ON THE BRUMER–STARK CONJECTURE AND REFINEMENTS, II

Samit Dasgupta
Duke University

Mahesh Kakde
Indian Institute of Science

ICTS, Bangalore
9th August 2022

MOTIVATION

Let F be a number field (a finite extension of $\mathbf{Q}$). We would like to understand the maximal abelian extension F^{ab}.

This is known classically for $F = \mathbf{Q}$ and $F = \mathbf{Q}(\sqrt{-d}), d > 0$.

Hilbert asked for the generation of F^{ab} using the special values or transformation properties of *complex analytic* functions depending on F. We use a *p-adic approach* to solve this problem.

Class field theory does not describe the field F^{ab}, but it does describe $\mathrm{Gal}(F^{ab}/F)$.

CLASS FIELD THEORY

For every positive integer n, there is a field extension F_n of F called the **narrow ray class field of conductor** n such that:

- $F_n \subset F_m$ if $n \mid m$
- $F^{ab} = \bigcup_{n \geq 1} F_n$
- $\mathrm{Gal}(F_1/F) \cong \mathrm{Pic}^+(\mathcal{O}_F)$ and $\mathrm{Gal}(F_n/F_1) \cong (\mathcal{O}_F/n)^*/(\mathcal{O}_F^*)_+$.

Example: $\mathbf{Q}_n = \mathbf{Q}(e^{2\pi i/n})$ and $\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^*$.

EXPLICIT CLASS FIELD THEORY

Class field theory describes the automorphism group

$$\mathrm{Gal}(F^{ab}/F) = \varprojlim \mathrm{Gal}(F_n/F).$$

The goal of **explicit class field theory** is to construct the field F^{ab}, or equivalently, each of the fields F_n, using analytic functions depending only on the ground field F.

Example:

$$\mathbf{Q}^{ab} = \mathbf{Q}(S), \qquad S = \{e^{2\pi i x} : x \in \mathbf{Q}\}.$$

COMPLEX MULTIPLICATION

Quadratic imaginary fields.

$$F = \mathbf{Q}(\sqrt{-d}), \qquad d = \text{ positive integer}.$$

Theorem. $F_n = F(j(E), w(E[n]))$ where E is an elliptic curve with complex multiplication by $\mathcal{O}_F$ and $w =$ "Weber function."

Here $j(q) = q^{-1} + 744 + 196884q + 2149360q^2 + \cdots$ is the usual modular function. For $F = \mathbf{Q}(\sqrt{-d})$, modular functions play the role of the exponential function for $F = \mathbf{Q}$.

HILBERT'S 12TH PROBLEM (1900)

"The theorem that every abelian number field arises from the realm of rational numbers by the composition of fields of roots of unity is due to Kronecker."

"Since the realm of the imaginary quadratic number fields is the simplest after the realm of rational numbers, the problem arises, to extend Kronecker's theorem to this case."

"Finally, the extension of Kronecker's theorem to the case that, in the place of the realm of rational numbers or of the imaginary quadratic field, any algebraic field whatever is laid down as the realm of rationality, seems to me of the greatest importance. I regard this problem as one of the most profound and far-reaching in the theory of numbers and of functions.

SETUP

$F =$ totally real field.

$H =$ finite Galois extension, CM field.

$G = \mathrm{Gal}(H/F)$, abelian.

$S = \{$infinite places, ramified places$\}$.

$T =$ finite set of places, disjoint from S.

$$L_{S,T}(\chi, s) = \prod_{\mathfrak{p} \notin S} \frac{1}{1 - \chi(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s}} \prod_{\mathfrak{p} \in T} (1 - \chi(\mathfrak{p})\mathrm{N}\mathfrak{p}^{1-s}) \,.$$

THE BRUMER-STARK CONJECTURE

Let $\mathfrak{p}$ be a prime ideal of F that splits completely in H.

Let

$$U_T^- = \{u \in \mathcal{O}_H[1/\mathfrak{p}]^* \colon |u|_w = 1 \text{ for all } w \nmid \mathfrak{p},$$
$$u \equiv 1 \pmod{\mathfrak{q}} \text{ for all } \mathfrak{q} \in T\}.$$

Conjecture. Fix a prime $\mathfrak{P}$ of H above $\mathfrak{p}$. There exists (a unique) $u \in U_T^-$ such that for all $\chi \in \hat{G}$ we have

$$L_{S,T}(\chi, 0) = \sum_{\sigma \in G} \chi(\sigma) \operatorname{ord}_{\sigma^{-1}(\mathfrak{P})}(u).$$

HILBERT'S 12TH PROBLEM

If H is a cyclic CM extension of F in which $\mathfrak{p}$ splits completely, then the Brumer-Stark unit u for H can be shown to generate H.

