Checking the Brumer-Stark conjecture using PARI/GP

Xavier-François Roblot

IGD, Université Claude Bernard – Lyon 1

September 16th, 2004

- k is a number field of degree n
- K is a finite abelian extension over k
- $G := \mathrm{Gal}(K/k)$
- w_K is the number of roots of unity in K
- Cl_K is the class group of K
- S is the set of the infinite primes of k and of the finite prime ideals in k that ramify in K
- For each $\sigma \in G$, the partial zeta-function is

$$\zeta_S(s, \sigma) := \sum_{\substack{(\mathfrak{a}, S)=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \frac{1}{\mathcal{N}\mathfrak{a}^s}$$

- k is a number field of degree n
- K is a finite abelian extension over k
- $G := \mathrm{Gal}(K/k)$
- w_K is the number of roots of unity in K
- Cl_K is the class group of K
- S is the set of the infinite primes of k and of the finite prime ideals in k that ramify in K
- For each $\sigma \in G$, the partial zeta-function is

$$\zeta_S(s,\sigma) := \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \frac{1}{\mathcal{N}\mathfrak{a}^s}$$

- k is a number field of degree n
- K is a finite abelian extension over k
- $G := \mathrm{Gal}(K/k)$
- w_K is the number of roots of unity in K
- Cl_K is the class group of K
- S is the set of the infinite primes of k and of the finite prime ideals in k that ramify in K
- For each $\sigma \in G$, the partial zeta-function is

$$\zeta_S(s,\sigma) := \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \frac{1}{\mathcal{N}\mathfrak{a}^s}$$

- k is a number field of degree n
- K is a finite abelian extension over k
- $G := \mathrm{Gal}(K/k)$
- w_K is the number of roots of unity in K
- Cl_K is the class group of K
- S is the set of the infinite primes of k and of the finite prime ideals in k that ramify in K
- For each $\sigma \in G$, the partial zeta-function is

$$\zeta_S(s, \sigma) := \sum_{\substack{(\mathfrak{a}, S)=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \frac{1}{\mathcal{N}\mathfrak{a}^s}$$

- k is a number field of degree n
- K is a finite abelian extension over k
- $G := \mathrm{Gal}(K/k)$
- w_K is the number of roots of unity in K
- Cl_K is the class group of K
- S is the set of the infinite primes of k and of the finite prime ideals in k that ramify in K
- For each $\sigma \in G$, the partial zeta-function is

$$\zeta_S(s,\sigma) := \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma_{\mathfrak{a}}=\sigma}} \frac{1}{\mathcal{N}\mathfrak{a}^s}$$

Theorem (Deligne and Ribet, Barsky, and Pi. Cassou-Noguès)

For every $\sigma \in G$

$$w_K \, \zeta_S(0, \sigma) \in \mathbb{Z}$$

The *Brumer element* is the element of the group ring $\mathbb{Z}[G]$ defined by

$$\gamma := w_K \sum_{\sigma \in G} \zeta_S(0, \sigma) \sigma^{-1}$$

Theorem (Deligne and Ribet, Barsky, and Pi. Cassou-Noguès)

For every $\sigma \in G$

$$w_K \, \zeta_S(0, \sigma) \in \mathbb{Z}$$

The *Brumer element* is the element of the group ring $\mathbb{Z}[G]$ defined by

$$\gamma := w_K \sum_{\sigma \in G} \zeta_S(0, \sigma)\sigma^{-1}$$

The Brumer-Stark Conjecture

Conjecture (The Brumer part)

The element γ kills Cl_K.
That is, for every fractional ideal $\mathfrak{A}$ of K, the ideal $\mathfrak{A}^\gamma$ is principal.

Let K° be the set of *anti-units* of K

$$K^\circ := \{x \in K : |x|_{\mathfrak{P}_\infty} = 1,\ \forall \mathfrak{P}_\infty \mid \infty\}$$

Conjecture (The Stark part)

For every fractional ideal $\mathfrak{A}$ of K, there exists a generator $\alpha_{\mathfrak{A}}$ of $\mathfrak{A}^\gamma$ that is an anti-unit. Furthermore, define $\lambda_{\mathfrak{A}} \in \overline{K}$ by $\lambda_{\mathfrak{A}}^{W_K} = \alpha_{\mathfrak{A}}$, then $K(\lambda_{\mathfrak{A}})/k$ is an abelian extension.

