Atelier PARI/GP — 17 janvier 2018

Some remarks and experiments on Greenberg's p-rationality conjecture

Razvan Barbulescu and Jishnu Ray

CNRS and IMJ-PRG (Sorbonne Université, Paris Diderot and CNRS)

The quest for open representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Problem

Given an integer n and a prime p, find a continous representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{Z}_p)$$

such that $[\mathrm{GL}_n(\mathbb{Z}_p) : Im(\rho)]$ *is* *finite*.

Chronology

- $n = 2$ (Serre 1972)

$$\begin{array}{llll} \rho : & \lim_{\leftarrow} \mathrm{Gal}(\mathbb{Q}(E[p^k])/\mathbb{Q}) & \to & \lim_{\leftarrow} \mathrm{Aut}(E[p^k]) \simeq \lim_{\leftarrow} \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}_p) \\ & \sigma & \mapsto & (P = (x,y) \mapsto (\sigma(x), \sigma(y)); \end{array}$$

- $n = 3$ case $p \equiv 8 \pmod{21}$ (Hamblen 2008) using deformation theory;
- $n = 3$ case $p \equiv 1 \pmod 3$ (Upton 2009) using abelian varieties;
- $\forall n \in \mathbb{N}$ (Greenberg 2016) under a new conjecture; It suffices to find examples in order to proove his construction for small values of n and p, for example $p = 5, 7, 11, 13, 17, 19$ and $n = 4, \ldots, 63$.

p-rational fields

Notation

- M the compositum of all finite p-extensions of K which are unramified outside primes above p;
- M^{ab} the maximal abelian extension of K contained in M;
- $\Gamma := \mathrm{Gal}(M/K)$;
- $\Gamma^{ab} \cong \mathrm{Gal}(M^{ab}/K)$.

Proposition-Definition (Movahhedi 1990)

The number field K is said to be p-rational if the following equivalent conditions are satisfied:

1. $\mathrm{rank}_{\mathbb{Z}_p}(\Gamma^{ab}) = r_2 + 1$ and Γ^{ab} is torsion-free as a $\mathbb{Z}_p$-module,
2. Γ is a free pro-p group with $r_2 + 1$ generators,
3. Γ is a free pro-p group.

If K satisfies Leopoldt's conjecture (Washington Sec 5.5), e.g. K is abelian, then the above conditions are also equivalent to

4. - $\left\{ \alpha \in K^\times \mid \begin{array}{c} \alpha\mathcal{O}_K = \mathfrak{a}^p \text{ for some fractional ideal } \mathfrak{a} \\ \text{and } \alpha \in (K_\mathfrak{p}^\times)^p \text{ for all } \mathfrak{p} \in S_p \end{array} \right\} = (K^\times)^p$
   - and the map $\mu(K)_p \to \prod_{\mathfrak{p} \in S_p} \mu(K_\mathfrak{p})_p$ is an isomorphism.

Greenberg's contribution

Let K be a p-rational abelian number field and $\Omega = \mathrm{Gal}(K/\mathbb{Q})$ has exponent dividing $p-1$. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on μ_{p^∞} defines a continuous homomorphism χ_{cyc} from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathbb{Z}_p^*$. $\hat{\Omega}_{\mathrm{odd}}$ is the set of characters non trivial on the complex multiplication.

Proposition

Assume also that one can find distinct characters $\chi_1, \ldots, \chi_n$ in $\hat{\Omega}_{\mathrm{odd}} \bigcup \{\chi_0\}$ such that their product is χ_0. Then there exists a continuous homomorphism

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{Z}_p)$$

such that $\rho_0(\Gamma) = S_n^{(0)}(\mathbb{Z}_p)$, the Sylow pro-$p$ subgroup of $\mathrm{SL}_n(\mathbb{Z}_p)$. Furthermore, $\rho = \rho_0 \otimes \kappa$ is a continuous homomorphism from $\mathrm{Gal}(M/\mathbb{Q})$ to $\mathrm{GL}_n(\mathbb{Z}_p)$ with open image.

Corollary

Let K be complex such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$, where $t \geq 4$. For every $4 \leq n \leq 2^{t-1} - 3$ there exists a continuous homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{Z}_p)$ with open image.

Greenberg's p-rationality conjecture

Conjecture (Greenberg 2016)

For any odd prime p and for any t, there exist a p-rational field K such that $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t$.

