof of the abelian lower bound

Assume now that $p|m$. Let σ be a generator of $\mathrm{Gal}(K_m/K_{m/p})$. We have $\sigma\zeta_m = \zeta_p\zeta_m$ for some primitive p-root of unity ζ_p. Thus, for any integer $\gamma = f(\zeta_m) \in \mathbb{Z}[\zeta_m]$

$$\gamma^p \equiv f(\zeta_m^p) \equiv f(\sigma\zeta_m^p) \equiv \sigma\gamma^p \pmod p$$

i.e. $|\gamma^p - \sigma\gamma^p|_v \leq 1/p$ for any $v \in \mathcal{M}_K$ dividing p. Using the Strong Approximation Theorem and the Product Formula 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 $\sigma\alpha^p = \alpha^p$. Then $\sigma\alpha = \zeta_p^u\alpha$ for some integer u. It follows that $\sigma(\alpha/\zeta_m^u) = \alpha/\zeta_m^u$, hence $\alpha/\zeta_m^u \in K_{m/p} \subsetneq K_m$, which contradict the minimal property of α. Applying the product formula to $\alpha^p - \sigma\alpha^p \neq 0$, we obtain again

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

□

Exponent of the class group of a cyclotomic extension

In a cyclotomic extension K_m we do not need GRH for a lower bound for the exponent e_m. Let $p(m,1)$ be the smallest prime satisfying $p \equiv 1 \mod m$. By Linnik's theorem $p(m,1) \leq m^L$, where $L > 0$ is an effective constant. It is well known that $p(m,1)$ splits completely in K_m.

Recall:

Proposition (Main Principle)

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

1. $\hat{h}(\alpha) = \frac{e_K}{D_K} \log N_{K/\mathbb{Q}} P > 0$
2. $K = \mathbb{Q}(\alpha)$

Exponent of the class group of a cyclotomic extension

In a cyclotomic extension K_m we do not need GRH for a lower bound for the exponent e_m. Let $p(m,1)$ be the smallest prime satisfying $p \equiv 1 \mod m$. By Linnik's theorem $p(m,1) \leq m^L$, where $L > 0$ is an effective constant. It is well known that $p(m,1)$ splits completely in K_m.

Thus, there exists a not-root of unity $\alpha \in K^*$ such that

$$\hat{h}(\alpha) = \frac{e_m \log p(m,1)}{\phi(m)} \leq \frac{e_m L \log m}{\phi(m)} .$$

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

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

Masley-Montgomery revised

A bound of the shape

$$\log p(m, 1) = o(\phi(m))$$

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 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 K_m has class number 1. We have (McCurley, 1984)

$$\log p(m,1) \leq 15.08 \log^2 m \quad \text{for} \quad m \geq 10^4 .$$

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 $p(m,1)$ 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 imaginary abelian extensions

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

$$\hat{h}(\alpha) \ll \frac{e_K}{D_K} \log\log|\mathrm{disc}(K)| \; .$$

Assume K abelian. By Kronecker-Weber's theorem K is contained in a cyclotomic extension. Thus, by A.-Dvornicich lower bound:

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

We obtain

$$e_K \gg \frac{D_k}{\log\log|\mathrm{disc}(K)|} \; .$$

Exponent of imaginary abelian extensions

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

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

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

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

Non-abelian CM fields

Main problem. There are examples of CM fields and of not-root of unities $\alpha \in K^*$ such that $\hat{h}(\alpha) \ll 1/D_K$. 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 $P_1, \dots, P_n$ such that $P_i \neq \overline{P_j}$ for $i \neq j$ and
$$\log N_{K/\mathbb{Q}} P_j \ll \log |\mathrm{disc}(K)| + \log n \ .$$
2. Let $P_j^{e_K} = (\gamma_j)$ and $\alpha_j = \overline{\gamma_j}/\gamma_j$. Then, by the Main Principle,
$$\hat{h}(\alpha_j) \ll \frac{e_K}{D_K}(\log \log |\mathrm{disc}(K)| + \log n) \ .$$
Moreover $\alpha_1, \dots, \alpha_n$ are multiplicatively independent.

