Checking the Brumer-Stark conjecture using PARI/GP

Xavier-François Roblot

IGD, Université Claude Bernard – Lyon 1

September 16th, 2004
1. Statement of the conjecture
   - Definitions
   - The Brumer element
   - The Brumer-Stark Conjecture

2. Current status of the conjecture
   - Some reductions and special cases
   - Further results

3. Checking the conjecture on an example
   - The example
   - The strategy
   - The verification
- $k$ is a number field of degree $n$
- $K$ is a finite abelian extension over $k$
- $G := \text{Gal}(K/k)$
- $w_K$ is the number of roots of unity in $K$
- $\text{Cl}_K$ 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

$$\zeta_S(s, \sigma) := \sum_{(a, S) = 1, \sigma_a = \sigma} \frac{1}{N_a^s}$$
- $k$ is a number field of degree $n$
- $K$ is a finite abelian extension over $k$
- $G := \text{Gal}(K/k)$
- $w_K$ is the number of roots of unity in $K$
- $\text{Cl}_K$ 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

$$\zeta_S(s, \sigma) := \sum_{(a, S)=1, \sigma_a = \sigma} \frac{1}{N(a)^s}$$
- \( k \) is a number field of degree \( n \)
- \( K \) is a finite abelian extension over \( k \)
- \( G := \text{Gal}(K/k) \)
- \( w_K \) is the number of roots of unity in \( K \)
- \( \text{Cl}_K \) 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

\[
\zeta_S(s, \sigma) := \sum_{\substack{(\alpha, S) = 1 \\ \sigma \alpha^s = \sigma}} \frac{1}{N\alpha^s}
\]
- $k$ is a number field of degree $n$
- $K$ is a finite abelian extension over $k$
- $G := \text{Gal}(K/k)$
- $\nu_K$ is the number of roots of unity in $K$
- $\text{Cl}_K$ 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

$$\zeta_S(s, \sigma) := \sum_{\substack{(a, S) = 1 \\ \sigma_a = \sigma}} \frac{1}{N a^s}$$
• $k$ is a number field of degree $n$
• $K$ is a finite abelian extension over $k$
• $G := \text{Gal}(K/k)$
• $\omega_K$ is the number of roots of unity in $K$
• $\text{Cl}_K$ 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

$$\zeta_S(s, \sigma) := \sum_{\substack{(\alpha, S) = 1 \\ \sigma\alpha = \sigma}} \frac{1}{N\alpha^s}$$
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 $\gamma$ kills $\mathcal{C}l_K$.
That is, for every fractional ideal $\mathfrak{A}$ of $K$, the ideal $\mathfrak{A}^\gamma$ is principal.

Let $K^\circ$ be the set of anti-units of $K$

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

Conjecture (The Stark part)
For every fractional ideal $\mathfrak{A}$ of $K$, there exists a generator $\alpha_{2l}$ of $\mathfrak{A}^\gamma$ that is an anti-unit. Furthermore, define $\lambda_{2l} \in \bar{K}$ by $\lambda_{2l}^{\mathcal{W}_K} = \alpha_{2l}$, then $K(\lambda_{2l})/k$ is an abelian extension.
The Brumer-Stark Conjecture

Conjecture (The Brumer part)

The element $\gamma$ kills $\text{Cl}_K$.
That is, for every fractional ideal $\mathcal{A}$ of $K$, the ideal $\mathcal{A}^\gamma$ is principal.

Let $K^\circ$ be the set of anti-units of $K$

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

Conjecture (The Stark part)

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

Conjecture (The Brumer part)

The element \( \gamma \) kills \( \text{Cl}_K \).
That is, for every fractional ideal \( \mathcal{A} \) of \( K \), the ideal \( \mathcal{A} \gamma \) is principal.

Let \( K^\circ \) 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 \( \mathcal{A} \) of \( K \), there exists a generator \( \alpha_{\mathcal{A}} \) of \( \mathcal{A} \gamma \) that is an anti-unit. Furthermore, define \( \lambda_{\mathcal{A}} \in \overline{K} \) by \( \lambda_{\mathcal{A}}^{\mathcal{W}_K} = \alpha_{\mathcal{A}} \), then \( K(\lambda_{\mathcal{A}})/k \) is an abelian extension.
The Brumer-Stark Conjecture

Conjecture (The Brumer part)
The element $\gamma$ kills $\text{Cl}_K$.
That is, for every fractional ideal $\mathfrak{A}$ of $K$, the ideal $\mathfrak{A}\gamma$ is principal.

