The Charm of Units

Preda Mihăilescu

University of Göttingen

September 2017

God gave a name to all the animals,
In the beginning, in the beginning.[1]

p irregular iff $p | B_{p-2n+1}$! ! !
But does $p | h_p^+$ occur ? ? ?

Preda Mihăilescu

Mathematisches Institut, Universität Göttingen.

[1] Bob Dylan – Nobel Rock star

Notations before facts

Let p be an odd (supersingular) prime.

- $\mathbb{K}' = \mathbb{Q}(\zeta) = \mathbb{Q}[X]/(\Phi_p(X)),\ \zeta$ a primitive $p-\mathrm{th}$ root of unity, $\mathbb{K} = \mathbb{Q}(\zeta + \overline{\zeta})$.
- $\mathbb{K}'_n = \mathbb{Q}(\zeta_n),\ \zeta_n$ primitive $p^{n+1}-\mathrm{th}$ roots of unity.
- $$\begin{aligned} \mathbb{K}'_\infty &= \cup_n \mathbb{K}'_n,\ \Gamma = \text{ Gal } (\mathbb{K}'_\infty/\mathbb{K}') \cong \mathbb{Z}_p, \\ \tau &\in \Gamma,\ T = \tau - 1. \end{aligned}$$
- Galois: $\sigma_c : \zeta \mapsto \zeta^c$ for $c \in \mathbb{F}_p^\times$. $G = \{\sigma_c\ :\ c \in P\} = $ Gal $(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $\sigma \in G$ a generator (as cyclic mult. group).
- G lifts canonically to $G_n =$ Gal $(\mathbb{K}_n/\mathbb{Q})$, tame ramification group of the unique prime above p in $\mathbb{K}_n$.

For arbitrary number fields $\mathbb{M}$, I denote:

- $$\begin{aligned} A(\mathbb{M}) &= (\mathcal{C}(\mathbb{M}))_p, \quad E(\mathbb{M}) = \mathcal{O}^\times(\mathbb{M}), \\ U(\mathbb{M}) &= \prod_{P|(p)} \mathcal{O}(\mathbb{M}_P)^\times, \\ U'(\mathbb{M}) &= \{u \in U(\mathbb{M}) \ : \ \mathbf{N}_{\mathbb{M}_p/\mathbb{Q}_p}(u) = 1\}. \end{aligned}$$
- The **group ring R** $= \mathbb{Z}[G]$ acting multiplicatively on $\mathbb{K}^\times, E(\mathbb{K}), A(\mathbb{K})$ etc.:

$$\Theta = \sum_{c=1}^{p-1} n_c \cdot \sigma_c \quad \rightarrow \quad \alpha^\Theta = \prod_{c \in P} \alpha^{n_c \sigma_c}.$$

- The orthogonal idempotents of **R** are

$$\varepsilon_j = \frac{1}{p-1} \sum_{c=1}^{p-1} \omega(\sigma_c)^j \cdot \sigma_c^{-1},$$

with ω the Teichmüller character.

$$\varepsilon_i \cdot \varepsilon_j = \delta_{i,j} \varepsilon_i,$$

and $\sum_j \varepsilon_j = 1$.

The Thaine Shift
Assume that $A(\mathbb{K}) \neq \{1\}$ – Vandiver false

- Fix some $\mathbb{L}/\mathbb{K}$, real unramified extension of degree p, galois over $\mathbb{Q}$. Its existence is equivalence with Vandiver failing for p. We shall investigate the consequences of the assumption along the tower $\mathbb{L}_n = \mathbb{L} \cdot \mathbb{K}_n$, with particular focus on **units and capitulation**.
- Let $\Phi =$ Gal $(\mathbb{L}/\mathbb{K})$, generated by ν, and $s = \nu - 1$.

$$\mathcal{N} = \sum_{i=0}^{p-1} \nu^i = p + sf(s)...$$

- The ramified primes $\lambda_n = (\zeta_n - \overline{\zeta}_n)$ split complitely in $\mathbb{L}_n$, into principal ideals. Assume $\pi_n \in \mathbb{L}_n$ is such that $(\mathcal{N}(\pi_n)) = (\lambda_n)$.
- Let σ denote a generator of the tame ramification of (π_n), and $\mu_n = \pi_n^{\sigma-1} \in E(\mathbb{L}_n)$.
  Metacyclotomic unit, maps surjectively on cyclotomic units, via norm.
-

$$
\begin{aligned}
U(\mathbb{L}_n) &\cong \prod_{i=0}^{p-1} \mathcal{O}^\times(\mathbb{L}_{\nu^i \pi_n}), \\
x \in U(\mathbb{L}_n) &\mapsto (x_0, x_1, \ldots, x_{p-1}) = \left(\iota_i(x) \in \mathcal{O}^\times(\mathbb{L}_{\nu^i \pi_n})\right)_{i=0}^{p-1}.
\end{aligned}
$$

Hilbert Theorems of CF

In Hilbert's Theorems, $\mathbb{L}/\mathbb{K}$ is an arbitrary cyclic extensions of number fields.