The Brumer-Stark Conjecture

Conjecture (The Brumer part)

The element γ kills Cl_K.
That is, for every fractional ideal $\mathfrak{A}$ of K, the ideal $\mathfrak{A}^\gamma$ is principal.

Let K° be the set of *anti-units* of K

$$K^\circ := \{x \in K : |x|_{\mathfrak{P}_\infty} = 1,\ \forall \mathfrak{P}_\infty \mid \infty\}$$

Conjecture (The Stark part)

For every fractional ideal $\mathfrak{A}$ of K, there exists a generator $\alpha_{\mathfrak{A}}$ of $\mathfrak{A}^\gamma$ that is an anti-unit. Furthermore, define $\lambda_{\mathfrak{A}} \in \overline{K}$ by $\lambda_{\mathfrak{A}}^{W_K} = \alpha_{\mathfrak{A}}$, then $K(\lambda_{\mathfrak{A}})/k$ is an abelian extension.

The Brumer-Stark Conjecture

Conjecture (The Brumer part)

The element γ kills Cl_K.
That is, for every fractional ideal $\mathfrak{A}$ of K, the ideal $\mathfrak{A}^\gamma$ is principal.

Let K° be the set of *anti-units* of K

$$K^\circ := \{x \in K : |x|_{\mathfrak{P}_\infty} = 1,\ \forall \mathfrak{P}_\infty \mid \infty\}$$

Conjecture (The Stark part)

For every fractional ideal $\mathfrak{A}$ of K, there exists a generator $\alpha_{\mathfrak{A}}$ of $\mathfrak{A}^\gamma$ that is an anti-unit. Furthermore, define $\lambda_{\mathfrak{A}} \in \overline{K}$ by $\lambda_{\mathfrak{A}}^{W_K} = \alpha_{\mathfrak{A}}$, then $K(\lambda_{\mathfrak{A}})/k$ is an abelian extension.

The Brumer-Stark Conjecture

Conjecture (The Brumer part)

The element γ kills Cl_K.
That is, for every fractional ideal $\mathfrak{A}$ of K, the ideal $\mathfrak{A}^\gamma$ is principal.

Let K° be the set of *anti-units* of K

$$K^\circ := \{x \in K : |x|_{\mathfrak{P}_\infty} = 1,\ \forall \mathfrak{P}_\infty \mid \infty\}$$

Conjecture (The Stark part)

For every fractional ideal $\mathfrak{A}$ of K, there exists a generator $\alpha_{\mathfrak{A}}$ of $\mathfrak{A}^\gamma$ that is an anti-unit. Furthermore, define $\lambda_{\mathfrak{A}} \in \overline{K}$ by $\lambda_{\mathfrak{A}}^{W_K} = \alpha_{\mathfrak{A}}$, then $K(\lambda_{\mathfrak{A}})/k$ is an abelian extension.

- The conjecture is true if $k = \mathbb{Q}$ (Stickelberger's Theorem)
- The conjecture is true if k is not totally real or K is not totally complex
- The conjecture is satisfied for $\mathfrak{A}$ if it is a principal ideal
- The conjecture is true if K is principal
- The set of ideals satisfying the conjecture forms a group, stable under the action of G

- The conjecture is true if $k = \mathbb{Q}$ (Stickelberger's Theorem)
- The conjecture is true if k is not totally real or K is not totally complex
- The conjecture is satisfied for $\mathfrak{A}$ if it is a principal ideal
- The conjecture is true if K is principal
- The set of ideals satisfying the conjecture forms a group, stable under the action of G

- The conjecture is true if $k = \mathbb{Q}$ (Stickelberger's Theorem)
- The conjecture is true if k is not totally real or K is not totally complex
- The conjecture is satisfied for $\mathfrak{A}$ if it is a principal ideal
- The conjecture is true if K is principal
- The set of ideals satisfying the conjecture forms a group, stable under the action of G

- The conjecture is true if $k = \mathbb{Q}$ (Stickelberger's Theorem)
- The conjecture is true if k is not totally real or K is not totally complex
- The conjecture is satisfied for $\mathfrak{A}$ if it is a principal ideal
- The conjecture is true if K is principal
- The set of ideals satisfying the conjecture forms a group, stable under the action of G