Theorem. Let $S = \{u\}_{\mathfrak{p},H} \cup \{\sqrt{\alpha_1}, \cdots, \sqrt{\alpha_{n-1}}\}$, where the α_i are elements of F^* whose signs in $\{\pm 1\}^n$ are a basis for this $\mathbf{Z}/2\mathbf{Z}$-vector space. Then

$$\boxed{F^{ab} = F(S).}$$

STICKELBERGER ELEMENTS

Theorem. (Deligne-Ribet, Cassou-Noguès)

There is a unique $\Theta \in \mathbf{Z}[G]$ such that

$$\chi(\Theta) = L_{S,T}(\chi^{-1}, 0)$$

for all characters χ of G.

TOWER OF FIELDS

Let L be another finite CM abelian extension of F, such that $L \supset H$ and L is unramified outside $S_{\mathfrak{p}} = S \cup \{\mathfrak{p}\}$

Write $\mathfrak{g} = \mathrm{Gal}(L/F),\ \Gamma = \mathrm{Gal}(L/H),$ so $\mathfrak{g}/\Gamma \cong G$.

Consider the augmentation:

$$\epsilon : \mathbf{Z}[\mathfrak{g}] \longrightarrow \mathbf{Z}[G].$$

Then

$$\begin{aligned}\epsilon(\Theta_{S_{\mathfrak{p}},T}(L/F)) &= \Theta_{S_{\mathfrak{p}},T}(H/F) \\ &= (1 - [\sigma_{\mathfrak{p}}])\Theta_{S,T}(H/F) = 0\end{aligned}$$

GROSS' TOWER OF FIELDS CONJECTURE

Therefore,

$$\Theta_{S_{\mathfrak{p}},T} \in I = \ker(\epsilon).$$

Consider $\mathrm{rec}_{\mathfrak{P}} \colon H_{\mathfrak{P}}^{*} \longrightarrow \mathbf{A}_{H}^{*} \longrightarrow \Gamma$.

Conjecture. (Gross)

We have

$$\sum_{\sigma \in G} (\mathrm{rec}_{\mathfrak{P}}(\sigma(u_{\mathfrak{p}})) - 1)\tilde{\sigma}^{-1} \equiv \Theta_{S_{\mathfrak{p}},T}$$

in I/I^2.

CONGRUENCE FOR THE BRUMER STARK-UNIT

We have $I/I^2 \cong \mathbf{Z}[G] \otimes \Gamma = \mathbf{Z}[G] \otimes (\mathbf{A}_H^*/J_L)$.

Gross' Conjecture gives a formula for $\sum_{\sigma \in G} \sigma^{-1} \otimes \sigma(u_\mathfrak{p})$ here,

i.e. for each $\sigma(u_\mathfrak{p})$ in $\mathbf{A}_H^*/J_L$.

Taking the union of all possible L, say $L_{S_\mathfrak{p}}$, we get a formula in

$$\mathrm{Gal}(L_{S_\mathfrak{p}}/H) \cong \mathbf{A}_H^*/J \cong \prod_{v \in S_\mathfrak{p}} F_v^* / \widehat{E_\mathfrak{p}(H,S)},$$

i.e a formula for $(u_\mathfrak{p},1,1,1,1)$ in this latter space.

EISENSTEIN MEASURE: SHINTANI'S METHOD

Let $E(\mathfrak{n}) = \{\epsilon \in (\mathcal{O}_F^*)_+ : \epsilon \equiv 1 \pmod{\mathfrak{n}}\}$.