Problem

Given a finite group G and a prime p, decide the following statements:

1. *Greenberg's conjecture holds for G and p: there exists a number field of Galois group G which is p-rational, in this case we say that $\mathrm{GC}(G, p)$ is true;*
2. *the infinite version of Greenberg's conjecture holds for G and p: there exist infinitely many number fields of Galois group G which are p-rational, in this case we say that $\mathrm{GC}_\infty(G, p)$ is true.*

A family of p-rational real quadratic fields

Lemma

For any prime $p \geq 5$ not belonging to $\{\frac{1}{2}a^2 \pm 1 \mid a \in \mathbb{N}\}$ the real quadratic number field $K = \mathbb{Q}(\sqrt{p^2-1})$ is p-rational.

Proof.

First note that $\varepsilon = p + \sqrt{p^2-1}$ is a fundamental unit of K.
By a result of Louboutin 1998 we have the effective bound

$$h(K) \leq \sqrt{\mathrm{Disc}(K)}\frac{e\log(\mathrm{Disc}(K))}{4\log\varepsilon}.$$

Since $\mathrm{Disc}(K) \leq p^2-1$, we conclude that $h(K) < p$ and hence $p \nmid h(K)$.

Let us show that ε is not a p-primary unit (p-th power locally but not globally). We have

$$\begin{aligned}
\varepsilon^{p^2-1} - 1 &\equiv (p^2-1)^{\frac{p^2-1}{2}} - 1 + p(p^2-1)^{\frac{p^2-3}{2}}\sqrt{p^2-1} \pmod{p^2\mathbb{Z}[\sqrt{p^2-1}]}\\
&\equiv \pm p\sqrt{p^2-1} \pmod{p^2\mathbb{Z}[\sqrt{p^2-1}]}.
\end{aligned}$$

Since $p^2\mathbb{Z}[\sqrt{p^2-1}] \subset p^2\mathcal{O}_K$ this shows that the p-adic logarithm of ε is not a multiple of p^2, so ε is not p-primary, hence K is p-rational. $\square$

Literature results

Lemma (Movahhedi 1990)

Assume K is a number field which satisfies Leopoldt's conjecture, $p > [K : \mathbb{Q}] + 1$ an odd prime such that $p \nmid h(K)$. Then K is p-rational if and only if $R_p(K)/p^r$ is not divisible by p.

Lemma (Hartung 1974)

For any prime odd prime p there exist infinitely many square-free $D < 0$ such that $h_{\mathbb{Q}(\sqrt{D})} \cdot D \not\equiv 0 \pmod{p}$.

Lemma (Byeon 2001 *)

For $p \geq 5$, there exists infinitely many integers $D > 0$ so that $h_{\mathbb{Q}(\sqrt{D})} \cdot D \not\equiv 0 \pmod{p}$ and $\mathbb{Q}(\sqrt{D})$ has no p-primary units.

Conjectural results

Conjecture (Cohen and Martinet 1987)

Let K be a cyclic cubic number fields and m an integer non divisible by 3. Then we have

$$\mathrm{Prob}(m \mid h_K) = \prod_{p \mid m, p \equiv 1 \mod 3} \left(1 - \frac{(p)_\infty^2}{(p)_1^2}\right) \prod_{p \mid m, p \equiv 2 \mod 3} \left(1 - \frac{(p^2)_\infty}{(p^2)_1}\right),$$

where $(p)_\infty = \prod_{k \geq 1}(1 - p^{-k})$ and $(p)_1 = (1 - p^{-1})$.

Conjecture (Hofman and Zhang 2016)

For primes $p > 3$ we have

$$\mathrm{Prob}(p \text{ divides } R'_{K,p}) = \begin{cases} \frac{1}{p^2}, & \text{if } p \equiv 2 \pmod 3 \\ \frac{2}{p} - \frac{1}{p^2}, & \text{if } p \equiv 1 \pmod 3, \end{cases}$$

where $R'_{K,p}$ is the normalized p-adic regulator.

Conjectural results

Conjecture (Cohen and Martinet 1987)

Let K be a cyclic cubic number fields and m an integer non divisible by 3. Then we have

$$\mathrm{Prob}(m \mid h_K) = \prod_{p\mid m, p\equiv 1 \mod 3} \left(1 - \frac{(p)_\infty^2}{(p)_1^2}\right) \prod_{p\mid m, p\equiv 2 \mod 3} \left(1 - \frac{(p^2)_\infty}{(p^2)_1}\right),$$

where $(p)_\infty = \prod_{k\geq 1}(1-p^{-k})$ and $(p)_1 = (1-p^{-1})$.

Conjecture (Hofman and Zhang 2016)

For primes $p > 3$ we have

$$\mathrm{Prob}(p \text{ divides } R'_{K,p}) = \begin{cases} \frac{1}{p^2}, & \text{if } p \equiv 2 \pmod 3 \\ \frac{2}{p} - \frac{1}{p^2}, & \text{if } p \equiv 1 \pmod 3, \end{cases}$$

where $R'_{K,p}$ is the normalized p-adic regulator.