Height of multiplicatively independent algebraic numbers

Theorem (A. - David, 1999)

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

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

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 K and $\alpha_1, \dots, \alpha_n$ be as before. Then, for any $\varepsilon > 0$

$$\max\{\hat{h}(\alpha_1), \dots, \hat{h}(\alpha_n)\} \geq c(n, \varepsilon) D_K^{-1/n - \varepsilon} .$$

Non-abelian CM fields

Using this theorem, we obtain:

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

for any $\varepsilon > 0$.

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

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

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

This conclude the proof of the lower bound for the exponent of the class group of a CM field.

More on class group of CM fields

Let again K a CM field and let K^+ its maximal real subfield. An inspection of the previous proof shows that the Height Method gives a lower bound for e_K^-, i.e. for the last positive integer e such that for all fractional ideal I of K there exists $\gamma \in K^+$ such that $(\gamma)I^e$ is the extension of a fractional ideal of K^+.

Consider the ideal extension $j\colon \mathcal{C}l(K^+) \to \mathcal{C}l(K)$.Thus e_K^- is the exponent of the abelian group $\mathcal{C}l(K)/j\mathcal{C}l(K^+)$. The Height Method provides even more informations on the abelian structure of this group.

A combinatorial function

Let G a finite abelian group and $l \geq 1$ an integer. Define $S(G;l)$ as the least positive integer A such that all $g_1, \ldots, g_l \in G$ satisfy a non-trivial multiplicative relation of length $\leq A$, i.e. there exist $\rho_1, \ldots, \rho_l \in \mathbb{Z}$ such that :

1. $(\rho_1, \ldots, \rho_l) \neq (0, \ldots, 0)$
2. $g_1^{\rho_1} \cdots g_l^{\rho_l} = 1$
3. $\sum_j |\rho_j| \leq A$.

We have

$$S(G;1) = e_G \quad \text{et} \quad S(G;|G|) \leq 2$$

More generally, $S(G;l)$ gives informations on the "size" of G. For instance, let $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{N}$ be the invariants of G, i.e. $\lambda_n \mid \lambda_{n-1} \mid \cdots \mid \lambda_1$ and G is isomorphic to the direct product of cyclic groups of order $\lambda_1, \lambda_2, \ldots, \lambda_n$. Then

$$S(G; \lambda_1 \ldots \lambda_{j-1}/\lambda_j^{j-1}) \leq 2\lambda_j \ .$$

An extension of the Main Principle

The Height Method can be extended to get lower bounds for $S(\mathcal{C}l(K)/j\mathcal{C}l(K^+);l)$. Let $l \geq 1$ and $A = S(\mathcal{C}l(K)/j\mathcal{C}l(K^+);l)$. Let $P_1, \dots, P_l$ be distinct integral prime ideals of norm $\leq N$ and such that $P_i \neq \overline{P_j}$ for $i \neq j$. By the choice of A, there exists $\rho_1, \dots, \rho_l \in \mathbb{Z}$ with $\sum_j |\rho_j| \leq A$ and $\gamma \in K$ such that

$$P_1^{\rho_1} \cdots P_l^{\rho_l} = (\gamma) I$$

where I is the extension of a fractional ideal of K^+. A generalization of the Main Principle shows that $\alpha = \overline{\gamma}/\gamma$ has height

$$\hat{h}(\alpha) = \frac{A \log N}{D_K}$$

Size of the class group of CM fields

Using suitable versions of this generalization of the Main Principle, we obtain:

Theorem

Let $K/\mathbb{Q}$ be a CM field. Let $l \in \mathbb{N}$ and $\varepsilon > 0$. Then,

$$S(\mathcal{C}l(K)/j\mathcal{C}l(K^+); l) \gg_\varepsilon \frac{\max\left\{D_K^{-1}\log|\mathrm{disc}(K)|, D_K^{1-\varepsilon}\right\}}{\log\log|\mathrm{disc}(K)| + \log l}.$$

Moreover, if $K/\mathbb{Q}$ is abelian, then the conclusion holds also for $\varepsilon = 0$.

Class number

This gives "good" (conditional) lower bounds for the class number of a CM field:

Corollary

Let $\varepsilon \in (0,1/2)$*; then,*

$$\frac{h_K}{h_{K^+}} \geq \exp\left\{C(\varepsilon)\max\left\{D_K^{-1}\log|\mathrm{disc}(K)|, D_K^{1-\varepsilon}\right\}\right\}.$$

which are already known by classical methods ...