Theorem (Shintani). There exists a (signed) fundamental domain for the action of $E(\mathfrak{n})$ on $(\mathbb{R}^{>0})^n$ consisting of simplicial cones generated by elements of F:

$$D = \sum_i a_i C_i\,.$$

Fix $z \in \mathfrak{b}^{-1}$ with $z \equiv 1 \pmod{\mathfrak{n}}$.

$$\zeta(\mathfrak{b}, U, D, s) = \sum_i a_i \sum_{\alpha \in C_i \cap (\mathfrak{b}\mathfrak{n}^{-1} + z) \cap U} (\mathrm{N}\alpha)^{-s}.$$

For every compact open $U \subset \mathcal{O}_p$, define

$$\mu(U) = \zeta(\mathfrak{b}, U, D, 0) - \ell \cdot \zeta(\mathfrak{b}\mathfrak{l}^{-1}, U, D, 0)\,.$$

REFINED CONJECTURE

Suppose $\mathfrak{p} = (p)$.

Conjecture. We have

$$u_{\mathfrak{p}} = p^{\zeta(0)} \times\!\!\!\!\!\!\int_{\mathcal{O}_p^*} x \, d\mu(x)$$

where μ is the Eisenstein measure.

RESULT WITH KAKDE

Theorem. Assume that $\mathfrak{p}$ lies above a rational prime p that does not ramify in F. Then the conjectural exact formula for the Brumer-Stark unit u holds up to a root of unity in $F_{\mathfrak{p}}^*$.

Darmon-Vonk-Pozzi have obtained essentially the same result in the case that F is real quadratic and p is inert in F.

COMPUTATIONAL EXAMPLE

Our formula for Brumer-Stark units is explicitly computable.

Example. $F = \mathbf{Q}(\sqrt{305})$, $\quad \mathcal{O} = \mathbf{Z}\left[\frac{1+\sqrt{305}}{2}\right]$.

$n = 1$, $F_1 =$ narrow Hilbert class field. $p = 3$.

Computing u and its conjugates to a high p-adic precision, we obtain a polynomial very close to:

$$81x^4 - \frac{9\sqrt{D}+345}{2}x^3 + \frac{15\sqrt{D}+419}{2}x^2 - \frac{9\sqrt{D}+345}{2}x + 81.$$

The splitting field of this polynomial is indeed F_1.

A LARGER EXAMPLE

$F = \mathbf{Q}(\sqrt{473}), \quad p = 5.$

To a high p-adic precision, u is a root of:

$$5^{10}x^6 + \frac{-253125\sqrt{D} - 4501875}{2}x^5$$
$$+\frac{496125\sqrt{D} + 5836125}{2}x^4 + \frac{-59535\sqrt{D} - 13546883}{2}x^3 +$$
$$\frac{496125\sqrt{D} + 5836125}{2}x^2 + \frac{-253125\sqrt{D} - 4501875}{2}x + 5^{10}.$$

Again, the splitting field of this polynomial is F_1.

CONNECTION TO GROSS' CONJECTURE

Recall that Gross's tower of fields conjecture states that

$$(u_{\mathfrak{p}},1,1,1,\ldots,1) \equiv \Theta_{S,T}(L_{S_{\mathfrak{p}}}/F)$$

in $\left(\prod_{v\in S_{\mathfrak{p}}} F_v^*\right)/\widehat{E_{\mathfrak{p}}(H,S)} \cong \mathrm{Gal}(L_{S_{\mathfrak{p}}}/H)$.

Lemma. Write $v_{\mathfrak{p}}$ for our conjectural analytic formula for $u_{\mathfrak{p}}$.

$$(v_{\mathfrak{p}},1,1,1,\ldots,1) \equiv \Theta_{S,T}(L_{S_{\mathfrak{p}}}/F) \text{ in } \left(\prod_{v\in S_{\mathfrak{p}}} F_v^*\right)/\widehat{E_{\mathfrak{p}}(H,S)}.$$

Conclusion. Gross's Conjecture implies that $u_{\mathfrak{p}} \equiv v_{\mathfrak{p}}$ in $F_{\mathfrak{p}}^*/D(H,S)$, where

$$D(H,S) = \{x \in F_{\mathfrak{p}}^* : (x,1,1,\ldots,1) \in \widehat{E_{\mathfrak{p}}(H,S)} \subset \prod F_v^*\}.$$

CHANGING S—"HORIZONTAL IWASAWA THEORY"

If we adjoin a prime $\mathfrak{q}$ to S, we find

$$u_{\mathfrak{p},S\cup\{\mathfrak{q}\},T} = u_{\mathfrak{p},S,T}/\sigma_{\mathfrak{q}}(u_{\mathfrak{p},S,T}).$$

Therefore, if $\sigma_{\mathfrak{q}}$ = complex conjugation, then

$$u_{\mathfrak{p},S\cup\{\mathfrak{q}\},T} = u^2_{\mathfrak{p},S,T}.$$

For such a $\mathfrak{q}$ we can also show $v_{\mathfrak{p},S\cup\{\mathfrak{q}\},T} = v^2_{\mathfrak{p},S,T}$.