Theorem

Under the two conjectures above, for all prime $p > 3$, $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, p)$ holds.

Proof.

For any D let $K(D)$ be the set of cubic cyclic number fields with conductor less than D. Then we have

$$\begin{aligned} \limsup_{D\to\infty} \frac{\#\{K \in K(D) \text{ non } p\text{-rational}\}}{\#K(D)} &\leq \limsup_{D\to\infty} \frac{\#\{K \in K(D),\ p \mid h_K R'_{K,p}\}}{\#K(D)} \\ &\leq \mathrm{Prob}(p \mid h_K) + \mathrm{Prob}(p \mid R'_{K,p}) < \frac{1}{2}. \end{aligned}$$

Computational results PARI/GP (in sage)

Proposition (Greenberg) p-rationality of a compositum $\Leftrightarrow$ p-rationality of its cyclic subfields.

p	t	$d_1, \ldots, d_t$
5	7	2,3,11,47,97,4691,-178290313
7	7	2,5,11,17,41,619,-816371
11	8	2,3,5,7,37,101,5501,-1193167
13	8	3,5,7,11,19,73,1097,-85279
17	8	2,3,5,11,13,37,277,-203
19	9	2,3,5,7,29,31,59,12461, -7663849
23	9	2,3,5,11,13,19,59,2803,-194377
29	9	2,3,5,7,13,17,59,293,-11
31	9	3,5,7,11,13,17,53,326,-8137
37	9	2,3,5,19,23,31,43,569,-523
41	9	2,3,5,11,13,17,19,241,-1

Greenberg's proposition $\Rightarrow$ open image representations for $4 \leq n \leq 2^{t-1} - 3$. Our example for $p = 5$ extended the proven values of n from 13 to 63.

Cohen-Lenstra-Martinet for $G = \mathbb{Z}/3\mathbb{Z}$

Conjecture (CLM)

If K is a cyclic cubic number field and m is an integer non divisible by 3, then

$$\mathrm{Prob}(m \mid h_K) = \prod_{p|m, p\equiv 1 \mod 3} \left(1 - \frac{(p)_\infty^2}{(p)_1^2}\right) \prod_{p|m, p\equiv 2 \mod 3} \left(1 - \frac{(p^2)_\infty}{(p^2)_1}\right),$$

où $(p)_\infty = \prod_{k\geq 1}(1 - p^{-k})$ and $(p)_1 = (1 - p^{-1})$.

p	theoretic density	stat. density cond. ≤ 8000	relative error	stat. density cond. $\leq 10^7$	relative error
5	0.00167	$\frac{3}{1269} \approx 0.0236$	46%		
7	0.0469	$\frac{45}{1269} \approx 0.0355$	24%		
11	0.0000689	0	100%		
13	0.00584	$\frac{6}{1269} \approx 0.00472$	19%		
19	0.0128	$\frac{11}{1269} \approx 0.0086$	48%		

In 1989 Cohen and Martinet wrote "we believe that the poor agreement [with the tables] is due to the fact that the discriminants are not sufficiently large".

Cohen-Lenstra-Martinet for $G=\mathbb{Z}/3\mathbb{Z}$

Conjecture (CLM)

If K is a cyclic cubic number field and m is an integer non divisible by 3, then

$$\mathrm{Prob}(m \mid h_K) = \prod_{p \mid m, p\equiv 1 \mod 3} \left(1 - \frac{(p)_\infty^2}{(p)_1^2}\right) \prod_{p \mid m, p\equiv 2 \mod 3} \left(1 - \frac{(p^2)_\infty}{(p^2)_1}\right),$$

où $(p)_\infty = \prod_{k\geq 1}(1-p^{-k})$ and $(p)_1 = (1-p^{-1})$.

p	theoretic density	stat. density cond. ≤ 8000	relative error	stat. density cond. $\leq 10^7$	relative error
5	0.00167	$\frac{3}{1269} \approx 0.0236$	46%	$\frac{3316}{1714450} \approx 0.00193$	15.5%
7	0.0469	$\frac{45}{1269} \approx 0.0355$	24%	$\frac{78063}{1714450} \approx 0.0456$	3%
11	0.0000689	0	100%	$\frac{133}{1714450} \approx 0.0000775$	12.5%
13	0.00584	$\frac{6}{1269} \approx 0.00472$	19%	$\frac{10232}{1714450} \approx 0.00584$	2%
19	0.0128	$\frac{11}{1269} \approx 0.0086$	48%	$\frac{21938}{1714450} \approx 0.0128$	0.2%

In 1989 Cohen and Martinet wrote "we believe that the poor agreement [with the tables] is due to the fact that the discriminants are not sufficiently large".