Class group structure

... and more new informations on the invariants of $\mathcal{C}l(K)/j\mathcal{C}l(K^+)$.

For instance, assume $\mathcal{C}l(K)/j\mathcal{C}l(K^+)$ isomorphic to the direct product of a cyclic group of order e and and an abelian group G of bounded exponent:

$$\mathcal{C}l(K)/j\mathcal{C}l(K^+) \cong \mathbb{Z}/e\mathbb{Z} \times G, \qquad e_G \ll 1 \,.$$

The lower bound for the exponent gives

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

while the finest result on $S(\mathcal{C}l(K)/j\mathcal{C}l(K^+); l)$ provides the bound

$$\log e \gg_\varepsilon \max\left\{ D_K^{-1} \log|\mathrm{disc}(K)|, D_K^{1-\varepsilon} \right\} \,.$$

Salem numbers again

The main problem in extending the Height Method to other fields is in the generalization of the Main Principle. We shall use elementary geometry of numbers to extend the construction of algebraic numbers of small Weil's height from prime ideals of small norm. In general, as we shall see later, these construction yields result only for fixed degree. But for fields generated by an algebraic number having only few conjugates outside the unit circle, we recover statements very similar to whose of CM fields. We born ourself to lower bound for the exponent of the class group of a field generated by a Salem number. We recall that a Salem number θ is an algebraic number > 1 such that θ^{-1} is an algebraic conjugate of θ and the others conjugates of θ lie on the unit circle.

Class number of Salem fields

We denote by T the set of Salem numbers. Chinburg (1984) proves the following analogous of Stark-Odlyzko's result for CM field.

Theorem

Let

$$H=\liminf_{\theta\in T}\left(\frac{h(\mathbb{Q}(\theta))\log\theta)}{h(\mathbb{Q}(\theta+\theta^{-1})}\right)^{1/[\mathbb{Q}(\theta):\mathbb{Q}]}\qquad .$$

Then, under GRH or Artin's conjecture on L-functions, $H>1$. Moreover, let H_0 the $\liminf$ *of the same quantity as for H, but now over the set of $\theta\in T$ such that there exists a tower of estension*

$$\mathbb{Q}=k_0\subset k_1\subset\cdots\subset k_t=\mathbb{Q}(\theta)$$

with k_i/k_{i-1} Galois. Then $H_0>1$.

Exponent of Salem fields

Let $\theta \in T$, $K = \mathbb{Q}(\theta)$ and $K^+ = \mathbb{Q}(\theta + \theta^{-1})$. Let also, as for CM fields, e_K^- be the exponent of $\mathcal{C}l(K)/j\mathcal{C}l(K^+)$.

Theorem (A.)

Assume GRH. Then for any $\varepsilon > 0$,

$$e_K^- \gg_\varepsilon \frac{\max(D_K^{-1} \log|\mathrm{disc}(K)|, D_K^{1-\varepsilon})}{\log\log|\mathrm{disc}(K)| + \log(\log\theta + 2)} .$$

Sketch of the proof. Let τ be the $\mathbb{Q}$-automorphism of K defined by $\theta \mapsto \theta^{-1}$.

Exponent of Salem fields

The Effective Prime Ideal Theorem gives $n \geq 2$ distinct integral prime ideals P_j of norm $\log N_{K/\mathbb{Q}} P_j \ll \log\log |\mathrm{disc}(K)| + \log n$. Write $P_j^{e_K} = (\gamma_j)$ and $\alpha_j = \gamma_j^{\tau - 1}$. We can assume γ_j real. Choose integers m_j such that

$$1 < \theta^{m_j} \alpha_j \leq \theta \, .$$

The box principle provides indexes $i \neq j$ such that $\alpha = \theta^{m_i - m_j} \alpha_i / \alpha_j$ satisfies

$$\theta^{-1/n} < |\alpha| < \theta^{1/n} \, . \qquad (*)$$

Let $v \in \mathcal{M}_K$ be a non-real archimedean place. Fix j. Write $\gamma_j = f(\theta)$ with $f \in \mathbb{Q}[x]$. Let $\sigma \colon K \to \mathbb{C}$ the embedding corresponding to v. Then $\sigma(\theta^\tau) = \overline{\sigma(\theta)}$. Thus $|\alpha_j|_v = |\sigma(\gamma^{\tau-1})|$ $= |\overline{f(\theta)}/f(\theta)| = 1$. Since $|\theta|_v = 1$ we also have $|\alpha|_v = 1$.