Let $K^\circ$ be the set of anti-units of $K$

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

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 $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $G \cong \mathbb{Z}/4\mathbb{Z}$ 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 $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $G \cong \mathbb{Z}/4\mathbb{Z}$ 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 $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $G \cong \mathbb{Z}/4\mathbb{Z}$ 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 $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $G \cong \mathbb{Z}/4\mathbb{Z}$ 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 $\{A_1, \ldots, A_s\}$ of $\mathbb{Z}[G]$-generators of $\text{Cl}_K$
• For each $A$
  • Compute $A^\gamma$ and check if it is principal
  • Call $\beta$ a generator of $A^\gamma$, find a unit $u$ such that $\alpha := u\beta$ is an anti-unit
  • Check if $K(\alpha^{1/w})$ is an abelian extension of $k$
• Compute the Brumer element using $L$-functions
• Find a minimal set $\{A_1, \ldots, A_s\}$ of $\mathbb{Z}[G]$-generators of $\text{Cl}_K$
• For each $A$
  • Compute $A^\gamma$ and check if it is principal
  • Call $\beta$ a generator of $A^\gamma$, find a unit $u$ such that $\alpha := u\beta$ is an anti-unit
  • Check if $K(\alpha^{1/w})$ is an abelian extension of $K$
Compute the Brumer element using $L$-functions
Find a minimal set \{A_1, \ldots, A_s\} of $\mathbb{Z}[G]$-generators of $\text{Cl}_K$
For each $A$
- Compute $A^\gamma$ and check if it is principal
- Call $\beta$ a generator of $A^\gamma$, 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 $\{A_1, \ldots, A_s\}$ of $\mathbb{Z}[G]$-generators of $\text{Cl}_K$

For each $A$

- Compute $A^\gamma$ and check if it is principal
- Call $\beta$ a generator of $A^\gamma$, 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 $\{A_1, \ldots, A_s\}$ of $\mathbb{Z}[G]$-generators of $\text{Cl}_K$

For each $A$

- Compute $A^\gamma$ and check if it is principal
- Call $\beta$ a generator of $A^\gamma$, 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 $\{A_1, \ldots, A_s\}$ of $\mathbb{Z}[G]$-generators of $\text{Cl}_K$
- For each $A$
  - Compute $A^\gamma$ and check if it is principal
  - Call $\beta$ a generator of $A^\gamma$, 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!
\[
\gamma = w_K \sum_{\chi \in \hat{G}} \overline{L_S(0, \chi)} e_\chi \quad \text{where} \quad e_\chi := \frac{1}{|G|} \sum_{\sigma \in G} \bar{\chi}(\sigma) \sigma^{-1}
\]
Let \( g \) be a generator of \( Cl_k(3\infty_1\infty_2) \).
Let \( \sigma := \sigma_g \). Thus \( G = \langle \sigma \rangle \).
Let \( \zeta_6 := \exp(2i\pi/6) \).

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

The character $\chi_a$ 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 $[a_0, a_1, \ldots, a_5]$. 

Xavier-François Roblot

Checking the Brumer-Stark conjecture using PARI/GP
Let $g$ be a generator of $\text{Cl}_k(3\infty_1\infty_2)$.
Let $\sigma := \sigma_g$. Thus $G = \langle \sigma \rangle$.
Let $\zeta_6 := \exp(2i\pi/6)$.

The character $\chi_a$ 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 $\mathfrak{P}$ is above $\mathfrak{p}$ is above $\mathfrak{p}$.

Let $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and assume that $\mathfrak{p} \nmid (\mathbb{Z}_K : \mathbb{Z}[\theta])$.

Then the Frobenius of $\mathfrak{p}$ is the unique element $\sigma \in G$ such that $\sigma(\theta) \equiv \theta^{N_{\mathfrak{P}}^\mathfrak{p}} \pmod{\mathfrak{P}}$. 
Let $\mathfrak{p}$ be a prime ideal of $k$, $\mathfrak{P}$ a prime ideal of $K$ such that $\mathfrak{P}$ is above $\mathfrak{p}$ 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 $p$ is the unique element $\sigma \in G$ such that $\sigma(\theta) \equiv \theta^{N_p} \pmod{\mathfrak{P}}$. 
Let $p$ be a prime ideal of $k$, $\mathfrak{P}$ a prime ideal of $K$ such that $\mathfrak{P}$ is above $p$ 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 $p$ is the unique element $\sigma \in G$ such that $\sigma(\theta) \equiv \theta^N_p \pmod{\mathfrak{P}}$. 
Recall that $w_K = 6$ so the torsion group of $K$ is generated by $\zeta_6$. 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 $\zeta_6$. 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 $K$. 