H91 Let $\mathcal{E} = \{e_1, e_2, \ldots, e_r\} \subset E(\mathbb{K})$ be a fundamental set of units. Then there are

$$\begin{array}{rcl} H_0 & ; & H_1, \ldots, H_r \in E(\mathbb{L}) \setminus E(\mathbb{L})^s \\ \mathcal{N}(H_0) & = & 1, \quad [\mathcal{N}(H_i), i > 0]_{\mathbb{Z}} = \mathcal{N}(E(\mathbb{L})), \end{array}$$

H94 If $\mathbb{L}/\mathbb{K}$ is unramified, then $H_0 = (\gamma^s)$, and $(\gamma) = \mathfrak{A} \cdot \mathcal{O}(\mathbb{L})$, with $\mathrm{ord}([\mathfrak{A}]) = p$. **Capitulation and capitulation units**

Units local and global.

- Recall that
$$U^{2j}(\mathbb{K}_n) = \varepsilon_{2j} U(\mathbb{K}_n) \cong (\xi_n^{2j})^{\Lambda},$$
are Λ-cyclic, and $\iota_k(U(\mathbb{L})) \cong U(\mathbb{K}_n)$.
- Let
$$U^{2j}(\mathbb{L}_n) = \{u \in U(\mathbb{L}_n) \ : \ \iota_k(u) \in U^{2j}(\mathbb{K}_n)\},$$
$\Xi_n^{2j} = (\xi_n, 1, \ldots, 1)$ under the CRT, so
$$U^{2j}(\mathbb{L}_n) = (\Xi_n^{2j})^{\Lambda[s]}.$$

- The singular space, for $W = \Xi^0(\mathbb{L}_0)$,

$$\mathcal{S} = U^0(\mathbb{L}_0) = W^{\mathbb{Z}_p[s]}.$$

Let $\Theta_n = (\Delta_n, 1, \ldots, 1) \in U^0(\mathbb{L}_n)$ and

$$\begin{aligned} R_n &= \Theta_n^{\Lambda[s]}, \\ \Omega_n &= R_n \oplus \bigoplus_{j=1}^{d-1} U^{2j}(\mathbb{L}_n) \subset U'(\mathbb{L}_n), \\ U(\mathbb{L}_n) &= \mathcal{S} \bigoplus \Omega_n, \quad \mathcal{N}(\Omega_n) = \mathcal{N}(U'(\mathbb{L}_n)). \end{aligned}$$

The natural map

$$\iota_r : U(\mathbb{L}_n) \to \mathcal{S}$$

acts also on $E(\mathbb{L}_n)$ via diagonal embedding.

- **Singularity index** $\ell : E(\mathbb{L}_n) \to \mathbb{N}_{>0}$,

$$\begin{aligned} \iota_r(e) &= W^{\text{unit} \cdot s^{\ell(e)}}, \\ \ell(\mathbb{L}_n) &= \min_{e \in E(\mathbb{L}_n)} (\ell(\mathbb{L}_n)). \end{aligned}$$

Theorem

There is a **singular unit**

$$\boxed{\delta_n \in E(\mathbb{L}_n) \setminus E(\mathbb{L}_n)^{(s,p)},}$$

such that $[\delta_n^{s^i}, \mu_n^{s^i T^j}]_{\mathbb{Z}}$ *are independent of finite index in* $E(\mathbb{L}_n)$*. Moreover,* $\iota_r(\delta_n) \neq 1$ *and there is a non principal ideal* $\mathfrak{A}_n \in a \in A(\mathbb{K}_n)[p]$*, with*

$$\mathfrak{A}_n \mathcal{O}(\mathbb{L}_n) = (\gamma_n), \quad \delta_n = \gamma_n^s.$$

Assume that $|A(\mathbb{K}_n)|$ are uniformly bounded (Greenberg λ-Conjecture)

Lemma

There is an integer n_0 such that for all $n > n_0$, the following hold:

- $A(\mathbb{K}_n) \cong A(\mathbb{K}_{n_0})$ *and*

$$Ker\ (\iota_{n,n+1} : A(\mathbb{K}_n) \to A(\mathbb{K}_{n+1})) = A(\mathbb{K}_n)[p].$$

- *The singular unit verifies* $\ell(\delta_n) = \ell(\mathbb{L}_n)$.

Consequence and final

Lemma

For $n > n_0$ there are units $e_{n+1} \in E(\mathbb{L}_{n+1})$ such that $\delta_n = e_{n+1}^s$. In consequence

$$\ell(\mathbb{L}_{n+1}) \leq \ell(e_{n+1}) < \ell(\delta_n) = \ell(\mathbb{L}_n).$$

But then there is some n such that $\ell(\mathbb{L}_n) = 0$, which is impossible.