The case when $G = (\mathbb{Z}/3\mathbb{Z})^2$: class number

Conjecture

If k_1, k_2, k_3 are the three cubic subfields of a number field K of Galois $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ then $\mathrm{Prob}(p \nmid h(K)) = \prod_i \mathrm{Prob}(p \nmid h(k_i)) = \mathrm{Prob}(p \nmid h(k_1))^3$.

p	theoretic density	stat. density cond. $\leq 10^6$	relative error
5	0.00334	$\frac{933}{203559} \approx 0.00458$	37%
7	0.0916	$\frac{23912}{203559} \approx 0.0354$	28%
11	0.000138	$\frac{26}{203559} \approx 0.000128$	7.5%
13	0.0116	$\frac{6432}{203559} \approx 0.0316$	72%
17	0.0000140	$\frac{4}{203559} \approx 0.0000197$	40.5%
19	0.0254	$\frac{3536}{203559} \approx 0.0173$	31.5%

The case when $G = (\mathbb{Z}/3\mathbb{Z})^2$: p-adic regulator

Lemma

Let p be an odd prime and $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with a, b and ab positive rational numbers which are not squares. Let R denote the normalized p-adic regulator of K, then R_1, R_2 and R_3 the p-adic regulators of $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$. Then there exists an integer α such that

$$R = 2^{\alpha} R_1 R_2 R_3.$$

Conjecture

Let $q = 2$ or 3, $p > q$ a prime and t an integer. Then the density of totally real number fields K such that $\mathrm{Gal}(K) = (\mathbb{Z}/q\mathbb{Z})^t$ for which the normalized p-adic regulator is divisible by p for at least one of the cyclic subgroups is

1. $\mathrm{Prob}\left(\exists F \subset K, R'_{F,p} \equiv 0[p] | \mathrm{Gal}(K) = (\mathbb{Z}/2\mathbb{Z})^t \text{ tot. real}\right) = 1 - (1 - \frac{1}{p})^{2^t - 1}$
2. $\mathrm{Prob}\left(\exists F \subset K, R'_{F,p} \equiv 0[p] \mid \mathrm{Gal}(K) = (\mathbb{Z}/3\mathbb{Z})^t\right) = 1 - (1 - \mathcal{P})^{\frac{3^t - 1}{2}}$, where

$$\mathcal{P} = \begin{cases} \frac{2}{p} - \frac{1}{p^2}, & \text{if } p \equiv 1 \pmod 3 \\ \frac{1}{p^2}, & \text{otherwise.} \end{cases}$$

p	experimental density	Conj density	relative error
5	$\frac{29301}{37820} \approx 0.775$	0.790	2%
7	$\frac{19538}{37820} \approx 0.517$	0.660	22%
11	$\frac{17872}{37820} \approx 0.473$	0.487	3%

An arithmétic criterion that $p \nmid R_p(K)/r^p$

Lemma

*For all integers $a \neq 21, 23 \pmod{25}$ the number field defined by f_a as defined in Equation (**??**) has no $R_{K,5} \not\equiv 0 \pmod 5$.*

Proof.

We have $\mathrm{Disc}(f_a) = \mathrm{Disc}(\mathbb{Q}(\alpha))[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]^2$ where α is a root of f_a in its number field. Since

$$\mathrm{Disc}(a) = a^4 + 6a^3 + 27a^2 + 54a + 81,$$

5 is not ramified and doesn't divide the index $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$. The definition of Schirokauer maps implies that if $f \equiv g \pmod{p^2\mathbb{Z}[x]}$ are two polynomials then they have the same Schirokauer maps.
For each a in the interval $[1, 5^2]$ other than 21 and 23 we compute the matrix

$$\begin{pmatrix} \lambda_0(\alpha) & \lambda_1(\alpha) & \lambda_2(\alpha) \\ \lambda_0(-\frac{\alpha+1}{\alpha}) & \lambda_1(-\frac{\alpha+1}{\alpha}) & \lambda_2(-\frac{\alpha+1}{\alpha}) \end{pmatrix},$$

where α is a root of f_a in its number field. Here the λ_i's are defined as in Algorithm **??**. Note that $\frac{\alpha+1}{\alpha}$ is the image of α by an automorphism of f_a. One verifies that in each case the normalized 5-adic regulator is not divisible by 5. Hence, for any integer $a \not\equiv 21, 23 (\mod 25)$, the 5-adic regulator of $\{\alpha, -\frac{\alpha+1}{\alpha}\}$ divided by 25 is not divisible by 5. Finally, the normalized 5-adic regulator of f_a is not divisible by 5. □