Exponent of Salem fields

If $v \nmid \infty$,

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

Let v_1, v_2 be the real places of K. By the product formula, $|\alpha|_{v_1}|\alpha|_{v_2} = 1$. By (*) $\log^+|\alpha|_{v_1} + \log^+|\alpha|_{v_2} \leq \frac{\log\theta}{n}$. We get:

$$D_K\hat{h}(\alpha) = \sum_{v\in\mathcal{M}_K}[K_v:\mathbb{Q}_v]\log^+|\alpha|_v \leq e_K\log N_{K/\mathbb{Q}}P + \frac{\log\theta}{n}$$

$$\ll e_K(\log\log|\mathrm{disc}(K)| + \log n) + \frac{\log\theta}{n}\ .$$

Exponent of Salem fields. Other fields.

Optimizing in n, we get

$$\hat{h}(\alpha) \ll \frac{e_K}{D_K}\left(\log\log|\mathrm{disc}(K)| + \log\frac{\log\theta}{e_K}\right) .$$

Using at this point lower bounds for the height, we obtain the announced result (with e_K instead of e_K^-), at least if $K/\mathbb{Q}$ is abelian. If $K/\mathbb{Q}$ is not abelian, we have to construct in a similar way more multiplicatively independent algebraic numbers of small height.

□

Other fields.

For arbitrary number fields, we must use the geometry of numbers in a space of dimension $\approx D_K$. This give a worst dependence in the degree, as we explain below. Let

- r be the rank of the unit group E_K
- δ be the minimum of the sum of the height of a system of generators of $E_K/(E_K)_{\mathrm{tors}}$

This quantities are of course related to the regulator:

$$\mathrm{reg}(K) \leq (4\delta)^r \qquad \text{and} \qquad \delta \leq 158 r!\, r^{3/2} (\log D_K)\, \mathrm{reg}(K)\ ,$$

Box Principle

The Effective Prime Ideal Theorem gives $n \geq 2$ distinct integral prime ideals P_j of norm $\log N_{K/\mathbb{Q}} P_j \ll \log\log|\mathrm{disc}(K)| + \log n$. Write $P_j^{e_K} = (\gamma_j)$. The box principle provides a unit u and indexes $i \neq j$ such that $\alpha = u\gamma_i/\gamma_j$ has height

$$\hat{h}(\alpha) \leq \frac{e_K(\log\log|\mathrm{disc}(K)| + \log n)}{D_K} + \frac{\delta}{n^{1/r} - 1} \, .$$

Optimizing in n, we get

$$\hat{h}(\alpha) \ll \frac{e_K}{D_K}\left(\log\log|\mathrm{disc}(K)| + r\log\frac{\delta D_K}{e_K}\right) \, .$$

Unfortunately, $r \geq D_K/2$, so that the r.h.s is $\geq e_K \log(\delta D_K/e_K)/2$. Thus, even a bound $\hat{h}(\alpha) \geq$ constant is not useful here.

A “Brauer-Siegel” bound for the exponent

Nevertheless, using the Discriminant Lower Bound for the height

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

we still obtain a result for fixed degree, which is an analogous of Brauer-Siegel theorem $h_K \mathrm{reg}(K) \gg_{D_K} |\Delta_K|^{1/2-\varepsilon}$.

Theorem (A.)

Let K be a field. Then,

$$e_K \gg_{D_K} \frac{\log|\mathrm{disc}(K)|}{\log\log|\mathrm{disc}(K)| + \log \mathrm{reg}(K)} .$$

Ankeny-Brauer-Chowla for the exponent

Ankeny, Brauer and Chowla (1956) construct an infinite family of number fields K of fixed signature $\mathbf{r} = (r_1, r_2)$ and such that $h_K \gg_{\mathbf{r}} |\mathrm{disc}(K)|^{1/2-\varepsilon}$.

Several authors consider the analogous question for the exponent. They construct families of number fields K of fixed small degree such that,

$$e_K \gg_{D_K} \frac{\log |\mathrm{disc}(K)|}{\log \log |\mathrm{disc}(K)|} .$$

For instance:

- Murty (1998) shows that the exponents of the class groups of $\mathbb{Q}(\sqrt{m^2+1})$ satisfy this inequality.
- Louboutin (1997, 2001, 2002) shows the same for infinite families of cubic fields.