- The conjecture is true if $k = \mathbb{Q}$ (Stickelberger's Theorem)
- The conjecture is true if k is not totally real or K is not totally complex
- The conjecture is satisfied for $\mathfrak{A}$ if it is a principal ideal
- The conjecture is true if K is principal
- The set of ideals satisfying the conjecture forms a group, stable under the action of G

The conjecture is true in the following cases

- if K/k is quadratic [Tate]
- if $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in general, and when G is of exponent 2 and has order > 4, assuming K/k is a tame extension [Sands]
- if $|G| = 4$ and K/k is a sub-extension of a non-abelian Galois extension K/k_0 of degree 8 [Tate]
- if K/k is a sub-extension of an abelian Galois extension K/k_0 for which the conjecture is true [Sands, Hayes]
- if $G \simeq \mathbb{Z}/4\mathbb{Z}$ and k is real quadratic [Greither]
- if $[K : k] = 6$, and $[k : \mathbb{Q}] = 2$, or 3 and the discriminant of k is coprime with 6 (except for some very special cases) [Greither-Roblot-Tangedal]

The conjecture is true in the following cases

- if K/k is quadratic [Tate]
- if $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in general, and when G is of exponent 2 and has order > 4, assuming K/k is a tame extension [Sands]
- if $|G| = 4$ and K/k is a sub-extension of a non-abelian Galois extension K/k_0 of degree 8 [Tate]
- if K/k is a sub-extension of an abelian Galois extension K/k_0 for which the conjecture is true [Sands, Hayes]
- if $G \simeq \mathbb{Z}/4\mathbb{Z}$ and k is real quadratic [Greither]
- if $[K : k] = 6$, and $[k : \mathbb{Q}] = 2$, or 3 and the discriminant of k is coprime with 6 (except for some very special cases) [Greither-Roblot-Tangedal]

The conjecture is true in the following cases

- if K/k is quadratic [Tate]
- if $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in general, and when G is of exponent 2 and has order > 4, assuming K/k is a tame extension [Sands]
- if $|G| = 4$ and K/k is a sub-extension of a non-abelian Galois extension K/k_0 of degree 8 [Tate]
- if K/k is a sub-extension of an abelian Galois extension K/k_0 for which the conjecture is true [Sands, Hayes]
- if $G \simeq \mathbb{Z}/4\mathbb{Z}$ and k is real quadratic [Greither]
- if $[K : k] = 6$, and $[k : \mathbb{Q}] = 2$, or 3 and the discriminant of k is coprime with 6 (except for some very special cases) [Greither-Roblot-Tangedal]

The conjecture is true in the following cases

- if K/k is quadratic [Tate]
- if $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in general, and when G is of exponent 2 and has order > 4, assuming K/k is a tame extension [Sands]
- if $|G| = 4$ and K/k is a sub-extension of a non-abelian Galois extension K/k_0 of degree 8 [Tate]
- if K/k is a sub-extension of an abelian Galois extension K/k_0 for which the conjecture is true [Sands, Hayes]
- if $G \simeq \mathbb{Z}/4\mathbb{Z}$ and k is real quadratic [Greither]
- if $[K : k] = 6$, and $[k : \mathbb{Q}] = 2$, or 3 and the discriminant of k is coprime with 6 (except for some very special cases) [Greither-Roblot-Tangedal]

The conjecture is true in the following cases

- if K/k is quadratic [Tate]
- if $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in general, and when G is of exponent 2 and has order > 4, assuming K/k is a tame extension [Sands]
- if $|G| = 4$ and K/k is a sub-extension of a non-abelian Galois extension K/k_0 of degree 8 [Tate]
- if K/k is a sub-extension of an abelian Galois extension K/k_0 for which the conjecture is true [Sands, Hayes]
- if $G \simeq \mathbb{Z}/4\mathbb{Z}$ and k is real quadratic [Greither]
- if $[K : k] = 6$, and $[k : \mathbb{Q}] = 2$, or 3 and the discriminant of k is coprime with 6 (except for some very special cases) [Greither-Roblot-Tangedal]