An arithmétic criterion that $p \nmid h(K)$

Lemma

Let m be an odd prime, p be inert in $\mathbb{Z}[\zeta_{\frac{m-1}{2}}]$, $\epsilon \in C_m^+$ be any cyclotomic unit. If ϵ is not a p-th power, then $p \nmid h_m^+$. In particular, if $p \nmid m-1$ then the class number of the unique cubic cyclic subfield of $\mathbb{Q}(\zeta_m)^+$ is not divisible by p.

Proof.

By [**?**, Thm. 8.2], $h_m^+ = [E_m^+ : C_m^+]$ where h_m^+, E_m^+, C_m^+ denote the class number, the group of units and the group of cyclotomic units of the maximal real subfield $\mathbb{Q}(\zeta_m)^+$ of $\mathbb{Q}(\zeta_m)$. Let $v \in C_m^+$ generate the group of cyclotomic units as a module over $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})]$ (cf. Washington Prop. 8.11). Note that E_m^+ is a $\mathbb{Z}[\zeta_{\frac{m-1}{2}}]$ module via the action $u^{\zeta_{\frac{m-1}{2}}} := \sigma(u)$, where $u \in E_m^+$ and σ is a generator of the Galois group $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})]$. We are going to show that if v is not a p-th power in E_m^+ then for all $\omega \in \mathbb{Z}[\zeta_{\frac{m-1}{2}}], p \nmid \omega$ V^ω is not a p-th power. Assume on the contrary, $v^\omega = u^p$ for some $u \in E_M^+$. Then $v^{N(\omega)} = u^{\frac{pN(\omega)}{\omega}}$ where $N(\omega)$ denotes the Norm of ω. With $a := N(\omega)^{-1}[p]$, $v^{aN(\omega)} = u^{ap\frac{N(\omega)}{\omega}}$. But this implies that $v \in (u^{a\frac{N(\omega)}{\omega}} E_m^+)^p$ which is a contradiction.

By Leopoldt p. 41, we can decompose h_m^+ as a product of class numbers of cyclic subfields of $\mathbb{Q}(\zeta_m)^+$ and a rational number which is divisible by primes not dividing $m-1$. Thus if $p \nmid m-1$, p does not divide the class number of the unique cubic cyclic subfield of $\mathbb{Q}(\zeta_m)^+$. □

Algorithms to find examples

Lemma (Pitoun and Varescon 2015)

Let K be a number field which satisfies Leopoldt's conjecture. Let e be the ramification index of p in K. Then there exists $n \geq 2+e$ so that the invariant factors of $\mathcal{A}_{p^n}$ can be divided into two sets $FI(\mathcal{A}_{p^n}) = [b_1, \ldots, b_s, a_1, \ldots, a_{r_2+1}]$ such that

1. $\min(\mathrm{val}_p(a_i)) > \max(\mathrm{val}_p(b_i)) + 1$;
2. $FI(\mathcal{A}_{p^{n+1}}) = [b_1, \ldots, b_s, pa_1, \ldots, pa_{r_2+1}]$.

Moreover, K is p-rational if and only if $\mathrm{val}_p(b_1) = \mathrm{val}_p(b_2) = \cdots = \mathrm{val}_p(b_s) = 0$.

Using the algorithm in practice

Input a prime p and a list of cyclic cubic fields
Output for each number field the information whether it is p-rationality

```
for K in list of cyclic cubic fields do
    Apply the arithmetic criterion to certify that p does divides h_K when it is possible
    Apply the arithmetic criterion to certify that p does not divides R'_{K,p} when it is possible
    if we have certificates that p ∤ h_K R'_{K,p} then
        return True and certificates
    else
        Apply the algorithm of Pitoun and Varescon to decide if K is p-rational
        Return answer and certificate
    end if
end for
```

Main result

Theorem

1. *For all odd primes p, $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ holds.*
2. *Assume there exist infinitely many odd integers $a \not\equiv 21, 23 \pmod{25}$ so that $m := \frac{1}{4}(a^2 + 27)$ is prime and [arithmetic conditions not published in the arxiv version]. Then $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, 5)$ holds.*
3. *Under conjectures based on heuristics and numerical experiments, when $q = 2$ or 3, for any prime p and any integer t such that $p > 5q^t$, $\mathrm{GC}_\infty((\mathbb{Z}/q\mathbb{Z})^t, p)$ holds.*