Ankeny-Brauer-Chowla for the exponent

Our result allow us to generalize these constructions, showing an analogue of Ankeny-Brauer-Chowla result for the exponent.

Corollary

For any signature $\mathbf{r} = (r_1, r_2)$ *there exists an infinite family of pairwise non-isomorphic number fields* K *of signature* $\mathbf{r}$*, such that*

$$e_K \gg_{\mathbf{r}} \frac{\log |\mathrm{disc}(K)|}{\log \log |\mathrm{disc}(K)|} .$$

Cyclotomic fields again

For a natural number $m \not\equiv 2 \mod 4$, let

- ζ_m a primitive m-root of unity
- $K_m = \mathbb{Q}(\zeta_m)$ and $\phi(m) = [K_m : \mathbb{Q}]$
- $\sigma_a \colon \zeta_m \mapsto \zeta_m^a$, for $\gcd(a, m) = 1$
- $\Gamma_m = \mathrm{Gal}(K_m/\mathbb{Q}) = \{\sigma_a \mid \gcd(a, m) = 1\}$
- $J = \sigma_{-1}$ be the complex conjugation
- $\mathcal{C}l_m^- = \mathcal{C}l(K_m)/\mathcal{C}l(K_m^+)$
- $\mathrm{Ann}(\mathcal{C}l_m^-)$ the annihilator of $\mathcal{C}l_m^-$ in the group ring $\mathbb{Z}[\Gamma_m]$

Size of elements in $\mathrm{Ann}(\mathcal{C}l_m^-)$

For

$$\psi = \sum_{\substack{1 \le a \le m-1 \\ \gcd(a,m)=1}} \psi_a \sigma_a \in \mathbb{Z}[\Gamma_m] \; ;$$

let $\|\psi\|_1 = \sum_a |\psi_a|$. The following result generalizes the lower bound for the exponent in a cyclotomic field.

Theorem (A.)

Let $\psi \in \mathrm{Ann}(\mathcal{C}l_m^-)$ and assume $(1-J)\psi \neq 0$. Then

$$\|\psi\|_1 \geq \frac{\log 5}{12L} \times \frac{\phi(m)}{\log m} \; ,$$

where L is Linnik's constant.

Size of elements in $\mathrm{Ann}(\mathcal{C}l_m^-)$

Proof. We generalize (again!) the Main Principle. Let

$$\psi = \sum_{\substack{1\le a\le m-1\\ \gcd(a,m)=1}} \psi_a\sigma_a \in \mathrm{Ann}(\mathcal{C}l_m^-)$$

such that $(1-J)\psi \neq 0$. Linnik's theorem gives a prime number $p \le m^L$ such that $p \equiv 1 \mod m$. This prime splits completely in $\mathbb{Z}[\zeta_m]$; let $P \subseteq \mathbb{Z}[\zeta_m]$ be a prime ideal over p. Then

$$P^\psi = (\gamma)I$$

for some $\gamma \in K_m^*$ and for a fractional ideal I which is an extension of a fractional ideal of K_m^+. Let $\alpha = \gamma^{1-J}$. Then

$$(\alpha) = (\gamma)^{1-J} = \prod_{\substack{1\le a\le m-1\\ \gcd(a,m)=1}} (\sigma_a P)^{\psi_a - \psi_{m-a}}$$

Size of elements in $\mathrm{Ann}(\mathcal{C}l_m^-)$

For the place v_a of K_m corresponding to the prime $(\sigma_a P)$ we have

$$|\alpha|_{v_a}^{[(K_m)_{v_a}:\mathbb{Q}_p]} = p^{\psi_{m-a}-\psi_a}.$$

For all the other places, $|\alpha|_v = 1$. Therefore,

$$\begin{aligned} \phi(m)\hat{h}(\alpha) &= \frac{\log p}{2} \sum_{\substack{1\leq a\leq m-1 \\ \gcd(a,m)=1}} |\psi_a - \psi_{m-a}| \\ &\leq L(\log m)\|\psi\|_1 \ . \end{aligned}$$

Remark that α is not a root of unity, since $(1-J)\psi \neq 0$ implies $P^{(1-J)\psi} \neq \mathbb{Z}[\zeta_m]$. Using A.-Dvornicich lower bound $\hat{h}(\alpha) \geq \frac{\log 5}{12}$ we get the desired conclusion. □

Index of the annihilator

Let

$$\mathbb{Z}[\Gamma_m]^- = \{\psi \in \mathbb{Z}[\Gamma_m] \mid (1+J)\psi = 0\} = (1-J)\mathbb{Z}[\Gamma_m]$$

and $\mathrm{Ann}(\mathcal{C}l_m^-)^- = \mathrm{Ann}(\mathcal{C}l_m^-) \cap \mathbb{Z}[\Gamma_m]^-$.