The conjecture is true in the following cases

- if K/k is quadratic [Tate]
- if $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in general, and when G is of exponent 2 and has order > 4, assuming K/k is a tame extension [Sands]
- if $|G| = 4$ and K/k is a sub-extension of a non-abelian Galois extension K/k_0 of degree 8 [Tate]
- if K/k is a sub-extension of an abelian Galois extension K/k_0 for which the conjecture is true [Sands, Hayes]
- if $G \simeq \mathbb{Z}/4\mathbb{Z}$ and k is real quadratic [Greither]
- if $[K : k] = 6$, and $[k : \mathbb{Q}] = 2$, or 3 and the discriminant of k is coprime with 6 (except for some very special cases) [Greither-Roblot-Tangedal]

Let $k = \mathbb{Q}(\sqrt{69})$, and $K = K^+(j)$ where K^+ is the ray class field of k of conductor 3 and j is a primitive third root of unity.

This example is one of the exceptions not covered by [GRT].

- Compute the Brumer element using L-functions
- Find a minimal set $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_s\}$ of $\mathbb{Z}[G]$-generators of Cl_K
- For each $\mathfrak{A}$
  - Compute $\mathfrak{A}^\gamma$ and check if it is principal
  - Call β a generator of $\mathfrak{A}^\gamma$, find a unit u such that $\alpha := u\beta$ is an anti-unit
  - Check if $K(\alpha^{1/w_K})$ is an abelian extension of k

- Compute the Brumer element using L-functions
- Find a minimal set $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_s\}$ of $\mathbb{Z}[G]$-generators of Cl_K
- For each $\mathfrak{A}$
  - Compute $\mathfrak{A}^\gamma$ and check if it is principal
  - Call β a generator of $\mathfrak{A}^\gamma$, find a unit u such that $\alpha := u\beta$ is an anti-unit
  - Check if $K(\alpha^{1/w_K})$ is an abelian extension of k

- Compute the Brumer element using L-functions
- Find a minimal set $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_s\}$ of $\mathbb{Z}[G]$-generators of Cl_K
- For each $\mathfrak{A}$
  - Compute $\mathfrak{A}^\gamma$ and check if it is principal
  - Call β a generator of $\mathfrak{A}^\gamma$, find a unit u such that $\alpha := u\beta$ is an anti-unit
  - Check if $K(\alpha^{1/w_K})$ is an abelian extension of k

- Compute the Brumer element using L-functions
- Find a minimal set $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_s\}$ of $\mathbb{Z}[G]$-generators of Cl_K
- For each $\mathfrak{A}$
  - Compute $\mathfrak{A}^\gamma$ and check if it is principal
  - Call β a generator of $\mathfrak{A}^\gamma$, find a unit u such that $\alpha := u\beta$ is an anti-unit
  - Check if $K(\alpha^{1/w_K})$ is an abelian extension of k

- Compute the Brumer element using L-functions
- Find a minimal set $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_s\}$ of $\mathbb{Z}[G]$-generators of Cl_K
- For each $\mathfrak{A}$
  - Compute $\mathfrak{A}^\gamma$ and check if it is principal
  - Call β a generator of $\mathfrak{A}^\gamma$, find a unit u such that $\alpha := u\beta$ is an anti-unit
  - Check if $K(\alpha^{1/w_K})$ is an abelian extension of k

- Compute the Brumer element using L-functions
- Find a minimal set $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_s\}$ of $\mathbb{Z}[G]$-generators of Cl_K
- For each $\mathfrak{A}$
    - Compute $\mathfrak{A}^\gamma$ and check if it is principal
    - Call β a generator of $\mathfrak{A}^\gamma$, find a unit u such that $\alpha := u\beta$ is an anti-unit
    - Check if $K(\alpha^{1/w_K})$ is an abelian extension of k

Let's start GP!

$$\gamma = w_K \sum_{\chi \in \hat{G}} \overline{L_S(0,\chi)} e_\chi \quad \text{where } e_\chi := \frac{1}{|G|} \sum_{\sigma \in G} \bar{\chi}(\sigma)\sigma^{-1}$$

Let $\mathfrak{g}$ be a generator of $\mathrm{Cl}_k(3\infty_1\infty_2)$.
Let $\sigma := \sigma_{\mathfrak{g}}$. Thus $G = \langle\sigma\rangle$.
Let $\zeta_6 := \exp(2i\pi/6)$.