Conclusion. If $p \neq 2$, we can adjoin primes $\mathfrak{q}_i$ to S such that each $\sigma_{\mathfrak{q}_i}$ is complex conjugation, and Gross's conjecture for $S' = S \cup \{q_1, \ldots q_k\}$ yields $u_{\mathfrak{p},S,T} \equiv v_{\mathfrak{p},S,T}$ in the pro-p part of $F^*_{\mathfrak{p}}/D(H, S')$.

MAKING D(H, S') ARBITRARILY SMALL

Theorem. Suppose that $F(\mu_{p^\infty}) \subset H^+$, the maximal totally real subfield of H. For any positive integer m, there exists $S' = S \cup \{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ with each $\sigma_{\mathfrak{q}_i}$ = complex conjugation such that $D(H, S') \subset 1 + \mathfrak{p}^m \subset F_{\mathfrak{p}}^*$.

Proof sketch. We choose the $\mathfrak{q}_i$ such that $\mathrm{N}\mathfrak{q}_i \equiv 1 \pmod{p^m}$, such that for each unit $\epsilon \in \mathcal{O}_F^*$, $\epsilon \not\equiv 1 \pmod{\mathfrak{p}^m}$, there exists $\mathfrak{q}_i$ such that $\epsilon \not\equiv 1 \pmod{\mathfrak{q}_i}$. These are Frobenius conditions, mutually exclusive by the assumptions.

GROSS'S CONJECTURE IMPLIES REFINED CONJECTURE

Theorem. Suppose that $p \neq 2$ and that p is unramified in F. Gross's tower of fields conjecture implies that $u_{\mathfrak{p}} \equiv v_{\mathfrak{p}}$ in $F_{\mathfrak{p}}^*/\mu$, where μ is the finite group of roots of unity in $F_{\mathfrak{p}}^*$.

PROOF OF GROSS'S CONJECTURE

Motivation—**Greenberg Stevens $\mathscr{L}$-invariant**: $\mathscr{L} = L_p'/L$.

Define

$$R_{\mathscr{L}} = \mathbf{Z}_p[\mathfrak{g}]_-/(\mathscr{L}\Theta_H - \Theta_L, I\mathscr{L}, \mathscr{L}^2, I^2).$$

We define an $R_{\mathscr{L}}$-module $\nabla_{\mathscr{L}}$ such that

$$\mathrm{Fitt}_{R_{\mathscr{L}}}(\nabla_{\mathscr{L}}) = \left(\sum_{\sigma \in G} \mathrm{rec}_{\mathfrak{P}}(\sigma(u_{\mathfrak{p}})) - 1)\tilde{\sigma}^{-1} - \Theta_L\right).$$

Inspired by work of Kurihara—Burns—Sano on the ETNC.

PROOF OF GROSS'S CONJECTURE

Gross's conjecture then follows from two results:

Theorem. We have $\mathrm{Fitt}_{R_{\mathscr{L}}}(\nabla_{\mathscr{L}}) = 0$.

Proof. Using Ribet's method as in the proof of Brumer—Stark. We give a cohomological interpretation of surjective maps $\nabla_{\mathscr{L}} \to N$ and construct a relevant cohomology class $\kappa \in H^1(G_F, N)$ such that $\mathrm{Fitt}_{R_{\mathscr{L}}}(N) = 0$.

Theorem. The map $\mathbf{Z}[\mathfrak{g}]_-/I^2 \to R_{\mathscr{L}}$ is injective.

Proof. Key fact is that $\Theta_L \in \prod_{v \in S_{\mathfrak{p}}} \ker(\mathbf{Z}_p[\mathfrak{g}]_- \to \mathbf{Z}_p[\mathfrak{g}/\mathfrak{g}_v]_-)$. This follows from our proof of strong Brumer—Stark:

$$\mathrm{Fitt}_{\mathbf{Z}_p[\mathfrak{g}]_-}(\nabla(L)) = (\Theta_L).$$

Thank you!