Question

What can we say on $\left[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}(\mathcal{C}l_m^-)^-\right]$ *?*

Let

$$\theta_m = \sum_{\substack{0 \le a < m \\ (a,m)=1}} \{a/m\}\sigma_a^{-1} \in \mathbb{Q}[\Gamma_m],$$

where $\{x\}$ denotes the fractional part. We consider the Stickelberger ideal $I_m = \mathbb{Z}[\Gamma_m] \cap \theta_m\mathbb{Z}[\Gamma_m]$ and its minus part $I_m^- = I_m \cap \mathbb{Z}[\Gamma_m]^-$ its minus part. Then (Stickelberger's theorem)

$$I_m^- \subseteq \mathrm{Ann}(\mathcal{C}l_m^-)^- \ .$$

Index of the annihilator

Sinnott proves:

$$\left[\mathbb{Z}[\Gamma_m]^- : I_m^-\right] = 2^{a(m)} h_m^-,$$

where $a(m) = 0$ if m is a prime power and $a(m) = 2^{k-2} - 1$ if m has $k \geq 2$ distinct prime factors. Since $\log h_m^- \sim \frac{1}{4}\phi(m)\log m$, for $m \to +\infty$ and since $a(m) = o(\phi(m)\log m)$,

$$\log\left[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}(\mathcal{C}l_m^-)^-\right] \leq \log\left[\mathbb{Z}[\Gamma_m]^- : I_m^-\right] \sim \frac{1}{4}\phi(m)\log m.$$

Our last theorem implies an inequality in the opposite direction:

Corollary

$$\log\left[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}(\mathcal{C}l_m^-)^-\right] \gg \frac{\phi(m)\log\log m}{\log m}.$$

Unfortunately, this gives no nontrivial upper bounds for $[\mathrm{Ann}(\mathcal{C}l_m^-)^- : I_m^-]$, since the RHS is $o(\phi(m)\log m)$.

Index of the annihilator

Proof of corollary. Let $c = \frac{\log 5}{12L}$ and $n = \frac{c\phi(m)}{4\log m}$. The set

$$\Lambda_m = \left\{ \psi = \sum_{\substack{1\leq a\leq (m-1)/2 \\ \gcd(a,m)=1}} \psi_a \sigma_a \in \mathbb{Z}[\Gamma_m] \;\middle|\; \psi_a \geq 0,\ \|\psi\|_1 \leq [n] \right\}$$

has cardinality

$$\binom{\phi(m)/2 + [n]}{[n]} \geq \left(\frac{\phi(m)/2}{n}\right)^{n-1} \geq \left(\frac{2\log m}{c}\right)^{\frac{c\phi(m)}{4\log m}-1} .$$

Since $(1-J)^2 = 2$, the map $\psi \mapsto (1-J)\psi$ is injective. Thus

$$\mathrm{Card}((1-J)\Lambda_m) = \mathrm{Card}(\Lambda_m) .$$

Index of the annihilator

Let ψ and ψ' two distinct elements of $(1-J)\Lambda_m$. Then $(1-J)(\psi-\psi') = 2(\psi-\psi') \neq 0$ and

$$\|\psi-\psi'\|_1 \leq 4[n] < \frac{c\phi(m)}{\log m}.$$

By the theorem, $\psi-\psi' \notin \mathrm{Ann}(\mathcal{C}l_m^-)$. Thus

$$\left[\mathbb{Z}[\Gamma_m]^- : \mathrm{Ann}(\mathcal{C}l_m^-)^-\right] \geq \mathrm{Card}((1-J)\Lambda_m) = \mathrm{Card}(\Lambda_m)$$

$$\geq \left(\frac{2\log m}{c}\right)^{\frac{c\phi(m)}{4\log m}-1}.$$

$\square$