The character χ_a represented by $[a]$ is the one defined by

$$\chi_a(\sigma) := \zeta_6^a.$$

An element $a_0 + a_1\sigma + \cdots + a_5\sigma^5 \in \mathbb{Z}[G]$ is represented by the vector $[a_0, a_1, \ldots, a_5]$.

Let $\mathfrak{g}$ be a generator of $\mathrm{Cl}_k(3\infty_1\infty_2)$.
Let $\sigma := \sigma_{\mathfrak{g}}$. Thus $G = \langle\sigma\rangle$.
Let $\zeta_6 := \exp(2i\pi/6)$.

The character χ_a represented by $[a]$ is the one defined by

$$\chi_a(\sigma) := \zeta_6^a.$$

An element $a_0 + a_1\sigma + \cdots + a_5\sigma^5 \in \mathbb{Z}[G]$ is represented by the vector $[a_0, a_1, \ldots, a_5]$.

Let $\mathfrak{g}$ be a generator of $\mathrm{Cl}_k(3\infty_1\infty_2)$.
Let $\sigma := \sigma_{\mathfrak{g}}$. Thus $G = \langle\sigma\rangle$.
Let $\zeta_6 := \exp(2i\pi/6)$.

The character χ_a represented by $[a]$ is the one defined by

$$\chi_a(\sigma) := \zeta_6^a.$$

An element $a_0 + a_1\sigma + \cdots + a_5\sigma^5 \in \mathbb{Z}[G]$ is represented by the vector $[a_0, a_1, \ldots, a_5]$.

Let $\mathfrak{p}$ be a prime ideal of k, $\mathfrak{P}$ a prime ideal of K such that

$$\mathfrak{P} \text{ is above } \mathfrak{p} \text{ is above } p.$$

Let $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and assume that

$$p \nmid (\mathbb{Z}_K : \mathbb{Z}[\theta]).$$

Then the Frobenius of $\mathfrak{p}$ is the unique element $\sigma \in G$ such that

$$\sigma(\theta) \equiv \theta^{\mathcal{N}\mathfrak{p}} \pmod{\mathfrak{P}}.$$

Let $\mathfrak{p}$ be a prime ideal of k, $\mathfrak{P}$ a prime ideal of K such that

$$\mathfrak{P} \text{ is above } \mathfrak{p} \text{ is above } p.$$

Let $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and assume that

$$p \nmid (\mathbb{Z}_K : \mathbb{Z}[\theta]).$$

Then the Frobenius of $\mathfrak{p}$ is the unique element $\sigma \in G$ such that

$$\sigma(\theta) \equiv \theta^{\mathcal{N}\mathfrak{p}} \pmod{\mathfrak{P}}.$$

Let $\mathfrak{p}$ be a prime ideal of k, $\mathfrak{P}$ a prime ideal of K such that

$$\mathfrak{P} \text{ is above } \mathfrak{p} \text{ is above } p.$$

Let $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and assume that

$$p \nmid (\mathbb{Z}_K : \mathbb{Z}[\theta]).$$

Then the Frobenius of $\mathfrak{p}$ is the unique element $\sigma \in G$ such that

$$\sigma(\theta) \equiv \theta^{\mathcal{N}\mathfrak{p}} \pmod{\mathfrak{P}}.$$

Recall that $w_K = 6$ so the torsion group of K is generated by ζ_6. Let $N \in \mathbb{Z}$ be such that

$$\sigma(\zeta_6) = \zeta_6^N.$$

Then an element $\alpha \in K$ is such that $K(\alpha^{1/6})/k$ is an abelian extension iff

$$\alpha^{N-\sigma} = \frac{\alpha^N}{\sigma(\alpha)}$$

is a 6-th power in K.

Recall that $w_K = 6$ so the torsion group of K is generated by ζ_6. Let $N \in \mathbb{Z}$ be such that

$$\sigma(\zeta_6) = \zeta_6^N.$$

Then an element $\alpha \in K$ is such that $K(\alpha^{1/6})/k$ is an abelian extension iff

$$\alpha^{N-\sigma} = \frac{\alpha^N}{\sigma(\alpha)}$$

is a 6-th power in K.